INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

Penetratietesten

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

Naam document

Handreiking penetratietesten

Versienummer

2.2

Versiedatum

April 2020

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	November 2014	
1.0.1	Augustus 2016	Taskforce BID verwijderd, WBP vervangen door Wbp, GBA vervangen door BRP
2.0	Februari 2019	BIO update
2.1	Juli 2019	Verwijzingen aangepast
2.2	April 2020	Whitepaper Securitytesten van NCSC

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is om aandachtspunten met betrekking tot het uitvoeren van penetratietesten aan te reiken zodat invulling gegeven kan worden aan de gemeentelijke nformatiebeveiligingsbeleidsregels.

Doelgroep

Dit document is van belang voor de CISO, de systemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente
- Whitepaper Securitytesten (NCSC)

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

12.6.1 Beheer van technische kwetsbaarheden

18.2.3 Beoordeling van technische naleving

18.2.3.1 Informatiesystemen worden jaarlijks gecontroleerd bijv. door kwetsbaarheidsanalyses of pentesten

Wat is er veranderd ten opzichte van de BIG?

Er is weinig veranderd ten opzichte van de BIG, de maatregelen en controls zijn net iets anders opgeschreven maar als er al werd voldaan aan de BIG dan wordt er ook voldaan aan de BIO.

Inhoudsopgave

1. Inleiding

Het doel van penetratietesten is het verkrijgen van inzicht in de status en effectiviteit van de beveiligingsmaatregelen. Het resultaat geeft aan wat de aandachtsgebieden zijn en biedt concrete handvatten voor adequate maatregelen en investeringen, met als doel de beveiligingsrisico's te reduceren. Het geeft inzicht in de gevonden inbraakmogelijkheden, de genomen maatregelen en de restrisico's en de mogelijkheid hierover aan het management te rapporteren.
Een penetratietest kan ook worden ingezet als onderdeel van een bewustwordingscampagne om de bewustwording van de medewerkers te verhogen.

Voordelen

- Tijdens oplevering of bij grote wijzigingen kan een penetratietest kwetsbaarheden op te sporen, waardoor de kwaliteit en het beveiligingsniveau van het informatiesysteem wordt verhoogd.
- Met penetratietesten kunnen gemeenten nagaan hoe goed de gemeentelijke informatiesystemen en gegevens beschermd zijn tegen aanvallen en het geeft gemeenten zodoende een diepgaand en compleet overzicht van het beveiligingsniveau van de gemeentelijke ICT-infrastructuur. Penetratietesten zijn dan ook een middel voor gemeenten om de kwaliteit van de digitale bescherming aan te tonen.
- Op basis van de resultaten van de penetratietesten kunnen gemeenten een risicoafweging maken en zodoende de belangrijke risico's van beveiligingslekken reduceren en daarmee de vertrouwelijkheid en integriteit van gemeentelijke informatie en informatiesystemen verhogen.

1.1. Aanwijzing voor gebruik

Deze handreiking is geschreven om aandachtspunten met betrekking tot het uitvoeren van penetratietesten aan te reiken zodat invulling gegeven kan worden aan de gemeentelijke informatiebeveiligingsbeleidsregels. Deze handreiking is geen volledige procesbeschrijving en bevat geen productnamen, maar bevat wel voldoende informatie om goede (beleids)keuzes te maken en bewustwording te creëren met betrekking tot het uitvoeren van penetratietesten.

1.2. Whitepaper Securitytesten van het NCSC

Het NCSC heeft een whitepaper securitytesten geschreven die een goede aanvulling is op deze handreiking. [1]
Deze whitepaper gaat met name over het proces die een opdrachtgever van een securitytest moet doorlopen. Dit proces wordt middels vier stappen beschreven:

1. Bepaal uw doel: Stel uzelf de juiste vragen voor een goede doelstelling.
2. Bepaal het middel: Kies het passende type securitytest en bepaal de scope en diepgang.
3. Voer regie over de uitvoering: Selecteer een partij om de test uit te voeren en begeleid de testers.
4. Borg de verbeteringen in uw organisatie: Zorg ervoor dat u de verbeterpunten toepast.

