Best practice: Projectontwerp van beveiligingstests van webapplicaties

Versie 1.01, 08. oktober 2009
Vertaling, december 2013

Auteur: *OWASP German Chapter* met medewerking van (in alfabetische volgorde):
Marco Di Filippo Tobias
Glemser Achim
Hoffmann Barbara
Schachner Dennis
Schröder Feiliang Wu
Henk-Jan Angerman

Vertaling: SECWATCH Nederland i.s.m. Ottenhof taal & media, Almere

Over ...

Dit document is samengesteld door *OWASP German Chapter*. De auteurs zijn medewerkers van ondernemingen die penetratietests van webapplicaties uitvoeren, respectievelijk aan de kant van de klant actief zijn en het project op zich nemen.

Auteurs (alfabetische volgorde)

Marco Di Filippo marco.difilippo@csnc.ch Compass Security AG

Tobias Glemser tglemser@tele-consulting.com Tele Consulting security | networking | training GmbH Achim

Hoffmann ah@securenet.de SecureNet GmbH

Barbara Schachner barbara.schachner@siemens.com Siemens AG - Corporate Technology Dennis

Schröder d.schroeder@tuvit.de TÜV Informationstechnik GmbH

Feilang Wu feiliang.wu@siemens.com Siemens AG - Corporate Technology

Terminologie

De in dit document gebruikte vaktermen worden niet nader uitgelegd, maar als bekend verondersteld. Er is bewust afgezien van een begrippenlijst, zodat de omvang overzichtelijk blijft en de inhoud geconcentreerd blijft op het eigenlijke thema: de beschrijving van eisen.

Uitvoerige begripsverklaringen en uitgebreidere beschrijvingen die betrekking hebben op op WAS – Web Application Security – zijn hier te vinden:

- http://www.owasp.org/index.php/Category:Attack OWASP Category:Attack
- http://www.owasp.org/index.php/Category:Threat OWASP Category:Threat
- http://www.owasp.org/index.php/Category:Vulnerability OWASP Category:Vulnerability
- http://projects.webappsec.org/Threat-Classification-Reference-Grid
  WASC Web Application Security Consortium: WASC Threat Classification
- http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.de.pdf
  WASC Web Application Security Consortium: Web Security Threat Classification

Licentie

Inhoud

1. Inleiding tot en doel van dit document

1.1 Inleiding

Het testen van de beveiliging van webapplicaties wordt inmiddels door vele bedrijven als noodzakelijke stap erkend. Met name voor de eerste test is het voor exploitanten van webapplicaties lastig een adequaat project op te zetten. Het gaat er enerzijds om de projectfocus helder te definiëren, om offertes te kunnen vergelijken, en anderzijds zo transparant mogelijk de expertise van de dienstverleners te kunnen bepalen.

1.2 Begripsdefinities

Klant: een klant in de zin van dit document is een exploitant van webapplicaties, die op zoek is naar een dienstverlener (intern of extern) voor een beveiligingstest van zijn webapplicaties.

Interne of externe dienstverlener: afdeling of onderneming met expertise in de uitvoering van beveiligingstests van webapplicaties.

Webapplicatie: met webtechnologie gebouwde applicatie (bijv. klassieke internetpresentatie, web-API, web-frontend van applicatieservers). Dit kunnen eenvoudige applicaties (meestal statische, op een server opgeslagen inhoud), maar ook complexe, dynamische applicaties (meerdere servers, loadbalancer, 3-tier-architectuur, etc.) zijn.

1.3 Doelgroep en doelstelling

De doelgroep bestaat in de eerste plaats uit exploitanten van webapplicaties, die een projectontwerp voor het testen van de beveiliging van hun webapplicatie willen. Zij krijgen met dit document een leidraad in handen voor het volledige proces. Deze leidraad begint met de definitie van de projectdoelen, en gaat van de projectplanning tot de aanbesteding. De keuze van de juiste dienstverlener hangt van veel factoren af en is voor elke klant en elk project anders en op het eerste gezicht voor de klant zelden transparant. Daarom wordt in het kader van dit document geprobeerd een generiek hulpmiddel te bieden, om met transparante methoden de geschiktste dienstverlener te bepalen.

1.4 Afbakening

Er is geprobeerd het document zo ‘ontechnisch’ mogelijk te formuleren en niet de technische inhoud van andere publicaties te herhalen. Voor zover het de algemene begripsvorming dient, is hier en daar technische uitleg opgenomen, in het bijzonder bij de beschrijving van de soorten tests. Deze dienen echter alleen tot een vlug begrip van de concepten en afbakeningen en worden niet uitputtend behandeld. Daarom zijn referenties opgenomen naar andere documenten, waarin de technische details te vinden zijn.

1.5 Actualiseringen

Het projectteam is altijd blij met opbouwende feedback en doet zijn best die in toekomstige versies mee te nemen. De actuele versie van dit document bevindt zich op de projectwebsite. Feedback kan worden gestuurd naar een van de auteurs die bij de samenstelling van dit document betrokken zijn.

2. Eisen

Als het besluit tot een beveiligingstest van een webapplicatie is genomen, zijn er reeds eisen van de kant van de klant bekend, ook als deze in voorkomende gevallen nog niet volledig gedefinieerd zijn. Zo bestaan er ook meestal bepaalde beelden van de eisen die aan de dienstverlener worden gesteld.

Het volgende hoofdstuk is dienovereenkomstig ingedeeld. Paragraaf 2.1 gaat over de vraagstellingen die een klant in zijn productvereistendocument kan opnemen. Paragraaf 2.2 zet uiteen welke minimumeisen er aan een dienstverlener worden gesteld en met welke methoden dat eisenprofiel kan worden getoetst.

2.1 De kant van de klant

Als men het testen van een webapplicatie wil laten uitvoeren – door een interne of externe partij – dan is de ontwerpfase van het project doorslaggevend voor het succes ervan. Hierin moet de klant bindende richtlijnen vastleggen voor de omvang en de aard van de test en de toe te passen methodiek. Grove fouten in deze fase zijn tijdens de uitvoering van het project maar moeilijk goed te maken. Bovendien is het vastleggen van randvoorwaarden belangrijk voor de vergelijkbaarheid van offertes. Wie water wil en later wijn krijgt (en betalen moet) is net zo ontevreden als wie het omgekeerde overkomt.

De volgende paragrafen geven daarom passende tips voor vaak optredende moeilijkheden en aanbevelingen voor het vermijden van eventuele misverstanden.

Omdat er ook in de ontwerpfase van het project reeds fundamentele kennis nodig is, kan het met name bij het eerste onderzoek zinvol zijn, in het kader van een workshop gezamenlijk met interne of externe experts een aanpak te ontwikkelen. Tips voor de keuze van dienstverleners vindt u in paragraaf 2.2. Voor zover er een externe dienstverlener bij de ontwikkeling van het programma van eisen betrokken is, mag deze om de neutraliteit te waarborgen en op grond van eventuele wettelijke regelingen niet aan de uiteindelijke aanbesteding deelnemen.

2.1.1 Aard van de test

Voor het ontwerp van het project en vooral voor de aanbestedingsfase is het van cruciaal belang om vast te leggen welke soort test gewenst is. Er zijn zeer verschillende testopzetten, die steeds voortkomen uit andere motivaties en zich onderscheiden qua methodiek, omvang, tijdsinvestering, diepgang van de resultaten en informatiewaarde.

