Versie 1.0
26-5-2014

Gemeente Amsterdam
Dienst ICT

CIO office

Richtsnoer beveiliging webapplicaties gemeente Amsterdam

Beleidskader en methodiek voor het beoordelen van de beveiliging van nieuwe en bestaande webapplicaties

Inhoud

De belangrijkste beleidsregels voor beveiliging van webapplicaties samengevat

1) Elke webapplicatie heeft een eigenaar die zorgt voor continue aandacht, van bouw tot beëindiging, voor de informatiebeveiliging.

2) Bij de start van de ontwikkeling van een nieuwe webapplicatie vindt eerst een intakegesprek plaats met Concern Communicatie, Dienst Facilitair Management (dienstverlening) en het CIO-office. U ontvangt dan advies over alle actuele regels en hoe deze toe te passen.

3) Volg voor de hosting van webapplicaties de afspraken vanuit de Amsterdamse raamcontracten.

4) U bent verplicht om voorafgaand aan de bouw van een webapplicatie eerst een risicoanalyse uit te (laten) voeren, zodat direct de juist beveiligingsmaatregelen worden afgewogen.

5) Het richtsnoer beveiliging webapplicaties is uitgangspunt bij het sluiten van contracten met derden.

6) Amsterdam volgt voor de beveiliging van webapplicaties de (intern-) nationale open standaarden ISO27001/2 en OWASP. OWASP staat voor Open Web Application Security Project.

7) Een nieuwe webapplicatie kan pas in productie gaan, nadat via een onafhankelijke hack en penetratietest is aangetoond dat dit verantwoord kan gebeuren.

8) Toezicht: Voor operationele webapplicaties die vanaf Internet benaderbaar zijn geldt dat de CISO/CIO-office jaarlijks een kwetsbaarheidsonderzoek uitvoert. Indien de beveiliging niet op orde is krijgt de eigenaar van de webapplicatie de aanwijzing tot het treffen van maatregelen.

Inleiding

De maatschappij is vandaag de dag niet meer denkbaar zonder het gebruik van internet en webapplicaties. Amsterdam biedt als publieke organisatie haar diensten aan over internet en is zelf afhankelijk van internet voor haar dienstverlening en bedrijfsvoering.
Een verstoring op Internet of het niet beschikbaar zijn van een webapplicatie kan betekenen dat paspoorten niet meer kunnen worden uitgereikt, parkeerautomaten niet meer werken, betaalverkeer niet meer functioneert, ketenpartners niet meer kunnen worden voorzien van informatie, welke noodzakelijk is om een goede dienstverlening aan de burger en het bedrijfsleven te garanderen. Het hacken van systemen waarop gegevens van burgers, ambtenaren of werkgevers staan geregistreerd of de manipulatie van deze gegevens, kan rampzalige gevolgen hebben voor het individu en voor het vertrouwen in de Overheid en de gemeente Amsterdam in het bijzonder.

Amsterdam is in tegenstelling tot de meeste gemeenten zeer rijk aan webapplicaties. De Amsterdamse gemeentelijke externe webapplicaties, gericht op burger, ambtenaar, toerist en ondernemer, bestaan uit ongeveer 300 verschillende web applicaties die bij verschillende organisaties worden gehost en door vele partijen zijn ontworpen en worden beheerd.

Naar aanleiding van “lektober” 2011, waarbij aangetoond werd dat vele webapplicaties bij de Overheid makkelijk gehackt konden worden en de daaruit voortvloeiende publiciteit, is de Overheid gestart met het ontwerpen van richtlijnen voor de beveiliging van web applicaties . Zo heeft het Nationaal Cyber Security Centrum (NCSC)[1] in 2012 een tweedelige richtlijn voor de beveiliging van web applicaties gepubliceerd, heeft Logius beveiligingsrichtlijnen voor webapplicaties[2] gepubliceerd die gebruik maken van de DIGID koppelingen. King heeft in opdracht van het ministerie van Binnenlandse Zaken een baseline informatiebeveiliging Gemeenten[3] opgesteld.