1 https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten

2. Aandachtspunten Penetratietesten

Een manier om de kwaliteit van de digitale bescherming van een gemeente te bewijzen is om te proberen in de ICT-omgeving van de gemeente binnen te dringen. Hierbij kan gebruik worden gemaakt van verschillende methoden en technieken, welke worden ondersteund door diverse hulpmiddelen.

Penetratietesten kunnen bestaan uit interne en externe aanval scenario's. Interne aanvallen zijn pogingen om toegang tot het informatiesysteem te krijgen, nadat toegang verkregen is tot een component binnen de gemeentelijke infrastructuur. Externe aanvallen zijn pogingen om binnen te dringen vanaf een willekeurige computer buiten de gemeentelijke infrastructuur.

Alle vormen van penetratietesten kunnen worden uitgevoerd op verschillende lagen in het systeem, zowel op de infrastructuur- als op de applicatielaag. De infrastructuurlaag omvat servers, besturingssystemen, netwerkapparatuur en beveiligingscomponenten (Bijvoorbeeld: firewalls[2], intrusion detection systems (IDS)[3], et cetera). Testen op de applicatielaag worden uitgevoerd als de onderzochte server bijvoorbeeld een applicatie- of webserver is. Er wordt dan gekeken of de applicatie mogelijk lekken bevat, die de veiligheid van het informatiesysteem of de achterliggende ICT-infrastructuur in gevaar brengen.

Periodiek

Het is van belang om periodiek een penetratietest uit te (laten) voeren:

- Periodiek (jaarlijks/tweejaarlijks) om bestaande systemen te testen op nieuwe inbraaktechnieken en 'exploits'.
- Periodiek (jaarlijks/tweejaarlijks) als onderdeel van het Information Security Management System (ISMS).[4]

Andere redenen om een penetratietest uit te (laten) voeren kunnen zijn:

- Er zijn wijzigingen ten opzichte van de vroegere situatie.
- De acceptatiefase van een nieuw systeem of een nieuwe applicatie.

2 https://nl.wikipedia.org/wiki/Firewall

3 https://nl.wikipedia.org/wiki/Intrusion_Detection_System

4 Zie hiervoor ook het operationele product 'Information Security Management System (ISMS)'

Ketenpartijen

Bij het (laten) uitvoeren van een penetratietest is het noodzakelijk aandacht te besteden aan het bijzondere karakter van het werken in ketenverband[5]. Dit kan ook een gemeenschappelijke regeling of een Shared Service Center (SSC) van meerdere gemeenten zijn. Direct houdt dit in dat het noodzakelijk is dat elke ketenpartij niet alleen de eigen infrastructuur (het eigen computernetwerk) test, maar steeds bedacht moet zijn op effecten van die test naar de andere ketenpartijen en op de effecten van testen die de andere ketenpartijen uitvoeren. Bovendien is het noodzakelijk dat er specifieke tests worden uitgevoerd, waarin wordt geprobeerd om het gemeenschappelijke computernetwerk te penetreren vanuit, of via, het computernetwerk van een ketenpartij. Waar mogelijk is het noodzakelijk om specifieke tests uit te voeren waarin wordt geprobeerd om het gemeenschappelijke computernetwerk te penetreren vanuit, of via, het computernetwerk van een ketenpartij. Hierover dienen afzonderlijke afspraken gemaakt te worden.

Vulnerability scan

Naast penetratietesten kan ook gebruik worden gemaakt van vulnerability scans. Deze scan zijn fundamenteel anders dan penetratietesten. Penetratatietesten gaan van buiten naar binnen en vulnerability scans worden eigenlijk altijd van binnenuit uitgevoerd op de server, host of platform. Deze scans worden vaak gebruikt om te testen op bekende kwetsbaarheden in de breedte. De security tester laat zien dat er een kwetsbaarheid gedetecteerd is maar maakt geen daadwerkelijk misbruik van deze omissie in de beveiliging en probeert niet de systemen verder binnen te dringen, waar een security tester dat bij een penetratietest wel zou doen. Dit is handig voor snelheid vanwege het automatische karakter van de test of wanneer er zeer kritieke objecten onderzocht worden waarbij men niet verder wil testen dan de oppervlakte testen vanwege mogelijke onberekenbare vervolgschade door verouderde technologie.