Er wordt aangeraden de aanbesteding af te stemmen op erkende teststandaarden of ten minste op de methodiek daarvan. Daarmee worden richtlijnen geformuleerd en wordt gezorgd voor een fundamentele vergelijkbaarheid van de uitvoering.

Het doel van een onderzoek is, naast transparantie van de methoden, de reproduceerbaarheid van de tests. Deze eis moet in de aanbestedingsdocumenten opgenomen zijn. IT-beveiliging wordt pas door transparantie sterk, anders kunnen de omvang en informatiewaarde van het resultaat behalve door de tester zelf door niemand op waarde worden geschat.

2.1.1.1 Vulnerability-Assessment (VA) / penetratietest van de webapplicatie

Om een aanval op een webapplicatie te simuleren, kan men gebruikmaken van de methodiek van Vulnerability-Assessment (VA) of penetratietests. Een Vulnerability Assessment wordt in dit verband beschouwd als een onderzoek dat uitsluitend bekende zwakke plekken bepaalt (overwegend toolgebaseerd). Als deze aanpak wordt aangevuld met handmatige methoden en de ervaring en creativiteit van de tester, dan wordt de test aangeduid als penetratietest.

Er zijn verschillende aanpakken voor de uitvoering van penetratietests. Enkele zijn zeer algemeen geformuleerd, om liefst in elke IT-omgeving toepasbaar te zijn. Een bekende aanpak is het *Durchführungskonzept für Penetrationstests* [Uitvoeringsconcept voor penetratietests] van het Bundesamt für Sicherheit in der Informationstechnik (BSI: www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf). Een andere standaard biedt het *Open Source Security Testing Methodology Manual* van de ISECOM (http://www.osstmm.org/), waar internationaal vaak naar wordt verwezen. Veel adviesbureaus hebben overeenkomstig hun eigen zwaartepunten deels eigen methoden ontwikkeld, die echter vaak gebaseerd zijn op standaarden en daarmee compatibel zijn.

Typische beschrijvingen van de uitvoering van penetratietests op webapplicaties zijn bijvoorbeeld te vinden in de *OWASP Testing Guide* (http://www.owasp.org/index.php/Category:OWASP_Testing_Project). Een algemene, maar toch webapplicatiespecifieke aanpak, waarin meerdere methoden verenigd zijn, is de *OWASP Application Security Verification Standard* (http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project).

Een algemeen onderscheid dat wordt gemaakt, is dat tussen black- en whiteboxtests. Dit verschil is voor het configureren van de test van een doorslaggevende factor en bepaalt het type (gesimuleerde) aanval.

Bij blackboxtests geeft de klant de dienstverlener meestal geen of slechts zeer gemakkelijk op te sporen gegevens om te gebruiken. Het louter beschikbaar stellen van aanmeldingsgegevens wordt in de rest van dit document als een blackboxtest beschouwd. Blackboxonderzoeken zijn in principe dynamische onderzoeken, omdat de tests op het lopende systeem worden uitgevoerd. De broncode wordt in dit soort onderzoeken niet beschikbaar gesteld. Daarom nemen de dienstverleners hier de rol op zich van een aanvaller zonder verdere kennis van de IT-infrastructuur en proberen zij de applicatie te compromitteren. Het voordeel is dat de klant een beeld krijgt van het gemak waarmee de applicatie van buiten is aan te vallen. Het nadeel is dat de dienstverleners slechts de zwakke plekken volgens de huidige stand van de kennis kunnen vinden. Zwakke plekken die pas met betere kennis (bijv. architectuur) misbruikt kunnen worden, worden normaal gesproken niet geïdentificeerd. De klant moet ervan uitgaan dat een aanvaller een onbepaalde hoeveelheid tijd heeft om naar zwakke plekken te zoeken en dus ten opzichte van de dienstverlener in het voordeel is.

Verder moet de klant zorgvuldig overwegen of hij opdracht geeft tot blackboxtests van productieve systemen, in plaats van een testsysteem met overeenkomstige testgegevens beschikbaar te stellen. Bepaalde tests kunnen het productieve systeem zelf in een functioneel instabiele toestand brengen of zelfs productieve gegevens wissen, veranderen en voor derden zichtbaar maken. Overigens kan dit gevaar bij de applicatie door de methodiek worden ingeperkt.

Bij whiteboxonderzoeken krijgt de dienstverlener van de klant uitvoerige informatie over de applicatie. Zo kan bijvoorbeeld een aanval van de kant van een externe contractpartner of een medewerker worden gesimuleerd. Aan deze aanpak zitten wel grenzen, omdat bijvoorbeeld het aanvalstype beheerder vanwege de vele kennis van een beheerder of zelfs een beheerdersteam niet reëel is toe te passen.

Het gaat er dus om te zorgen voor een voor de huidige behoeften van de klant optimale kennispositie en een goede kennisoverdracht van de informatie aan de dienstverlener.

Bij alle tests is van belang dat er zonder speciale testprogramma's geen serieuze test kan plaatshebben. De omvang van webapplicaties overstijgt tegenwoordig in de regel duidelijk de omvang en complexiteit die een handmatige test mogelijk zou maken. Toch is een handmatige test van de webapplicatie, net als een aanvullende handmatige verificatie van alle resultaten, noodzakelijk.

De definitie van de testomvang kan groter zijn dan de webapplicatietest alleen. Zo kunnen bijvoorbeeld aanvullende netwerkgebaseerde penetratietests worden ingezet, die de webserverdienst, de databankserver, firewalls en dergelijke in het onderzoek betrekken.

Of een opdeling, dus een modularisering van de tests, zinvol is, hangt af van het betreffende scenario. Met name als er vele diensten worden geleverd, kan modularisering efficiëntiewinst betekenen.

Ook moet de vraag worden beantwoord of Denial-of-Service-aanvallen (DoS) moeten worden uitgevoerd. Deze zijn erop gericht onbereikbaarheid te bewerkstelligen door gebruik te maken van zwakke plekken of door het systeem respectievelijk de dienst te overspoelen met aanvragen. Dit is echter maar heel zelden werkelijk zinvol. Het is beter specificaties van de belasting op te stellen en de maximale belasting te laten testen. Dit zou bij juiste toepassing van de specificaties niet tot uitval mogen leiden.

SaaS - Software as a Service

Naast de gebruikelijke vorm, waarbij de dienstverlener de beveiligingstests expliciet op verzoek aanbiedt en oplevert, bestaat er nog de mogelijkheid om de beveiligingstests door – min of meer – volledig geautomatiseerde diensten te laten plaatsvinden. De term hiervoor is SaaS, en deze wordt hieronder kort beschreven.

SaaS (Software as a Service) is een softwareverspreidingsmodel, dat software als dienstverlening, gebaseerd op internettechniek, beschikbaar stelt (ook bekend als ASP - Application Services Provider). Dat wil zeggen dat de software door een dienstverlener via internet wordt bediend, waardoor een installatie bij de klant (consument) vervalt.

Als het testen van de beveiliging van webapplicaties als automatische, regelmatige dienstverlening wordt aangeboden, gaat het daarbij in wezen om een nauwkeurig gedefinieerde scan van de website op zwakke plekken.