---

[1] https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[2] http://www.logius.nl/fileadmin/logius/product/digid/documenten/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf

[3] https://new.kinggemeenten.nl/informatiebeveiliging/downloads-informatiebeveiligingsdienst

Deze frameworks zijn echter dusdanig uitgebreid en alles omvattend dat deze niet geschikt zijn als toetsingskader voor de Amsterdamse webapplicaties die veelal extern worden gehost en door derden zijn ontwikkeld en worden beheerd.

Amsterdam kent van oudsher de GIBN (2005) en de Baseline Informatiebeveiliging als nadere uitwerking van de GIBN (2009). De GIBN is inmiddels een gedateerd organisatorisch framework dat vooral de inrichting van de beveiliging beschrijft[4]. De Baseline is een nadere uitwerking hiervan maar als zodanig niet volledig toepasbaar als beleid voor de beveiliging van webapplicaties, vandaar dat is gezocht naar een hanteerbare variant..

In dit richtsnoer dat deel uitmaakt van de BIG (Baseline Informatiebeveiliging Gemeenten) zal nader worden ingegaan op hoe zowel nieuwe en bestaande webapplicaties moeten worden beveiligd en hoe het beveiligingsproces van ontwikkeling tot beheer dient te worden ingericht. Op hoofdlijnen zal worden aangegeven waar rekening mee moet worden gehouden. Deze notitie beschrijft daarmee het beveiligings- en toetsingskader voor alle Amsterdamse webapplicaties.

Gezien de zich razend snel ontwikkelende techniek wordt niet ingegaan op specifieke kwetsbaarheden. De focus ligt op het moeten voldoen aan een aantal basale beveiligingsrichtlijnen van alle Amsterdamse webapplicaties en achterliggende infrastructuren.

[4] een herziening is vanaf Q3 2013 beschikbaar.

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.2	Juli 2013	J. de Munnik	
0.3	Juli 2013	A. van der Valk	Verwerking opmerkingen CPIB en CIO-office
0.4	Mei 2014	J. de Munnik	Verwerking opmerkingen Kernteam, Dir Comunicatie en CIM

Reviews

Versie	Datum	Review door
0.2	Juli 2013	CPIB en CISO
0.3	November 2013	CIO-office beleidsteam

Goedkeuring

Versie	Datum	Naam
1.0	November 2013	CIO-office,beleidsteam
1.0	April 2014	Kernteam DICT
	Mei 2014	CIM
	Mei 2014	AT

Distributie

Directies, Clusters, Stadsdelen, Intranet, CPIB, Informatiebeveiliging coördinatoren, Leveranciersmanagement DICT, Communicatie, AT

1 Webapplicaties

1.1 Webapplicaties in Amsterdam

Amsterdam is als een van de eerste gemeenten in de jaren tachtig van de vorige eeuw gestart met het ontwikkelen en beschikbaar stellen van webapplicaties. Inmiddels voert de gemeente, deels samen met ketenpartners, ca 300 webapplicaties die vanaf internet te benaderen zijn. Deze zijn gericht op de burger, het bedrijfsleven, de toerist, de expat, de reiziger, de ambtenaar, etc. De gemeentelijke website www.amsterdam.nl, is het primaire communicatie – en dienstverleningskanaal richting de burger.

Al deze webapplicaties zijn ontwikkeld door verschillende partijen; op verschillende tijdstippen; draaien op verschillende technieken; worden beheerd door verschillende partijen en worden in de praktijk gehost in verschillende landen. Aan Amsterdam gelieerde webapplicaties worden naast in Nederland onder meer gehost in de VS, Groot Brittannië en Duitsland. Er bestaat nu kortom een grote mate van versnippering, waardoor er geen sprake is van een eenduidige beveiliging van bestaande webapplicaties.

In deze beleidsnotitie staan de beveiligingskaders aangegeven waarmee Amsterdam webapplicaties kan inkopen, laten ontwikkelen en kan controleren of deze webapplicaties ook veilig worden beheerd en gehost.

1.2 Wat zijn webapplicaties?

Webapplicaties zijn applicaties welke via het internet ter beschikking worden gesteld via een webbrowser of een ander programma dat gebruik maakt van het http protocol of de versleutelde variant https. De functionaliteit die kan worden geboden is onbeperkt.
Ook de bijbehorende infrastructuur, opslag van gegevens, en de netwerkservices worden beschouwd als onderdeel van dergelijke applicaties uit het oogpunt van beveiliging en zijn met webapplicaties onlosmakelijk verbonden.