Het uitbreiden van de penetratietest als gevolg van de invloed op de computernetwerken, geeft inzicht in:

- De mate waarin het computernetwerk van de gemeente meer of anders kwetsbaar is voor inbraken, als gevolg van het werken in ketenverband.
- De mate waarin het computernetwerk van elk van de ketenpartijen meer of anders kwetsbaar is voor inbraken, als gevolg van het werken in ketenverband.

5 Een keten is een samenwerkingsverband tussen organisaties die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) doelstellingen nastreven. Deze ketenpartners zijn zelfstandig, maar zijn ook afhankelijk van elkaar waar het gaat om het bereiken van de gezamenlijke doelstellingen, hierna ketendoelstellingen genoemd. (Bron: https://www.noraonline.nl/wiki/Ketensturing/De_wereld_van_ketens/Wat_is_een_keten%3F)

Gemeentelijke informatiebeveiligingsbeleidsregels

De gemeentelijke informatiebeveiligingsbeleidsregels met betrekking tot penetratietesten zijn onder andere:[6]

- De gemeente/directie/afdeling bevordert algehele communicatie en bewustwording rondom informatieveiligheid.[7]
- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de proceseigenaar).
- Het computernetwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het computernetwerk niet onder het afgesproken minimum niveau (service levels) komt.
- In opdracht van de eigenaar van data, maakt ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
- Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen.
- Er worden maatregelen getroffen om te verzekeren dat gegevens over logging[8] beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.
- Applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals de ICT-beveiligingsrichtlijnen voor webapplicaties.[9] Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10.[10]
- Webapplicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL-injectie, cross site scripting, et cetera).
- Technische kwetsbaarheden worden regulier met een minimum van vier keer per jaar gerepareerd door ‘patchen’ van software, of ‘ad hoc’ bij acute dreiging.[11] Welke software wordt geüpdatet wordt mede bepaald door de risico’s.

6 Zie ook het voorbeeld algemene informatiebeveiligingsbeleid

7 Bewustwording is sowieso een belangrijk onderdeel van informatiebeveiliging, maar in dit kader dient enerzijds aandacht te worden besteedt aan het belang de eindgebruikers te informeren over het belang van informatiebeveiliging en hen anderzijds te trainen op het herkennen van oneigenlijk gebruik. Denk hierbij aan de volgende aanvalstechnieken: persoonlijk contact (bijvoorbeeld door zich als helpdeskmedewerker voor te doen), een aanvaller verstuurt een e-mailtje met een belangwekkende tekst (phishing) en de aanvaller probeert vertrouwelijke informatie te krijgen door het snuffelen in vuilnisbakken, containers en prullenbakken.

8 Zie hiervoor ook het operationele product ‘Aanwijzing Logging’.

9 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

11 Zie hiervoor ook het operationele product ‘Patch management voor gemeenten’.

- ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatiebeveiligingsbeleid.
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD[12], Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI[13]) en Basisregistratie Personen (BRP[14])/ Gemeentelijke Basisadministratie Persoonsgegevens Verstrekkingsvoorziening (GBA-V[15]).
    - Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO/CISO onderzocht door gemeentelijke auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Jaarlijks worden ca. drie audits/onderzoeken gepland. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.

12 https://www.digid.nl/

13 https://wetten.overheid.nl/BWBR0013280/

14 De Basisregistratie Personen is een samenvoeging van de Gemeentelijke Basisadministratie Personen (GBA) en Register Niet Ingezetenen (RNI) (https://www.rvig.nl/brp).

15 https://www.rvig.nl/documenten/richtlijnen/2012/01/03/dienstverleningsafspraken-gba-v-en-tmv

3. Uitvoeren penetratietest

Hier worden de stappen voor penetratietesten toegelicht, in bijlage 1 is een draaiboek te vinden die meer op het detail ingaat. Per stap staat op hoofdlijnen beschreven welke acties ondernomen dienen te worden en welke resultaten verwacht worden. Het draaiboek is gebaseerd op best practices.