Dit bedrijfsmodel vormt een dienstverleningsalternatief voor zowel de aanschaf van een scantool als een eenmalige penetratietest.

De voordelen voor de klant ten opzichte van dienstverlening per enkele opdracht zijn:

- eenmalige uitgave voor het projectontwerp, en daardoor goedkoper;
- gemakkelijke herhaling van beveiligingstests;
- regelmatige tests, en daardoor voortdurende kennis over de beveiligingstoestand.

De vaak beloofde enorme kostenbesparing ten opzichte van het alternatief heeft echter ook enige nadelen met betrekking tot de beveiligingstests zelf en de daarmee verbonden omgeving. Men moet vooral letten op het volgende:

- De invoering van SaaS kan belemmerd worden doordat er binnen de onderneming (klant) bedenkingen bestaan met betrekking tot de betrouwbaarheid van en de controle op de aanbieder, omdat deze geautomatiseerd in bezit komt van gevoelige data en zwakke plekken. Hier moeten dus extra veiligheidsmaatregelen tegen misbruik worden getroffen.
- Wat gebeurt er met de gegevens van de test(s) als de dienstverlener bijvoorbeeld failliet gaat of verkocht wordt?
- De te testen applicaties moeten in de regel over het open internet toegankelijk zijn.
- De ontwikkeling van bijvoorbeeld firewallregels, VPN-tunnels of inrichting van speciale applicatie-proxy's voor de scans kost een extra inspanning voor de klant.

Verder moet de klant overwegen of de bij reguliere, herhaalde scans betrokken IDS/IPS en met name WAF's gedeactiveerd moeten worden of als onderdeel van het totale systeem meegetest zullen worden.

Een regelmatige, herhaalde beveiligingstest in de vorm van SaaS zal men wellicht willen inrichten voor de productieve webapplicaties. In tegenstelling tot de gebruikelijke penetratietests, die op een werk- of referentieplatform plaatsvinden, moet er rekening mee worden gehouden dat de normale werking door de verhoogde workload wordt gestoord.

Als men kiest voor SaaS, gelden dezelfde regels en aanbevelingen bij de keuze voor de dienstverlener en de latere uitvoering als bij de andere beveiligingstests. Men moet er echter rekening mee houden dat er extra vragen gesteld moeten worden en daarmee ook aanvullende eisen aan de dienstverlener moeten worden gesteld.

Samenvattend moet er bijzondere aandacht aan de volgende eisen worden besteed:

- **Klanteisen**
  - test van de productieve webapplicatie?
  - speciale testtoegang (VPN)?
  - met of zonder IDS/IPS en WAF?
  - testtijden;
  - is de webapplicatie automatisch scanbaar?
- **Dienstverlenerseisen**
  - bescherming van de gegevens en testresultaten;
  - toegang tot de testresultaten;
  - deskundige ondersteuning bij de evaluatie van de testresultaten;
  - zijn er geschikte scantools voorhanden?

2.1.1.2 Broncodeanalyse

In vergelijking met penetratietests levert een broncodeanalyse een grotere informatiewaarde. Hierbij wordt de webapplicatie op basis van de volledige broncodes geanalyseerd op zwakke plekken. De broncode is evenwel, bijvoorbeeld bij toepassing van een commerciële webapplicatie, niet altijd beschikbaar.

Omdat de code meestal vele regels omvat, is een zuiver handmatige analyse ook hier niet meer mogelijk. Van belang bij de uitvoering van broncodeanalyses zijn de kracht van de tool en de competentie van de tester, aangezien elke tool op vele manieren te parametriseren is.

2.1.1.3 Architectuuranalyse

Bij de architectuuranalyse kunnen vele parameters van de totale omgeving worden onderzocht. Doel hierbij is om eventuele bestaande zwakke plekken – door de structuur van de omgeving, door de gebruikte serverdiensten of andere omstandigheden – aan te tonen. Mogelijke zaken om te bekijken zijn onder andere:

- gebruikte serverdiensten;
- netwerkverbindingen intern, extern (internet);
- versleuteling van de data bij verzending en opslag;
- bewaartijden van naar voren gekomen gegevens;
- uitvalzekerheid van componenten.

2.1.1.4 Proces- en documentatieanalyse

Duidelijk verder dan de hiervoor genoemde analyses gaat de proces- en documentatieanalyse. Deze omvat zowel richtlijnen als omzetting van probleemstellingen als:

- ontwikkelaarsrichtlijnen;

- reactierichtlijnen;
- systeem- en serverdiensten-richtlijnen (hardingsconcepten, administratieve richtlijnen, patchmanagement);
- versleutelingsrichtlijnen (cryptoconcept).

Veel van deze vragen worden door Information-Security-Management-System-Standards (ISMS) behandeld. In het Duitse taalgebied vindt hier meer en meer de *ISO 27001 auf der Basis von IT-Grundschutz* (www.gshb.bund.de) ingang; internationaal is dat de *ISO/IEC 27001*. In Nederland is NEN-norm NEN-ISO/IEC 27001:2005 vertaald naar het Nederlands verplicht gesteld voor Nederlandse overheden.

2.1.2 Doelformulering en omgevingsbeschrijving

2.1.2.1 Definitie van de testdoelen

Zoals uit de beschrijving van de soorten tests kan worden afgeleid, kunnen beveiligingstests van webapplicaties verschillende doelen hebben. De volgende matrix geeft de verschillende uitgangssituaties en de daaruit voortvloeiende aanbevolen tests weer. De beoordeling vindt afzonderlijk plaats, d.w.z. dat er geen ontwikkelingsmodel wordt gevolgd. Het spreekt vanzelf dat de matrix niet op elke omgeving in dezelfde mate toepasbaar is, maar zij geeft toch een indruk van de benodigde inspanning. In de matrix wordt onderscheid gemaakt tussen de interne tijdsinvestering, die door de klant voor voorbereiding, evaluatie en medewerking tijdens de tests moet worden ingepland, en de externe tijdsinvestering, die van de dienstverlener wordt gevergd.

Doel	Soort test	Tijdsinvestering	
		intern	extern
Bekende en misbruikbare zwakke plekken van de webapplicatie identificeren	Blackboxtest	gering	gemiddeld
Betrouwbaar bekende en misbruikbare zwakke plekken van de webapplicatie identificeren	Whiteboxtest	gemiddeld	gemiddeld
Bekende en misbruikbare zwakke plekken van de omgeving identificeren	Blackboxtest	gering	gemiddeld
Betrouwbaar bekende en misbruikbare zwakke plekken van de omgeving identificeren	Whiteboxtest	gemiddeld	gemiddeld
Bekende en potentiële zwakke plekken van de webapplicatie identificeren	Broncode-analyse	gemiddeld	groot
Infrastructurele problemen identificeren	Architectuur-analyse	gemiddeld	gemiddeld
Problemen in de structuur en zwakheden in de richtlijnen identificeren, eventueel opbouw van een ISMS	Proces- en documentatie-analyse	groot	groot

Indien budgettair niet alle gewenste tests kunnen worden uitgevoerd, dan bestaat er ook de mogelijkheid om een worstcasescenario te definiëren en het onderzoek te concentreren op dit scenario.