Webapplicaties zijn globaal te verdelen in:

- Internetsites, Voor iedereen toegankelijke websites zoals www.amsterdam.nl, www.ggd.amsterdam.nl etc.

- Extranetten, Afgeschermde websites die vanaf iedere plek te raadplagen zijn maar alleen voor geauthoriseerde gebruikers toegankelijk zijn. Meestal afgeschermd d.m.v. een inlog zoals bijvoorbeeld http://www.contractorportal.ca

- Intranetten Websites die alleen toegankelijk zijn binnen een bedrijfsnetwerk en niet vanaf andere plekken kunnen worden geraadpleegd zoals http://intranet.dictinsite.amsterdam.nl ;

- Webservices, stukjes online software waarmee een bepaalde taak uitgevoerd wordt, bijvoorbeeld het boeken van een vlucht of het live tonen van vrije plekken in een parkeergarage. Deze webservices worden meestal getoond op een website en hebben vaak koppelingen met andere (backoffice)systemen. Voorbeeld; het boeken van een vlucht op klm.com

- Apps, applicaties die speciaal gemaakt zijn voor een smartphone of tablet en beschikbaar zijn via een appstore:

- SAAS software die als een onlinedienst wordt aangeboden.
  De klant hoeft de software niet aan te schaffen en hoeft deze niet te installeren maar kan deze via internet benaderen.
  Bijvoorbeeld http://www.sgfacilitor.nl/services/saas/ :

Kortom, alle programma's die kunnen worden benaderd met een browser zijn feitelijk webapplicaties.

1.3 Waarom webapplicaties beveiligen?

Amsterdam is voor de dienstverlening en bedrijfsvoering volledig afhankelijk geworden van Internet en webapplicaties en deze afhankelijkheid zal alleen maar toenemen..

Bijvoorbeeld: via de webapplicatie Paraplu worden de gegevens van de burger opgehaald en gemuteerd in het GBA. Voor de uitwisseling van gegevens met ketenpartners in het sociaal domein wordt onder meer gebruik gemaakt van JN12+ en Matchpoint. Voor het verlenen van uitkeringen wordt door DWI gebruik gemaakt van de applicatie Socrates die via WIGO4IT ter beschikking wordt gesteld via beveiligde verbindingen.

Uitlekken van vertrouwelijke informatie, het onbeschikbaar zijn van informatie of de verstrekking van foutieve informatie kan grote gevolgen hebben voor de gemeente Amsterdam en haar burgers. Ook het opzettelijk verstrekken van foutieve informatie of het moedwillig verspreiden van schadelijke software door middel van een gehackte webapplicatie of account kan desastreuze gevolgen hebben, zoals uit onderstaande twee recente voorbeelden blijkt:

"Het account van persbureau Associated Press (AP) is op 23 april 2013 korte tijd gehackt geweest. In die tijd verstuurde het account een tweet waarin gemeld werd dat de Amerikaanse president gewond zou zijn geraakt na twee explosies in het Witte Huis. Het account werd kort daarna uit de lucht gehaald. AP gaf vrijwel direct aan dat de melding op Twitter onjuist was.
De woordvoerder van het Witte Huis, Jay Carney, liet aan Reuters weten dat president Obama niets is overkomen.

Het valse bericht zorgde dinsdag even voor paniek op Wall Street. De Amerikaanse aandelenbeurzen zakten sterk in, maar veerden al heel snel weer op, toen AP bekendmaakte dat het om een hackersaanval ging".

Schade: Beurs kelderde met ruim honderd punten, honderden miljoenen verlies in enkele uren tijd

"'Gehackt' medisch centrum eist 85.000 euro schadevergoeding
De claim van 85.000 euro is uit diverse componenten opgebouwd en bestaat alleen uit materiële schade, zegt de advocaat. Een audit die door een extern bedrijf moest worden uitgevoerd nadat de zaak aan het licht kwam, koste 23.500 euro. De GGZ-E (Eindhoven) claimt een schade van 10.500 euro. Verder bestaat de schade uit intern gemaakte uren aan probleemoplossing, externe communicatie en dergelijke"

1.4 Eigenaarschap webapplicaties en verantwoordelijkheden

Soms is nu niet eenduidig afgesproken wie de feitelijke eigenaar is van een web applicatie. Webapplicaties worden bijvoorbeeld vaak vanuit een actuele communicatiebehoefte ontwikkeld, zonder dat de verantwoordelijkheden voor het continue beheer en de informatiebeveiliging worden vastgelegd. Vaak worden ook geen eenduidige afspraken gemaakt met de leveranciers van de oplossingen omtrent beveiliging en onderhoud.