Het draaiboek fungeert als praktisch hulpmiddel voor degene die verantwoordelijk is voor het uitvoeren van de penetratietest. Het biedt handvatten voor een planning van de te ondernemen acties en de monitoring van de voortgang van de test. Tevens kan degene binnen de gemeente die de penetratietest uitvoert, het draaiboek gebruiken om zijn/haar vorderingen bij te houden.

3.1. Stap 1 Penetratietest voorbereiden

Deze stap beschrijft de activiteiten die uitgevoerd dienen te zijn, voordat een penetratietest – kortweg ook wel pentest genoemd - daadwerkelijk uitgevoerd kan worden. In bijlage 1 worden de verschillende activiteiten voor deze stap beschreven inclusief het beoogde resultaat.

Het doel van de stap is het treffen van de voorbereidingen zodat de opdracht, tot uitvoeren van de penetratietest, verleend kan worden. Voor het verlenen van de opdracht is er mogelijk toestemming noodzakelijk van de bestuurder. Of deze toestemming noodzakelijk is hangt onder andere af van de scope van de pentest en, of er een mogelijkheid bestaat dat er gegevens van derden kunnen worden gevonden.

Voor de inhuur van penetratietesters is het noodzakelijk dat gemeenten een offerteaanvraag opstellen. De whitepaper securitytesten [16] van het Nationaal Cyber Security Centrum (NCSC) biedt een handleiding die beschrijft hoe dit succesvol kan verlopen en welke elementen ten minste in de offerteaanvraag beschreven dienen te worden. Hoe beter een organisatie de opdracht in de offerteaanvraag verwoordt, hoe beter de markt kan offreren. Deelnemers van GGI-Veilig perceel 3 kunnen binnenkort een template aanvraag securitytesten verwachten die gebruikt kan worden voor een minicompetitie. [17]

3.2. Stap 2 Penetratietest uitvoeren

Deze stap kan aantonen of systemen in de praktijk te ‘hacken’[18] zijn. Een penetratietestleverancier (penetratietester) probeert de systemen van de gemeente te ‘hacken’ zodat duidelijk wordt of/waar de systemen kwetsbaar zijn. Het is noodzakelijk dat door alle betrokken partijen een vrijwaringsverklaring getekend is, voordat de penetratietest uitgevoerd kan worden. In bijlage 1 worden de verschillende activiteiten voor deze stap beschreven inclusief het beoogde resultaat.

Het doel van deze stap is het verlenen van de opdracht tot uitvoering van de penetratietest en de daadwerkelijke uitvoering daarvan, inclusief het vastleggen en analyseren van de bevindingen.

16 https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten

17 https://forum.vng.nl/do/startpage?id=1810104-737461727470616765

18 Met een hack wil een persoon zwakke plekken aantonen dat computerprogramma’s en –netwerken (nog) niet veilig zijn. Dit kan met kwade (criminele) bedoelingen of zonder er verder misbruik van te maken.

3.3. Stap 3 Bevindingen penetratietest oplossen

Bij deze stap gaat het er om, om op basis van de bevindingen uit de penetratietest, een gemeentelijk verbeterplan op te stellen, of het eerder opgestelde gemeentelijke verbeterplan bij te werken. Als externe partijen betrokken zijn bij het oplossen van de bevindingen is het noodzakelijk om duidelijke afspraken te maken over hoe de bevindingen uit de penetratietest worden opgelost en op welke termijn. In bijlage 1 worden de verschillende activiteiten voor deze stap beschreven, inclusief het beoogde resultaat.

Het doel van deze stap is het opstellen of aanpassen van het verbeterplan op basis van de bevindingen uit de pentest. Op basis van de uitgevoerde penetratietest is het mogelijk dat er maatregelen getroffen dienen te worden ter verbetering van de ICT-beveiliging.