2.1.2.2 Beschrijving van de omgeving

Om een algemeen geldend begrip voor interne en externe betrokkenen mogelijk te maken, is het noodzakelijk om de te testen omgeving te beschrijven. De volgende uiteenzetting concentreert zich primair op de technische tests van de webapplicatie, zonder een uitbreiding naar de tests op de omgeving. De aanbeveling is om de volgende elementen te beschrijven:

- overzicht van de webapplicatie: taak, ondersteund bedrijfsproces, rechtenmanagement;

  Deze informatie maakt het mogelijk dat een tester die tot dan toe nog niet vertrouwd is met de applicatie een eerste inschatting van de taakstelling kan maken.

- toegangswegen: internet, intranet, VPN, proxy;

  Met name de beveiligingsbeoordeling en de soort test (bijv. bij de inzet van een proxy) zijn afhankelijk van deze technische factoren.

- eventuele speciale clients: fat clients, alleen specifieke browsers;

  De beperking tot specifieke clients heeft directe gevolgen voor de testmogelijkheden en verhoogt meestal de omvang van de voorbereidingen.

- logica van de webapplicatie: aantal rechtenprofielen, sessiemanagement;

  Met het aantal rechtenprofielen wordt ook het aantal aanbevolen teststappen groter, om een rechtenuitbreiding in de afzonderlijke bevoegdhedenniveaus te kunnen testen.

- beschrijving van het rollenconcept van de gebruiker: welke authenticatieprocedure is beschikbaar resp. wordt gebruikt:

  - alleen anonymous users;
  - authenticatie met gebruikersnaam en wachtwoord;
  - gebruikersnaam+wachtwoordt met zelfregistratie, User/Pass/OneTimePass of client-certificaat;

- omvang en structuur van de webapplicatie: aantal pagina's/variabelen, gebruikte programmeertaal/scripttaal, databases;

  Het aantal pagina's resp. variabelen is meestal niet gemakkelijk vast te stellen en is ook slechts een indirecte indicator voor de testomvang. De programmeertaal is van invloed op de te gebruiken tests, net als de gebruikte databases en hun verbindingen (bijv. een database op dezelfde host, in hetzelfde netwerk).

- manier van functioneren van de webapplicatie: 'klassieke', controller-/single-URL- applicatie;

  De manier waarop de logische structuur van een functie technisch (programmatisch) in de webapplicatie is geïmplementeerd, is voor de tester van belang, want dat bepaalt de keuzemogelijkheden voor de in te zetten tools en dat er hogere testkosten kunnen ontstaan. Zo is het bijvoorbeeld moeilijker om een controller-applicatie te onderzoeken dan een applicatie die voor iedere functionaliteit een eigen URL heeft.

- architectuur: netwerkschema, serverdiensten, firewallsystemen (netwerk- en applicatiefirewalls)

  Met behulp van een overzicht van de architectuur is het mogelijk technische valstrikken op te sporen. Zo moet bijvoorbeeld de vraag worden beantwoord of de test met inbegrip van de Web Application Firewall zal plaatsvinden of niet. Betrekt men de WAF erbij, dan kan een eventuele onveilige applicatie door de WAF als veilig worden geattesteerd. Als de WAF niet onderzocht wordt, dan moet er rechtstreeks op de webapplicatie worden getest (de WAF moet dan dus doelbewust worden uitgezet/gedeactiveerd of er moet in de DMZ worden getest).

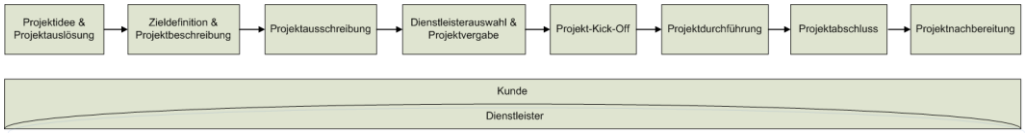
- datastroomschema

  Het datastroomschema maakt een snel overzicht mogelijk over het samenspel van de afzonderlijke componenten. De ervaring leert dat de eerste opbouw van een dergelijk schema bij complexere webapplicaties een kostbare aangelegenheid is en tot een of andere verrassing leidt, daar een dergelijk totaaloverzicht vaak ontbreekt en er daarom intern verschillende meningen bestaan over de verzameling, opslag, doorgifte en het wissen van data binnen de webapplicatie.

2.1.3 Organisatorische aspecten

Vrijwel alle plannen in bedrijfsleven, publieke sector, onderzoek en politiek worden tegenwoordig in de vorm van projecten gegoten. Om de kans op succes van een project in het domein van de beveiligingstests van webapplicaties te vergroten worden hierna de randvoorwaarden en kritieke factoren van projectmanagement toegelicht. Het verloop van een project om de beveiliging van webapplicaties te testen is vereenvoudigd weergegeven in figuur 1.

Opmerking [MTA1]: Projectidee e
projectinitiatie
Doeldefinitie en projectbeschrijving
Projectaanbesteding
Dienstverlenersselectie en
projectgunning
Project-kick-off
Projectuitvoering
Projectafsluiting
Projectevaluatie
Klant
Dienstverlener



Figuur 1: Schematische structuur van beveiligingstestprojecten

2.1.3.1 Projectidee en projectinitiatie

Er zijn vele gronden voor projecten op het terrein van IT-beveiliging. Voor projecten voor het testen van de veiligheid van webapplicaties is dat zeker niet anders. De projecten worden veroorzaakt door een idee, een probleemstelling, een verzoek, een compliance-eis, geconstateerde overtredingen van de beveiligingsrichtlijn of twijfels over de beveiliging. In deze fase vinden aan de kant van de klant de eerste gesprekken plaats over de zin en het nut van een beveiligingstest van webapplicaties. Daarbij komen ook niet zelden eerste contacten met belangrijke toekomstige projectaanspreekpunten en -beslissers tot stand.

2.1.3.2 Doeldefinitie en projectbeschrijving

In de voorbereidingsfase van het project is het zaak doelstellingen, termijndoelen, kostendoelen en eventuele bijzondere doelen te definiëren. Bijgevolg omvat de projectvoorbereiding aan de kant van de klant zowel inhoudelijke alsook organisatorische aspecten. In het kader van de inhoudelijke projectvoorbereiding is het aan de projectleiding de projectbeschrijving uit te werken. De inhoudelijke projectbeschrijving omvat in wezen het volgende:

- Uitgangssituatie en motivering: beknopte uiteenzetting van de 'is'-situatie en de beweegredenen voor de geplande beveiligingstests van de webapplicatie in het perspectief van de klant.
- Doelen en mijlpalen: formulering van de doelen die de klant met het realiseren van de beveiligingstests wil bereiken. Op deze plaats moet er rekening mee worden gehouden dat een oppervlakkige testdiepte of het uitsluitend testen van testsystemen een negatief effect heeft op de kwaliteit en informatiewaarde van de beveiligingstest. Vastlegging van de resultaten die door de opdrachtgever in het kader van het project worden verwacht en van de mijlpalen. Zo ontstaan een projectplan en specificaties, waarin de doelen zo precies mogelijk worden gedefinieerd, zodat het opstellen van taakblokken en de benodigde resources mogelijk wordt.
- Randvoorwaarden en afbakeningen: formulering van aspecten die bij de projectuitvoering als voorwaarden en/of eisen te beschouwen zijn, bijvoorbeeld: de beschikbaarheid van de webapplicatie en/of productieve systemen die niet binnen de verantwoordelijkheid van de klant liggen. Vastlegging van interfaces, datastromen, systemen en componenten die tot de te onderzoeken webapplicatie behoren.