1.4.1 De eigenaar

Een vereiste is dat elke webapplicatie een eigenaar heeft binnen de gemeente (ook al wordt de applicatie beheert of gemaakt door een partij buiten de gemeente) heeft die verantwoordelijk is voor:

- het voldoen van de webapplicatie aan de interne- en externe wet- en regelgeving, waaronder ook de baseline beveiliging voor webapplicaties;
- het organiseren van de incidenteel – en structureel benodigde middelen (financieel, menskracht), om het hele life-cycle-management (van ontwikkelen tot afvoeren) van een webapplicatie adequaat uit te laten voeren. In het kader van de informatiebeveiliging is m.n. het zorgdragen voor adequaat beheer (o.m. tijdig aanbrengen van beveiligingspatches, het organiseren van toezicht, onderhoud i.v.m. nieuwe wetgeving, etc.) een voortdurend aandachtspunt.
- Het maken van afspraken met de leverancier van de webapplicatie en de hostende partijen over o.m.: het gewenste beveiligingsniveau, het patchmanagement, het vastleggen van het auditrecht van Amsterdam, de plek waar de data wordt opgeslagen, hoe om te gaan met datalekken en de wijze waarop de leverancier onder meer controle en toezicht heeft ingeregeld.
  In de SLA of het contract dienen de gemaakte afspraken met de leverancier te worden vastgelegd. Indien er persoonsgegevens worden verwerkt, dient tevens een bewerkersovereenkomst met de leverancier te worden gesloten;
- Elke webapplicatie dient bij initiële oplevering een penetratie- en hacktest te ondergaan, waarbij de "veiligheid" onafhankelijk wordt vastgesteld. Op aanwijzing van het CIO-office/de CISO en/of de eigenaar van de

webapplicatie kan periodieke herhaling van deze test worden opgelegd.

1.4.2 Een nieuwe webapplicatie: eerst een intakegesprek.

De eerste stap is dat elke webapplicatie voordat deze wordt ontwikkeld of aangeschaft voor een intakegesprek wordt voorgelegd aan een delegatie van: Dienstverlening/DFM, Concern Communicatie en het CIO-office. In dat gesprek wordt uitleg en toelichting gegeven op alle verantwoordelijkheden, het toezicht en de regelgeving en krijgt u advies over de aanpak. Natuurlijk zal het intakegesprek bij een eenvoudige webapplicatie anders verlopen, dan bij een nieuwe zware webapplicatie waarin met vertrouwelijke gegevens wordt gewerkt. Als er sprake is van verwerking van persoonsgegevens dan dient de vraag “mag het eigenlijk?” in verband met de Wet Bescherming Persoonsgegevens aan de Commissie Persoonsgegevens Amsterdam (CPA) te worden voorgelegd en dient een privacy impact assessment te worden uitgevoerd.

1.4.3 Rol Directie Concern Communicatie

De Directie Concern Communicatie toets bij webapplicaties onder meer op:

- past de webapplicatie binnen het gemeentelijke communicatiebeleid en – afspraken.
- het voldoen aan de huistijlsafspraken binnen de gemeente (stijl van Amsterdam), zoals merk, vormgeving en geldige “url-naam”;
- de verkenning om webapplicatie onder te brengen in het stedelijke content management systeem IPROX;
- regelgeving rondom social media;

1.4.4 Rol CIO-office/CISO

De CISO (Chief Information Security Officer) ziet toe op:

- een adequaat en actueel gemeentelijk beleid rondom webapplicaties;
- het voldoen van webapplicaties aan landelijke en lokale wet – en regelgeving, zoals de cookiewet, voorliggende webrichtlijnen en het voldoen aan de richtlijnen t.a.v. PKI-overheidscertificaten voor web applicaties die door de burger benaderbaar zijn vanaf Internet;
- ingeval van verwerking van persoonsgegevens: het adviseren rondom een risicoanalyse en een bewerkersovereenkomst conform de WBP (afspraken over beveiliging, de data en periodieke toetsing. Hiertoe heeft het CBP in 2013 de CBP richtsnoeren beveiliging van persoonsgegevens[5] uitgebracht. Indien van toepassing zal het proces rondom de CPA worden toegelicht;
- een jaarlijkse toetsing op kwetsbaarheid van alle Amsterdamse webapplicaties, waarover gerapporteerd wordt aan de CIO en waarna de eigenaar van een webapplicatie verplichtende veiligheidsaanwijzingen gegeven kunnen worden.

[5] http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

1.4.5 Rol DFM/ dienstverlening

- afstemming van de centrale verantwoordelijkheid voor de dienstverlening aan de burger met de doelstellingen en effecten van een nieuwe webapplicatie;
- zorg dragen voor een voor de burger zo eenduidig mogelijk “gezicht” van Amsterdam qua dienstverlening.

1.4.6 Hosting

In de meeste gevallen zal een webapplicatie technisch niet door de gemeente Amsterdam worden beheerd. Qua hosting zijn daartoe met diverse mantelpartijen bindende afspraken gemaakt op concernniveau. Indien wordt besloten om de hosting uit te besteden dient gebruik te worden gemaakt van de diensten van door de gemeente Amsterdam geselecteerde leveranciers. Zie hiertoe ook Intranetsites van Concern Inkoop en dienst ICT.

1.4.7 Risicoanalyse vooraf

De eigenaar van een webapplicatie is verplicht om bestaande en nieuwe webapplicaties te laten classificeren naar beveiligingsrisico’s op basis van een risicoanalyse. Dit om de juiste beveiligingsmaatregelen al bij de bouw van de webapplicatie te kunnen laten treffen: “security & privacy by design”.

1.4.8 De verantwoordelijkheden van ontwikkelaars en hostende partijen

Een leverancier moet objectief (kunnen) aantonen dat de dienstverlening voldoet aan het met de verantwoordelijke van de webapplicatie gewenste en afgesproken beveiligingsniveau.

De leverancier is verantwoordelijk om de door hem aangeboden producten tijdens de ontwikkeling te checken op mogelijke beveiligingsissues en de opdrachtgever te adviseren over de eventueel te nemen maatregelen om beveiligingslekken te dichten. Hierbij dient de leverancier actief de kwetsbaarheden te volgen die gepubliceerd[6] worden en de nodige acties te ondernemen

Tevens dient de leverancier een bewerkersovereenkomst te tekenen en dient in een contract het auditrecht te zijn afgesproken. Leveranciers dienen qua beveiliging minimaal te voldoen aan de ISO 27001/27002 norm en de webapplicaties te beveiligen conform de OWASP criteria (minimaal de top 10). OWASP staat voor Open Web Application Security Project.

[6] http://www.cvedetails.com/

http://cve.mitre.org/

1.4.9 (Inter-) nationale beveiligingsstandaarden

Amsterdam hanteert voor haar webapplicaties de (inter-)nationale beveiligings-standaarden: ISO 27001/2 en de OWASP-criteria[7]. Beide standaarden zijn *de facto* de wereldwijde (open) standaard voor de beveiliging van webapplicaties en worden gebruikt en erkent door alle professionele leveranciers van Amsterdam.

1.4.10 Hack en pen testen

Amsterdam onderhoudt vele webapplicaties, al dan niet in regionale of specifieke (keten-) samenwerkingsverbanden, waarop enerzijds informatie wordt geboden aan de burger, werkgever, ambtenaren en anderzijds informatie van die personen, ambtenaren en werkgevers wordt opgeslagen en verwerkt in achterliggende systemen van de gemeente Amsterdam. Zie bijlage 1 voor een toelichting.

Initieel en bij elke majeure wijziging van een webapplicatie dient via een hack – en penetratietest te worden aangetoond dat het veilig en verantwoord is om een webapplicatie in productie te nemen. Tussentijds dient via adequaat beheer de veiligheid op een verantwoord niveau te worden gehouden, onder meer door tijdig veiligheidspatches aan te brengen en verouderde software tijdig te vervangen.