3.4. Checklist beoordelen kwaliteit penetratietesten

Onderstaande vragenlijst kan door de gemeente worden gebruikt om de penetratietesten te beoordelen. Deze vragenlijst is zeker niet volledig, maar geeft voldoende handvatten om een eerste inschatting van de status met betrekking tot penetratietesten te maken.

- Is de scope voor de penetratietesten vastgesteld?
- Is vastgesteld wie allemaal geïnformeerd dienen te worden over deze pentest?
- Is er een penetratietester geselecteerd?
- Zijn de penetratietesten ingepland?
- Is de vrijwaringsverklaring voor de penetratietest opgesteld en ondertekend door alle benodigde partijen?
- Staat de pentester onafhankelijk ten opzichte van het te onderzoeken object?
- Heeft de pentester aantoonbare eerdere ervaringen met pentesten?
- Zijn er afspraken over in te zetten tooling en methoden (bijv. stresstest en social engineering)?
- Is de vrijwaringsverklaring voor de penetratietest opgesteld en ondertekend door alle benodigde partijen?
- Is er een officiële opdracht verstrekt voor het uitvoeren van de penetratietest met een verwijzing naar de scope van de penetratietest die getest moeten worden?
- Is er een rapportageformat afgesproken met daarin vermeld welke onderwerpen minimaal behandeld dienen te worden.
- Is er een verbeterplan opgesteld op basis van de bevindingen van de penetratietest op basis van risico inschaling?
- Is in kaart gebracht wat de relevante bevindingen uit de penetratietest zijn op basis van prioriteit?
- Zijn de maatregelen, voor zowel de gemeente als de externe organisaties, vastgelegd, die nodig zijn op basis van de bevindingen van de penetratietest?
- Wordt de voortgang van de implementatie van de maatregelen uit het verbeterplan actueel gehouden en hierover gerapporteerd?

4. Beoordelen resultaat penetratietest

De gemeente als opdrachtgever, of een door de gemeente ingehuurde externe auditor zal degene zijn die de penetratietest beoordeelt. Hierbij dient vastgesteld te worden of de penetratietest voldoet aan de eisen die de gemeente aan deze penetratietest heeft gesteld. Deze eisen kunnen ook afkomstig zijn van een externe norm.[19] De aanpak voor het beoordelen van de resultaten van penetratietesten is gebaseerd op de bekende PDCA-cirkel afkomstig uit het kwaliteitsdenken. PDCA staat voor Plan, Do, Check en Act. Dit zijn vier processtappen om uiteindelijk tot een continue verbetering van penetratietraject (proces) te komen. De bevindingen dienen gebruikt te worden voor de verdere verbetering van de informatieveiligheid. Bij de beoordeling dient gelet te worden op de volgende zaken:

1. Worden de penetratietesten periodiek en conform planning (Plan) uitgevoerd (Do)?
2. Hebben de testen de juiste scope gehad (Check)?
3. Zijn de testen van voldoende kwaliteit geweest (Check)?
4. Zijn de bevindingen geëvalueerd (Check)?
5. Is er op basis van een risicoafweging een verbeterplan met prioriteitenstelling opgesteld (Act)?

In het verbeterplan met prioriteitenstelling worden acties (maatregelen) naar aanleiding van een penetratietest opgenomen. Het kan hierbij gaan om:

- Het uitvoeren van een source code review.
- Het aanbrengen van configuratieaanpassingen.
- Het inzetten van extra beveiligingsapparatuur of -programmatuur (bijvoorbeeld firewalls).
- Het aanpassen van procedures en werkvoorschriften.
- Et cetera.

19 Denk hierbij aan het ICT-Beveiligingsassessment DigiD (https://www.logius.nl/producten/toegang/digid/logiusnlbeveiligingsassessments/).

5. Vrijwaringsverklaring penetratietest

In bijlage 3 wordt een voorbeeld overeenkomst (hierna te noemen: Overeenkomst) inzake een regeling van aansprakelijkheid met betrekking tot de uitvoering van een penetratietest beschreven, die door gemeenten kan worden gebruikt bij de inhuur van een penetratietester. Deze Overeenkomst bevat een vrijwaringsverklaring.