De dienstverlener kan in de uitwerking van deze inhoudelijke gegevens worden beperkt als de klant geen eenduidige informatie kan verstrekken respectievelijk als deze hiaten,

tegenstrijdigheden of onregelmatigheden te zien geven. De organisatorische projectvoorbereidingen zijn voornamelijk als volgt ingedeeld:

- Deelnemers: op grond van de projectbeschrijving worden de betrokken domeinen (bijv. firewall, netwerk, systeem, database en applicatie) uitgekozen die aan de kant van de klant een wezenlijk aandeel hebben in de uitwerking van de projectresultaten. De gekozen medewerkers moeten voor de duur van de projectuitvoering worden vrijgesteld. Bovendien moeten de vertegenwoordigingsregelingen, de escalatieladder en overeenkomstige aanspreekpunten van de betrokken domeinen bekend worden gemaakt.
- Projectsturing en feedback: hoewel de projectsturing primair bij de klant als opdrachtgever ligt, blijkt het meestal voordelen te hebben om de dienstverlener daarbij te betrekken. Met name voor de uitvoering van de beveiligingstests, dus de afzonderlijke op elkaar afgestemde activiteiten en fasen, moet de projectsturing worden overgedragen aan de dienstverlener. Bovendien moet op dat punt in goed overleg een aanpak worden gevonden voor de terugmelding van zwakke plekken en voor de omgang met hardingsmaatregelen achteraf.
- Plaats en tijd: uit het projectplan blijken plaats, tijd en eisen aan resources zoals deelnemers en componenten van de webapplicatie.
- Scanvrijgaven: in het kader van de inhoudelijke projectvoorbereiding zijn de te onderzoeken systemen (test- en/of productieve systemen) en componenten vastgelegd. Om inconsistenties bij de doelen van de technische beveiligingstests tussen klant, exploitant (outsourcing) en dienstverlener te voorkomen, moeten de systeemverantwoordelijken de dienstverlener concrete scanvrijgave verstrekken.
- Vertrouwelijkheidsverklaringen: met behulp van een vertrouwensovereenkomst wordt de dienstverlener tot geheimhouding van informatie verplicht. De definitie van de geheim te houden informatie ressorteert bij de afzonderlijke contractanten. De resultaten, in het bijzonder de ontdekte zwakke plekken, moeten geheim te houden informatie zijn.
- Veiligheidstests en -verklaringen: over de vertrouwelijkheidsverklaring heen heeft de Duitse beveiligingstestwet voorwaarden en procedures vastgesteld voor de beveiligingstests van personen die bepaalde veiligheidsgevoelige werkzaamheden toevertrouwd moeten worden of reeds toevertrouwd zijn. De resulterende beveiligingsverklaringen kennen drie mogelijke gedaanten en zijn overwegend van toepassing op de overheid.
- Aansprakelijkheid: in de samenstelling van het contract respectievelijk de offertes van de dienstverleners zijn meestal aansprakelijkheidscriteria en -beperkingen opgenomen. De projectleiding van de kant van de klant moet de contractbepalingen verifiëren en zo nodig voorafgaand aan de projectgunning optimaliseringen van het volledige contract eisen.

2.1.3.3 Projectaanbesteding

De projectaanbesteding door de klant of eventueel door een bemiddelende instantie vindt meestal plaats aan de hand van wat gebruikelijk is in de branche in de particuliere of publieke sector. In deze fase moet de klant de potentiële niet-kritieke informatie voor het opstellen van de offerte ter beschikking stellen. Naast de inhoudelijke en organisatorische aspecten zijn voor de dienstverlener in het kader van de projectaanbesteding verder onder andere de volgende technische gegevens interessant:

- algemene korte beschrijvingen van de systemen resp. componenten;
- vereenvoudigde netwerkschema's;
- vereenvoudigde datastroomschema's.

2.1.3.4 Diensterverlenersselectie en projectgunning

De fase van de diensterverlenersselectie kan van klant tot klant zeer verschillen. Om het project zo optimaal mogelijk te gunnen, moeten de offertes van de dienstverleners aan de hand van paragraaf 2.2 voor het concrete project worden beoordeeld en op een adequate wijze worden vergeleken. Het moet voor de klant duidelijk zijn dat een oppervlakkige testdiepte een negatief effect heeft op de kwaliteit en informatiewaarde van de beveiligingstest en een positief effect op de kosten, en omgekeerd.

2.1.3.5 Project-kick-off

Bij de project-kick-off wordt alle projectinformatie van alle plaatsen en instanties doorgestuurd aan de projectmedewerkers. De projectinformatie onderscheidt zich in mate van detail en is in tegenstelling tot de projectbeschrijving meer van technische aard, zodat in deze fase de dienstverlener meestal de beschikking krijgt over concrete URL's, IP-adressen, hostnamen en aangeboden diensten alsmede gedetailleerde netwerkschema's en datastroomschema's. De dienstverlener beschrijft zijn aanpak van en omgang met terugmeldingen van gevonden zwakke plekken, wijst op mogelijke risico's en geeft aan welke scanvrijgaven van systemen en componenten nodig zijn. Alle betrokkenen stemmen gezamenlijk de projectaanpak af en leggen de werkwijze ter realisatie van de doelen en mijlpalen contractueel vast. Daarbij kan het beslist tot aanpassingen van de door de klant geplande doelen, mijlpalen en aanpak komen. Zo worden bijvoorbeeld afhankelijk van compliance-eisen (bijv. PCI DSS < Version 1.2) productieve systemen in plaats van testsystemen aan een DoS-aanval onderworpen, hoewel de eisen met betrekking tot de beschikbaarheid dit uit bedrijfspolitieke overwegingen verbieden.

2.1.3.6 Projectuitvoering

De projectuitvoering vindt plaats in van tevoren afgestemde samenwerking tussen klant en dienstverlener. Van de kant van de klant moeten de daarbij betrokken medewerkers de dienstverlener de benodigde toegangsgegevens en rechten geven en achtergrondinformatie alsmede terugmeldingen over bepaalde aanvalsvectoren kunnen geven.

2.1.3.7 Projectafsluiting

Na het realiseren van de doelen en mijlpalen wordt een project voor het testen van de beveiliging van webapplicaties afgesloten met een rapport en eventueel een presentatie van de dienstverlener.

2.1.3.8 Projectevaluatie

Na de projectafsluiting is het aan te raden de in het rapport gemelde beoordelingen intern met de verantwoordelijken van de domeinen te bespreken en de beoordeling van de dienstverlener zo nodig aan te passen. Van meer betekenis is het vastleggen van de verantwoordelijken voor het herstel van de technische en organisatorische zwakke plekken.

2.2 Gegevens van de dienstverlener

De selectie van een geschikte dienstverlener blijkt vaak zeer moeilijk te zijn, omdat er vele factoren een belangrijke rol spelen en een werkelijke vergelijkbaarheid van dienstverleners niet aan de orde is. In deze paragraaf worden daarom uiteenlopende eisen voor verplichtende en optionele informatie over de dienstverlener weergegeven, om de klant de mogelijkheid te geven verschillende dienstverleners te vergelijken.