Is het niet mogelijk om een bestaande webapplicatie afdoende te beveiligen dan zal de eigenaar direct de CISO moeten informeren en moeten besluiten om de webapplicatie up te graden naar een nieuw veilig platform of om deze uit de “lucht te halen”.
Na een upgrade dient door middel van een verkorte pen- en hacktest te worden aangetoond dat de omissies zijn verholpen. De rapportages dienen te worden overlegd aan de CISO.

Een middel dat kan worden gebruikt om webapplicaties te classificeren om mogelijk te beveiligingsrisico’s te kunnen onderkennen en risico beperkende maatregelen te nemen is een risicoanalyse op basis van de richtlijnen van het Open Web Application Security Project (OWASP)[8].

Met behulp van de risico analyse kan worden vastgesteld welke mogelijke kwetsbaarheden elementen van een applicatie moeten worden getoetst om vast te kunnen stellen in hoeverre een webapplicatie bestendig is tegen al dan niet geautomatiseerde aanvallen en in hoeverre de juiste maatregelen zijn getroffen om eventuele aanvallen afdoende te kunnen afslaan. Hiervoor is door OWASP een model ontwikkeld waarbij vier webapplicatie beveiligingsniveaus zijn benoemd. Zie ook bijlage 1.

[7] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

[8] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

De CISO houdt toezicht via een jaarlijkse toetsing op kwetsbaarheid van alle Amsterdamse webapplicaties, waarna de eigenaar van een webapplicatie verplichtende aanwijzingen gegeven kunnen worden.

1.4.11 Toezicht

De CISO laat jaarlijks alle operationele webapplicaties onderzoeken op kwetsbaarheden. Hierover wordt gerapporteerd aan de CIO.
Indien daar aanleiding toe is krijgen eigenaren van webapplicaties verplichtende aanwijzingen tot het treffen van adequate beveiligingsmaatregelen.

1.5 Resumé

Het aanbieden van onveilige webapplicaties is voor Amsterdam nooit een optie.

Deze notitie geeft daartoe de belangrijkste maatregelen die getroffen moeten worden en geeft aan hoe daarop toezicht wordt gehouden.

1) Elke webapplicatie heeft een eigenaar die zorgt voor continue aandacht, van bouw tot beëindiging, voor de informatiebeveiliging (zie 1.4.1).

2) Bij de start van de ontwikkeling van een nieuwe webapplicatie vindt eerst een intakegesprek plaats met Concern Communicatie, Dienst Facilitair Management (dienstverlening) en het CIO-office. U ontvangt dan advies over alle actuele regels en hoe deze toe te passen. Zie 1.4.2 t/m 1.4.5.

3) Volg voor de hosting van webapplicaties de afspraken vanuit de Amsterdamse raamcontracten (zie 1.4.6). Zie ook Intranetsites van Concern Inkoop en dienst ICT.

4) U bent verplicht om voorafgaand aan de bouw eerst een risicoanalyse uit te (laten) voeren, zodat direct de juiste beveiligingsmaatregelen worden afgewogen (1.4.7).

5) Het richtsnoer beveiliging webapplicaties is uitgangspunt bij het sluiten van contracten met derden. (1.4.8).

6) Amsterdam volgt voor de beveiliging van webapplicaties de (intern-) nationale open standaarden ISO27001/2 en OWASP (1.4.9).

7) Een nieuwe webapplicatie kan pas in productie gaan, nadat via een onafhankelijke hack- en pentest is aangetoond dat dit verantwoord kan gebeuren(1.4.10).

8) Toezicht: voor operationele webapplicaties geldt dat de CISO/CIO-office jaarlijks een kwetsbaarheidsonderzoek uitvoert. Bij geconstateerde gebreken krijgt de eigenaar aanwijzing voor het treffen van maatregelen (1.4.11).

Voor nadere vragen / toelichting kunt u altijd contact opnemen met de CISO / het CIO-office (zie contactgegevens op Intranet).