Toelichting

De penetratietester voert een penetratietest uit op verzoek van een gemeente. De gemeente wordt dan ook als 'opdrachtgever' aangeduid in de Overeenkomst. Omdat de penetratietester werkzaamheden verricht die strikt genomen niet legaal zijn (binnendringen van ICT-systemen) en tot aansprakelijkheid kunnen leiden, moet de gemeente als opdrachtgever de penetratietester vrijwaren. De Overeenkomst bevat een vrijwaringsverklaring (artikel 6, lid 5).

Indien (een deel van) de penetratietest uitgevoerd wordt bij de gemeente zelf, is de gemeente zowel 'opdrachtgever' als 'onderzochte partij'. De gemeente moet in dit geval dus vanuit beide rollen tekenen voor de vrijwaring. Indien de penetratietest niet bij de gemeentelijke organisatie alleen wordt uitgevoerd, maar ook bij externe partijen zoals een SaaS-dienstverlener en/of een hostingpartij, moeten ook deze partijen de penetratietester vrijwaren. Deze externe partijen worden als 'onderzochte partij' in de Overeenkomst aangeduid en worden, door ondertekening, partij van de Overeenkomst.

Mogelijke aansprakelijkheid van de penetratietester als gevolg van handelingen die buiten de scope van de opdracht vallen, wordt niet uitgesloten. De hoogte van de aansprakelijkheidsbeperking kan door de lokale overheidsorganisaties zelf worden ingevuld in de Overeenkomst (artikel 6, lid 7).

De penetratietester voert de penetratietest uit op verzoek van en bij de gemeenten. En, indien er sprake is van externe betrokken partijen, bij de extern onderzochte partij(en). Omdat de uitvoerder werkzaamheden verricht die tot aansprakelijkheid kunnen leiden, wil hij zich ervan verzekeren dat hij hiervoor gevrijwaard wordt. Die vrijwaringsverklaring is opgenomen in de Overeenkomst (artikel 6, lid 5). Normaliter is bijvoorbeeld het 'kraken' van een ICT-systeem aan te merken als computervredebreuk, en daarmee strafbaar. Vandaar de verwijzingen naar artikelen uit het Wetboek van Strafrecht.

De offerteaanvraag maakt onderdeel uit van de Overeenkomst. In de Overeenkomst wordt op diverse plekken verwezen naar deze offerteaanvraag. Zie hoofdstuk 3 voor onderwerpen die in ieder geval in de offerteaanvraag geregeld dienen te zijn.

Bijlage 1: Draaiboek uitvoeren penetratietest

Voorbereiding

Nr.	Activiteit	Omschrijving	Beoogde resultaat
1	Scope vaststellen	Elke gemeente dient zelf de scope te bepalen, aangezien deze sterk afhangt van de inrichting van het computernetwerk. Het advies is om aan te sluiten bij de penetratietests die al binnen de gemeente en eventueel binnen ketenpartijen plaatsvinden. Breng in kaart op welke (onderdelen van de) ICT-infrastructuur en software een penetratietest uitgevoerd moet worden, welke (externe) organisatie(s) deze expertise beheren en welke partijen een vrijwaringsverklaring moeten ondertekenen voor het uitvoeren van een penetratietest. Bij het bepalen van de scope en de uitvoeringsvorm van de pentest zijn minimaal de verantwoordelijk bestuurder of manager aanwezig en de CISO of informatiebeveiligingsfunctionaris van de gemeente betrokken. Afhankelijk van de ruchtbaarheid die aan de pentest wordt gegeven kunnen ook de proces- en systeemeigenaar (de verantwoordelijke) van het te onderzoeken object betrokken worden.	Een overzicht van de onderdelen van de ICT-infrastructuur en software waar een penetratietest op uitgevoerd moet worden en de verantwoordelijken die een vrijwaringsverklaring moeten tekenen.
2	Opstellen offerteaanvraag	Hieronder de onderwerpen die ten minste in de offerteaanvraag geregeld dienen te zijn: 1. Een scopedefinitie (reikwijdte en diepgang) waarin het object van de pentest beschreven wordt. Bijvoorbeeld: • Internetfacing van webpagina's van het te onderzoeken systeem (URL's). • (Systeem)koppelingen en infrastructuur die met het te onderzoeken systeem gekoppeld zijn en betrekking hebben op het proces. • Externe verbindingen met ketenpartijen. • Externe verbindingen met andere partijen, niet tot de keten behorend, voor zover deze verbindingen dezelfde systemen, gegevens of functionaliteit raken als via de gemeente worden ontsloten. • Verbindingen naar het openbare Internet ten behoeve van gebruik door burgers of private bedrijven. 2. Een opdrachtomschrijving met daarin een heldere onderzoeksvraag aan de pentester. Bijvoorbeeld: • Stel vast of het mogelijk is om ongeautoriseerd toegang tot het te onderzoeken systeem te krijgen. • Stel vast of het mogelijk is om ongeautoriseerd toegang te verkrijgen tot het te onderzoeken systeem en de achterliggende systemen. 3. Een omschrijving van de informatie die de opdrachtgever aan de pentester ter beschikking zal stellen voorafgaand aan de pentest (blackbox-, whitebox-, greybox-test).	De offerteaanvraag is opgesteld en goedgekeurd.