2.2.1 Noodzakelijke gegevens

2.2.1.1 Ondernemingsgeschiedenis – leeftijd, specialisatie

De beschrijving van de onderneming en haar geschiedenis dient om in te schatten wat haar vaktechnische kwalificaties zijn. Relevante gegevens zijn onder meer de beschrijving van het ontstaan en de ontwikkeling van de onderneming alsmede een dienstverleningsportfolio, waaruit blijkt welke aspecten van IT-beveiliging door de onderneming worden geleverd. Bovendien is het van belang dat de dienstverlener een overzicht geeft van zijn eerdere ervaringen met de behandelde thematiek.

De beschrijving en geschiedenis van een onderneming kunnen al enige aanwijzingen geven, maar zijn geen doorslaggevend bewijs voor de kwaliteit van de dienstverlener.

Uit de beschrijving moet eenduidig blijken dat de onderneming concreet gespecialiseerd is op het terrein van webapplicatiebeveiliging en ervaring op dit gebied heeft. Wordt het thema webapplicatiebeveiliging in de beschrijving helemaal niet genoemd, dan kan worden geconcludeerd dat de complexiteit van het thema wordt onderschat en het onderzoek slechts zeer oppervlakkig zal worden uitgevoerd. De dienstverlener moet een speciaal aan dit onderwerp gewijd team hebben, dat uit meerdere medewerkers bestaat. Alleen op die manier kan een uitwisseling van ervaring en kennis alsmede een kwaliteitsgarantie binnen het team worden gerealiseerd. Bij een eenmansteam moet bovendien worden bedacht dat een onverwachte uitval van de medewerker het project in gevaar kan brengen.

In principe moet de dienstverlener reeds meerdere jaren ervaring hebben op het terrein van webapplicatiebeveiliging. Als de onderneming pas is opgericht of als het thema pas onlangs is opgepakt, dan kunnen er op grond van de ervaring en kwalificaties van individuele medewerkers conclusies worden getrokken over de kwaliteit van de dienstverlener.

Als in de ondernemingsbeschrijving ook verwijzingen staan naar publicaties, lidmaatschappen van vakorganisaties of certificeringen van de onderneming, is dat een pluspunt.

Vanwege de daarmee samenhangende kosten laten veel ondernemingen dit ook met opzet achterwege. Daarom moeten dergelijke activiteiten niet als eis worden gesteld en worden ze in paragraaf 2.2.2 ‘Optionele gegevens, zwakke factoren’ nader uitgelegd.

2.2.1.2 Kwalificaties van de toegewezen projectmedewerkers (projectteam)

Het succes van een project hangt in hoge mate af van de kwalificaties en ervaring van de afzonderlijke projectmedewerkers. Daarom is het van groot belang dat de dienstverlener voor het project die medewerkers beschikbaar kan stellen die het best voldoen aan de eisen die de te testen webapplicatie stelt.

De dienstverlener moet van alle aan het project deelnemende medewerkers een profiel voorleggen, waaruit de bekwaamheid van de medewerkers blijkt. Een dergelijk profiel moet de volgende punten bevatten:

• Opleiding

De beschrijving van de genoten opleidingen dient ertoe een eerste indruk van de medewerker te krijgen. Ze zegt echter nog niets over de geschiktheid van de medewerker voor het project.

• Projectervaring

Deze beschrijving moet de projectervaring in jaren, alsmede het aantal, de duur en het type (broncodeanalyse/penetratietest) van de projecten bevatten. Zij kan ook duidelijk maken of de medewerker reeds in eerdere projecten ervaringen heeft opgedaan die nodig zijn voor het onderzoek van de webapplicatie.

• Specialisatie

Hier moet de dienstverlener ingaan op de bijzondere capaciteiten en kennis van een medewerker, zoals bijvoorbeeld bepaalde technologieën of programmeertalen. Deze informatie geeft – net als de projectervaringen – uitsluitsel of een medewerker voor het project in principe of zelfs in bijzondere mate geschikt is.

• Certificering

De dienstverlener moet hier – voor zover voorhanden – de certificeringen van de medewerker noemen. Hierbij moet worden aangetekend dat bij de auteurs ten tijde van het schrijven van dit paper geen speciale certificeringen met betrekking tot webapplicatiebeveiliging bekend waren.

Naast deelnemende medewerkers moet de dienstverlener nog minstens één extra medewerker kunnen noemen, die bij uitval van een van de aan het project toegewezen medewerkers diens rol kan overnemen.

2.2.1.3 Beschrijving van de methode en aanpak van het project

De beschrijving van de projectspecifieke aanpak en onderzoeksmethodiek van de dienstverlener moet garanderen dat de dienstverlener überhaupt een gestructureerde aanpak heeft, die door de klant te volgen is en kan worden ingepland. Een gestructureerde onderzoeksmethodiek moet ervoor zorgen dat de resultaten van het beveiligingsonderzoek te begrijpen zijn.

Op dit punt moet de dienstverlener uiteenzetten hoe hij zich het verloop van het project voorstelt. Een aanpak van een eenvoudig project kan er bijvoorbeeld aldus uitzien:

• kick-off-bijeenkomst bij de klant;

• documentenanalyse (bij whiteboxtests);

• praktisch webapplicatieonderzoek;

• rapportage opstellen;

• presentatie van de resultaten bij de klant.

Hierbij is het belangrijk dat de dienstverlener de afzonderlijke fasen reeds voorziet van kostenschattingen en concrete mijlpalen. Verder moet per fase zijn bepaald welke informatie van de klant nodig is, en welke resultaten (bijv. eindrapport) de dienstverlener oplevert. Alleen op die manier kan ook de klant de benodigde resources voor het project inplannen en de tijdige uitvoering van het onderzoek bewaken.

Bovendien moet de dienstverlener voor het punt ‘webapplicatieonderzoek’ een precieze methodiek voorstellen, die laat zien hoe de testers bij hun onderzoek te werk zullen gaan. De precieze methodiek zal van dienstverlener tot dienstverlener verschillen. Belangrijk is de analyse door de klant en of de dienstverlener zijn aanpak reeds aan de richtlijnen van de klant heeft aangepast en daardoor reeds in de offertefase een klantgerichte houding kan innemen. Gewoonlijk omvat de aanpak de volgende componenten:

• Geautomatiseerde tests

Met behulp van commerciële, vrij beschikbare of zelf ontwikkelde scantools kunnen websites en webapplicaties geautomatiseerd worden getest. Dergelijke tools kunnen vooral bekende zwakke plekken in bekende applicaties, eenvoudige applicatieproblemen alsmede zwakke plekken in de serversoftware identificeren. Geautomatiseerde tests kunnen reeds in zeer korte tijd ook complexere applicaties afdekken en ten minste een eerste indruk geven over de beveiligingstoestand van een applicatie.