Bijlage 1 Toelichting op de pen- en hacktest

Voor het uitvoeren van een initiële en een vervolg pen- en hacktest dient gebruik te worden gemaakt van gespecialiseerde bedrijven, die medewerkers kunnen inzetten die voldoende ervaring hebben en gecertificeerd zijn. Tevens dienen de medewerkers in het bezit te zijn van een verklaring omtrent gedrag en dient een geheimhoudingsverklaring te worden overlegd.

Voordat gestart wordt met de pen- en hacktest dient door Amsterdam een vrijwaringsverklaring aan de testende partij te worden overhandigd en dienen afspraken te worden gemaakt over de soort test en het moment waarop deze zal plaatsvinden. Ook dient de hostende partij schriftelijk van te voren te worden ingelicht over het moment van test en de IP-reeks waar vanaf de test zal gaan plaatsvinden.

Het framework dat voor de test van de webapplicaties moet worden gehanteerd is OWASP en de test moet bij voorkeur worden uitgevoerd in de vorm van een “whitebox” test waarbij de testers vooraf worden voorzien van netwerk tekeningen, technisch ontwerp en de meest recente technische documentatie. De test mag in de productie nooit schadelijk zijn en een webapplicatie onbereikbaar maken zoals met gerichte DDOS attack, waarbij dusdanig verkeer wordt genereerd dat de webapplicatie het verkeer niet meer aan kan. Tevens dient de hostende partij van te voren te worden ingelicht over de test en van welk IP adres deze test zal gaan plaatsvinden.

1.5.1 Rapportage pen- en hacktest

De rapportage dient bij voorkeur te bestaan uit de volgende onderdelen;

- Management samenvatting
- Inleiding
    - Opdrachtomschrijving
    - Scope en doelstelling
    - Auditomgeving en objecten
    - Gebruikte methoden en technieken
    - Risico niveaus
- Bevindingen
    - Oorzaak van de bevinding
    - Risico beschrijving incl. risicomatrix zie afbeelding
    - Bewijs
    - Aanbeveling
- Conclusies en aanbevelingen

Risico matrix per bevinding:

		Gevolgen		
		Laag	**Gemiddeld**	**Hoog**
Waarschijnlijkheid van optreden	**Laag**	LAAG	LAAG	GEMIDDELD
	Gemiddeld	**LAAG**	**GEMIDDELD**	**HOOG**
	Hoog	**GEMIDDELD**	**HOOG**	**ZEER HOOG**

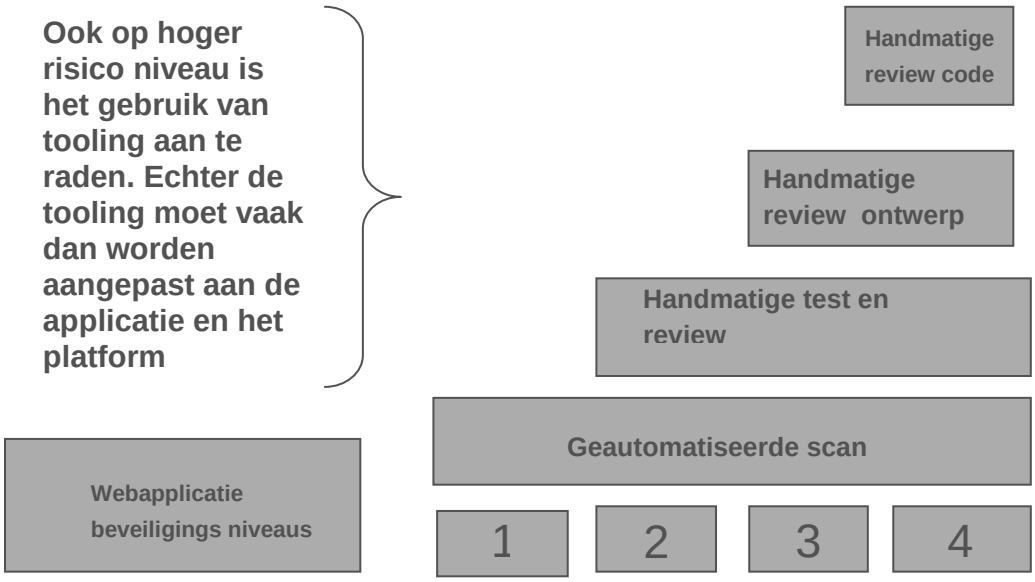
Tevens dient de partij die de pen- en hacktest heeft uitgevoerd de loggegevens van de test ter beschikking te stellen aan de opdrachtgever van de test zodat altijd achteraf kan worden geconstateerd of de aangetroffen kwetsbaarheden te repliceren zijn.