Nr.	Activiteit	Omschrijving	Beoogde resultaat
		• Wijze van penetratietesten: van buiten via het internet (non-privileged), blackbox, op basis van in ieder geval publiekelijk beschikbare exploits. • Wijze van penetratietesten: whitebox, waarbij de op het systeem aangesloten partij desgevraagd de benodigde privileges en configuratie-instellingen van relevante componenten (zoals netwerkapparatuur en servers) aan de penetratietester heeft verstrekt. 4. Welke technieken bij de penetratietest zullen worden gebruikt. Bijvoorbeeld: phishing[20], systeem en/of protocol hacks, database aanvallen (bijvoorbeeld: SQL-injectie[21]), trojaanse paarden[22], backdoors[23], sniffers[24], Denial of Service (DoS)[25], hijacking (bijvoorbeeld: sessie[26] of browser[27]), privilege escalatie[28] en bufferoverflows[29].[30] 5. Een planning, inclusief de momenten waarop er niet getest mag worden. 6. De in de rapportages op te leveren informatie. Bij voorkeur wordt gebruik gemaakt van een standaard manier van rapporteren. Bijvoorbeeld Open Source Security Testing Methodology Manual - Security Test Audit Report (OSSTMM STAR)[31]. 7. De offerteaanvraag dient op het juiste niveau goedgekeurd te worden. Bijvoorbeeld door een bestuurder of manager.	
3	Communicatie vaststellen	Er dient vastgesteld te worden wie binnen de gemeente geïnformeerd dienen te worden met betrekking tot deze pentest. Specifiek dient hierbij aandacht te worden gegeven of het noodzakelijk is om de afdeling communicatie op de hoogte te brengen. Dit hangt onder andere af van de scope van de pentest, of er gegevens van derden geraakt kunnen worden en de ruchtbaarheid die aan de pentest gegeven kan worden.[32] Het voordeel is dat er	Er is een vastgesteld wie geïnformeerd dienen te worden over deze pentest.

20 https://nl.wikipedia.org/wiki/Phishing

21 https://nl.wikipedia.org/wiki/SQL-injectie

22 https://nl.wikipedia.org/wiki/Trojaans_paard_%28computers%29

23 https://nl.wikipedia.org/wiki/Achterdeurtje

24 https://nl.wikipedia.org/wiki/Packet_sniffer

25 https://nl.wikipedia.org/wiki/Denial-of-service

26 https://nl.wikipedia.org/wiki/Session_hijacking

27 https://en.wikipedia.org/wiki/Browser_hijacking

28 https://en.wikipedia.org/wiki/Privilege_escalation

29 https://nl.wikipedia.org/wiki/Bufferoverloop

30 Als er tijdens de pentest gebruik wordt gemaakt van aanvalstechnieken waar medewerkers bij betrokken worden is het goed om de medewerkers hierover achteraf in te lichten. Bijvoorbeeld bij het inzetten van phishingsmails.