• Handmatige tests

Als een dienstverlener geautomatiseerde scans uitvoert, dan worden de gevonden zwakke plekken vaak ook nog een keer handmatig onderzocht, om valspositieve resultaten te vermijden. Daarnaast kunnen verdere handmatige tests worden uitgevoerd, die gebaseerd zijn op vooraf gedefinieerde en generieke 'testcases' of volledig op de creativiteit van de afzonderlijke testers berusten. Een dienstverlener kan bijvoorbeeld een lijst met generieke testcases (testsuite) bezitten, waaruit de af te werken testcases worden gekozen afhankelijk van de structuur en samenstelling van de applicatie. Hoewel de resultaten bij gebruik van een testsuite ook tussen verschillende testers zeer vergelijkbaar kunnen zijn, hangt de kwaliteit van de resultaten bij creatieve tests zeer sterk af van de kennis en ervaring van de individuele tester.

Het is onmogelijk om louter op grond van de beschrijving van de onderzoeksmethodiek conclusies te trekken over de kwaliteit van de onderzoeksresultaten. Enkele belangrijke punten moeten in ieder geval bij de beoordeling in aanmerking worden genomen. Vanwege de grote complexiteit en eigen aard van de meeste webapplicaties kunnen met geautomatiseerde en generieke tests slechts zeer beperkte resultaten worden verkregen. Alle beveiligingsproblemen die voortkomen uit de individuele programmering van de applicatie of uit problemen met de applicatielogica, kunnen slechts worden geïdentificeerd met behulp van creatieve tests die ingaan op de specifieke applicatie.

Daarom moet een webapplicatietest in ieder geval ook een duidelijke creatieve component bevatten. De basis daarvoor zijn de geautomatiseerde scans en/of van tevoren gedefinieerde testgevallen, die een systematisch onderzoek van de oppervlakkige zwakke plekken met een hoge afdekking mogelijk maken. Als geautomatiseerde scans worden uitgevoerd, dan mag in geen geval een handmatige verificatie van de resultaten ontbreken om valspositieven te elimineren. Aangezien bij de creatieve component vooral de kennis en ervaring van de tester doorslaggevend zijn voor de kwaliteit, moet hier voor de beoordeling van verschillende dienstverleners worden teruggevallen op kenmerken als de kwalificaties en ervaring van de projectmedewerkers, de algemene indruk van de onderneming en referenties van de onderneming tot nu toe.

De beschrijving van zowel de aanpak als de onderzoeksmethodiek moet in de offerte niet alleen generiek worden opgevoerd, maar reeds aan de specifieke klant aangepast zijn. Op grond van de op een bepaald ogenblik te testen applicatie, moet de dienstverlener ook de ingezette gereedschappen en scantools opsommen en kort beschrijven.

2.2.1.4 Beschrijving van de projectresultaten

Voor reparatie en de verdere behandeling van de zwakke punten in de beveiliging is het voor de klant van wezenlijk belang in welke vorm en met welke kwaliteit de resultaten van het beveiligingsonderzoek door de dienstverlener worden vastgelegd. Daarom is het belangrijk dat de klant reeds voorafgaand aan de keus voor een dienstverlener een indruk krijgt van de manier waarop die zijn resultaten beschrijft en beoordeelt.

Met dit doel moet de dienstverlener reeds in zijn offerte een overzicht geven van de indeling van het latere rapport en een beschrijving van zijn beoordelingsmethode meeleveren. De indeling van het rapport moet in ieder geval de volgende componenten bevatten:

• Executive summary

De resultaten en inzichten van het onderzoek moeten op één kantje kort en krachtig zijn samengevat.

• Samenvatting van de zwakke plekken

Op een centrale plaats moet een overzicht van het aantal, de aard en de ernst van de gevonden zwakke plekken staan.

• Inhoudsopgave

Om in een rapport vlot te kunnen navigeren, moet er een inhoudsopgave met paginanummers voorhanden zijn.

• Uitvoerige beschrijving van de zwakke plekken

Om beveiligingsproblemen efficiënt te kunnen verhelpen is een gedetailleerde beschrijving van de zwakke plekken nodig. Deze moet een korte omschrijving bevatten, en verder de gevolgen van de zwakke plek, een risicoschatting, referenties en zo nodig de precieze handelwijze voor misbruik van de zwakke plek beschrijven. Dit is noodzakelijk, zodat een aanval door de klant of een applicatieontwikkelaar kan worden getraceerd en gereproduceerd.

Om een nauwkeurig beeld van het daadwerkelijke rapport te krijgen, zou de dienstverlener idealiter een voorbeeldrapport beschikbaar moeten stellen. Voor de beoordeling van een dergelijk voorbeeldrapport is het belangrijk dat de gedetailleerde beschrijving en beoordeling (bijv. hoogte van de schade en misbruikbaarheid) van de beveiligingsproblemen specifiek aan het inzetscenario van de klant zijn aangepast en niet slechts toolgegeneerde resultaten of generieke beoordelingen bevatten. Een zwakke plek kan bijvoorbeeld als minder kritiek worden ingeschaald, als die uitsluitend door zeer weinig en te vertrouwen gebruikers kan worden benut. Veel kritieker is een zwakke plek als die voor anonieme gebruikers van het gehele internet toegankelijk is.

De dienstverlener moet bovendien uiteenzetten volgens welke methode of classificatie hij de gevonden zwakke plekken beoordeelt. Hierbij passen dienstverleners vaak zeer granulaire en gedetailleerde beoordelingen toe op willekeurige schalen (bijv. 3, 10 of 100). Hierbij moet in ieder geval in het oog worden gehouden dat een webapplicatietest een risicoanalyse niet kan vervangen. Voor een risicoanalyse zijn gedetailleerde gegevens van klanten nodig, om nauwkeurige inschattingen te kunnen maken van de waarschijnlijkheid en de hoogte van de schade door zwakke plekken. Deze informatie is vaak bij een beveiligingsonderzoek niet beschikbaar. Het is weliswaar belangrijk duidelijke randvoorwaarden van de klant (bijv. zeer beperkte toegang tot onveilige functionaliteit) bij de inschatting aan te stippen, maar een tester van een webapplicatie kan zonder gedetailleerde kennis van het inzetscenario en de processamenhangen in de regel geen onderscheid maken tussen een toegangswaarschijnlijkheid van 6 of 7 (op een schaal van 10). Het is daarom zinvoller grovere indelingen in beveiligingsniveaus te gebruiken zoals ‘hoog’, ‘gemiddeld’, ‘gering’ of ‘informatief’.

2.2.1.5 Samenstelling van de prijs

In de offerte moet de dienstverlener zijn prijs in precieze werkpakketten opdelen. Alleen op die manier wordt het voor de klant inzichtelijk hoe de prijs van het beveiligingsonderzoek is samengesteld en hoe de zwaartepunten in de werkzaamheden bij de verschillende dienstverleners ongeveer geprijsd zijn.

2.2.2 Optionele gegevens, zwakke factoren

Naast de vereiste gegevens over de onderneming, de kwalificaties van de projectmedewerkers en de aanpak van het project, zijn ook andere, optionele gegevens interessant voor een besluit over de geschiktheid van een dienstverlener. Daartoe behoren bijvoorbeeld de referenties of referentieprojecten van de dienstverlener, zijn publicaties of zijn lidmaatschap van erkende organisaties.