Indien blijkt dat er kwetsbaarheden zijn aangetroffen dient er na het verhelpen van de bevindingen altijd door een hertest te worden aangetoond dat de kwetsbaarheden niet langer bestaan.

De rapportage van de pentest en de eventuele hertest dienen ter informatie te worden geleverd aan de CISO.

Bijlage 2. De webapplicatie security verificatie niveaus

De Web applicatie security verificatie niveaus zijn volgens het Open Web Application Security Project (OWASP) in 4 beveiligingsniveaus in te delen.
Schematisch ziet dat er als volgt uit



Niveau 1:
Vaak kan met tooling worden vastgesteld of een eenvoudige webapplicatie kwetsbaar is voor aanvallen. Dit is de basis check om te controleren of het patchlevel van de diverse onderdelen van de webapplicatie en de hardware op orde is en de software geen bekende kwetsbaarheden bevat die direct met eenvoudige tooling kunnen worden misbruikt.
Onder aanvallen wordt verstaan het veranderen van content, het plaatsen van malware en virussen.

Niveau 2:
Met bijzondere tooling en handmatige checks kan vervolgens worden vastgesteld of het beveiligingsniveau van een eenvoudige webapplicatie voldoende vertrouwen geeft om mogelijke hacks te kunnen voorkomen. In deze fase wordt niet alleen passief getest maar wordt ook gekeken naar de opbouw van de site met behulp van spidering technieken en wordt getracht om actief de site te hacken op basis van de weblogic en aangepaste scripts. webapplicaties die hiervoor in aanmerking komen zijn applicaties die persoonlijke/zakelijke transacties of persoonlijk identificeerbare informatie bevatten. Bij dit soort scan wordt ook de sourcecode van de applicatie gescand op kwetsbaarheden

Niveau 3:
Wordt via de webapplicatie (bijzondere) persoonsgegevens verkregen en wordt deze op enigerlei wijze opgeslagen in achterliggende systemen dan is het verplicht om naast de voornoemde tooling van niveau 1 en 2 ook het ontwerp van de applicatie in detail te testen.

Niveau 4:
Hebben we het over zeer bijzondere webapplicaties waarbinnen bijvoorbeeld wordt gewerkt met uiterst vertrouwelijke gegevens, is het mogelijk om tijdens de bouw van de applicatie het ontwerp en de code beide handmatig te reviewen bovenop de hiervoor genoemde geautomatiseerde en handmatige beveiligingschecks.
Voor Amsterdam is dit niveau van testen niet direct noodzakelijk. Beveiligingsniveau 4 testen worden uitgevoerd uitsluitend uitgevoerd op uiterst cruciale webapplicaties die toegang geven tot uiterst vertrouwelijke informatie.
Samengevat betekent dit dat we met behulp van het OWASP model de webapplicaties classificeren naar een van de bovenstaande categorieën en dan gaan checken in hoeverre een webapplicatie voldoende beveiligd is conform dit model.

1.6 Verificatie eisen OWASP

Binnen het OWASP framework worden de volgende gegroepeerde security eisen gedefinieerd waarmee bij ontwikkeling van nieuwe en het testen van bestaande webapplicaties voor zo ver van toepassing rekening moet worden gehouden.

V1. Documentatie van de security architectuur
V2. Authenticatie
V3. Sessie management
V4. Toegangscontrole
V5. Input validatie
V6. Output codering
V7. Cryptografie
V8. Foutafhandeling en logging
V9. Data protectie
V10. Beveiliging van communicatie
V11. Http security
V12. Configuratie security
V13. Schadelijke software opsporing
V14. Interne beveiliging

Voor al deze gebieden, zijn eisen gespecificeerd waaraan moet worden voldaan om de benoemde risico niveaus te kunnen afdekken;

Door middel van de geautomatiseerde scan en een handmatige verificatie kan worden vastgesteld of webapplicaties aan deze eisen voldoen.