2.2.2.1 Referenties/referentieprojecten

Referenties en/of referentieprojecten kunnen een aanwijzing zijn dat andere klanten tevreden waren over de dienstverlener. De klant mag zich echter niet verlaten op een eenvoudige opsomming van referenties of de 'grote namen' onder de referenties. Alleen persoonlijke navraag bij de referenties over hun tevredenheid ten aanzien van de projectresultaten, de aanpak of ook de bekwaamheid van de medewerkers, kan doorslaggevende argumenten voor of tegen een dienstverlener leveren. De klant moet echter ook begrijpen dat de dienstverlener in veel gevallen op grond van geheimhouding of discretie geen referenties mag of kan noemen. Daarbij kan het bijvoorbeeld gaan om organisaties die in een gevoelige omgeving opereren (overheid, leger, financiële instellingen).

2.2.2.2 Publicaties

Als de dienstverlener kan wijzen op publicaties, bijvoorbeeld vakmatige artikelen of security-advisories, of ook voordrachten op bekende beveiligingscongressen, moeten deze ook met een korte beschrijvingen worden aangegeven. De klant heeft zo de mogelijkheid om erachter te komen met welke onderwerpen de dienstverlener zich bezighoudt, en kan zo diens geschiktheid voor het project beter beoordelen.

2.2.2.3 Lidmaatschappen

De lidmaatschappen van de dienstverlener van voor IT-beveiliging relevante organisaties moeten worden genoemd. Daarbij moet de dienstverlener in ieder geval aangeven of het om een passief of actief lidmaatschap gaat. Een actief lidmaatschap kan duiden op een erkenning van de expertise van de dienstverlener en zijn voortrekkersrol in het betreffende domein.

2.2.2.4 Certificeringen van de onderneming

De dienstverlener moet relevante certificeringen (bijv. *ISO/IEC 27001* of *ISO 9001*) van zijn onderneming opgeven. Deze kunnen betekenen dat hij een gedocumenteerde, methodische aanpak gebruikt.

2.2.2.5 Omgang met data

Er moet worden gegarandeerd dat de uitwisseling en opslag van documenten die potentieel gevoelige informatie bevatten (bijv. broncode, interne documenten van de klant, resultaten van het beveiligingsonderzoek), versleuteld plaatsvinden. De dienstverlener moet daarom aangeven over welke mogelijkheden van veilige communicatie, overdracht en opslag hij beschikt. De klant moet nagaan of de aangeboden oplossingen compatibel zijn met de zijne respectievelijk door hem kunnen worden gebruikt.

2.2.2.6 Aanwezigheid van een aansprakelijkheidsverzekering

De dienstverlener moet aangeven of er een aansprakelijkheidsverzekering voorhanden is en voor welke hoogte deze is afgesloten. Dat geldt in het bijzonder voor projecten waarbij schadeclaims kunnen ontstaan. Dit kan bijvoorbeeld het geval zijn bij het onderzoeken van productieve applicaties waarvan uitval of een foutieve behandeling van data op grond van nalatigheid van de penetratietester kosten met zich mee kan brengen. Dergelijke kosten moeten door een passende aansprakelijkheidsverzekering gedekt zijn.

A Bijlagen

A.1 Literatuur

http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf
BSI Bundesamts für Sicherheit in der Informationstechnik: *Durchführungskozept für Penetrationstests*

http://www.gshb.bund.de
BSI: *IT-Grundschutz Handbuch*

http://www.osstmm.org/
ISECOM: *Open Source Security Testing Methodology Manual*

http://www.owasp.org/index.php/Category:OWASP_Testing_Project
OWASP: *Testing Guide*

http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
OWASP: *Application Security Verification Standard*

http://www.owasp.org/index.php/Category:Attack
OWASP Category:Attack

http://www.owasp.org/index.php/Category:Threat
OWASP Category:Threat

http://www.owasp.org/index.php/Category:Vulnerability
OWASP Category:Vulnerability

http://projects.webappsec.org/Threat-Classification-Reference-Grid
WASC Web Application Security Consortium: WASC Threat Classification

http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.de.pdf
WASTC Web Application Security Consortium: Web Security Threat Classification

http://www.gesetze-im-internet.de/s_g/index.html
Wet over de eisen en procedures voor beveiligingstests van de Bondsregering

A.2 Checklist: Eisen van de zijde van de klant

	Eis	Opmerking /
Aard van de test		
O	Vulnerability-Assessment (VA) / penetratietest van webapplicatie Blackbox, whitebox, Denial-of-Service	
O	Broncodeanalyse Geautomatiseerd/handmatig onderzoek	
O	Architectuuranalyse Toegepaste serverdiensten, netwerkverbindingen, dataversleuteling, uitvalbeveiliging	
O	Proces- en documentatieanalyse ISMS, reglementen, richtlijnen/guidelines	
Doelformulering en omgevingsbeschrijving		
O	Definitie van de testdoelen Soort test, worstcasescenario's	
O	Beschrijving van de omgeving Overzicht van de webapplicatie, toegangswegen, logica, rollenconcept, omvang en structuur, manier van functioneren, architectuur, datastroom	
Organisatorische aspecten		
O	Projectidee en projectinitiatie Probleemstelling, eis, zin, nut	
O	Doeldefinitie en projectbeschrijving Uitgangssituatie, doelen en mijlpalen, randvoorwaarden en afbakening, deelnemers, projectsturing en feedback, plaats en tijd, scanvrijgaven, vertrouwelijkheidsverklaring, veiligheidstests van personen, aansprakelijkheid	
O	Projectaanbesteding Informatie over de offerte-uitwerking, globaal technisch overzicht	
O	Diensterverlenersselectie en projectgunning Proces, tijdskader, communicatie	
O	Project-kick-off Technische details (URL's, IP-adressen, hostnamen, netwerkschema's, datastroomschema's, testsystemen/productieve systemen), aanpak	
O	Projectuitvoering Betrokken medewerkers, rechten, afstemming, aanvalsvectoren	
O	Projectafsluiting Rapport, presentatie	

O	Projectevaluatie Afstemming beoordeling zwakke plekken en tegenmaatregelen, verantwoordelijkheden	

A.3 Checklist: Eisen aan de dienstverlenersofferte

	Eis	Opmerking / commentaar
Noodzakelijke gegevens		
O	Ondernemingsgeschiedenis – leeftijd, specialisatie Ontstaan, dienstverleningsportfolio, ervaring, specialisatie in webapplicatiebeveiliging	
O	Kwalificaties van de toegewezen projectmedewerkers (projectteam) Opleiding, projectervaring, specialisatie, certificering, mogelijkheid van vervanging projectmedewerkers	
O	Beschrijving van de methode en aanpak van het project Verloop van het project, beschrijving van de projectfasen, methodiek van het onderzoek (geautomatiseerde/handmatige test, creatieve componenten)	
O	Beschrijving van de projectresultaten Voorbeeldrapport, classificatie van de zwakke plekken	
O	Samenstelling van de prijs Indeling in werkpakketten, transparantie	
Optionele gegevens, zwakke factoren		
O	Referenties/referentieprojecten Projectomvang, soort project, navraag doen bij referenties	
O	Publicaties Vakmatig artikel, voordracht, beschrijving van de inhoud	
O	Lidmaatschappen Actief/passief lidmaatschap, rol, taken	
O	Certificeringen van de onderneming Aard en omvang van de certificering, geldigheid	
O	Omgang met data Versleuteling (overdracht, opslag)	
O	Aanwezigheid van een aansprakelijkheidsverzekering Verzekerd bedrag, dekking	