31 Zie hiervoor 'Chapter 13 – Reporting with the STAR' in het handbook 'OSSTMM 3 – The Open Source Security Testing Methodology Manual' (https://www.isecom.org/OSSTMM.3.pdf).

32 Vaak wil men het aantal medewerkers wat op de hoogte is van de pentest zo klein mogelijk houden, om de pentest zo realistisch mogelijk te laten zijn.

Nr.	Activiteit	Omschrijving	Beoogde resultaat
		door de afdeling communicatie op voorhand verklaringen opgesteld kunnen worden voor het geval er zaken naar buiten komen. Bijvoorbeeld het lekken van gegevens of het niet beschikbaar zijn van de dienstverlening doordat er gebruik gemaakt wordt van bestaande kwetsbaarheden gedurende de pentest.	
4	Selecteer een penetratietester	Voor de selectie van een penetratietester kan gebruik worden gemaakt van de criteria zoals beschreven in paragraaf 2.3. Als de resultaten van de penetratietest onderdeel uit gaan maken van een audit, is het advies om er voor te zorgen dat de (RE-)auditor, die de uiteindelijke audit gaat uitvoeren, akkoord is met de manier van testen en rapporteren van de penetratietester. Dit zodat de uitkomsten van de penetratietest ook voor de audit bruikbaar zijn.	Er is een geschikte penetratietester geselecteerd.
5	Vrijwaringverklaring ondertekenen	Laat de vrijwaringverklaring die door de gemeente en externe organisatie(s) (Bijvoorbeeld: hostingpartij) is ondertekend door de penetratietester ondertekenen.	De vrijwaringsverklaring(en) zijn ondertekend door alle juiste partijen (Zie bijlage 1: Voorbeeld overeenkomst inzake een regeling van aansprakelijkheid met betrekking tot de uitvoering van een penetratietest).

Tabel 1 Activiteiten bij de voorbereiding van penetratietesten

Uitvoeren

Nr.	Activiteit	Omschrijving	Resultaat
1	Verstrek de opdracht tot uitvoering van de penetratietest.	Nadat de vrijwaringverklaring is ondertekend door alle betrokken partijen, kan de gemeente de definitieve opdracht tot uitvoering van de penetratietest verstrekken aan de penetratietester. Tijdens de uitvoering van de penetratietest dient de verantwoordelijk bestuurder of manager en de CISO of informatiebeveiligingsfunctionaris door de penetratietester op de hoogte gehouden te worden over de voortgang en de gevonden resultaten.	De testen worden uitgevoerd door de penetratietester, onder de voorwaarden die in de vrijwaringsverklaring zijn vastgelegd.
2	Leg de bevindingen die uit de penetratietest(en) komen vast.	Alle bevindingen die uit de penetratietest(en) voortkomen dienen vastgelegd te worden. De gemeente kan dan op basis van een risicoafweging vaststellen welke bevindingen wel en welke bevindingen niet acceptabel zijn. Deze risicoafweging dient door de proces- en systeemeigenaar (de verantwoordelijke) van het te onderzoeken object te worden gemaakt in overleg met de CISO of informatiebeveiligingsfunctionaris van de gemeente.[33] De rapportage dient de volgende onderdelen te bevatten: • Beschrijving beveiligingslek en risicoclassificatie. • Hoe is de constatering van het beveiligingslek gedaan. • Hoe kan het beveiligingslek gereproduceerd worden.[34] • Details beveiligingslek, niet alleen technisch maar ook in begrijpbare taal Indien bekend, verbetervoorstellen. Bijvoorbeeld oplossing of workaround. De vorm en verwoording van de rapportage dient zodanig te zijn dat deze in voorkomend geval met één of meer ketenpartijen kan worden besproken. De gemeenschappelijke risico's worden gedeeld met de ketenpartij(en).	De bevindingen van de penetratietest(en) zijn vastgelegd.
3	Geef waar nodig aan welke maatregelen noodzakelijk zijn op basis van de bevindingen.	Stel een verbeterplan op waarin is opgenomen welke maatregelen noodzakelijk zijn, op basis van de bevindingen. Er kunnen ook maatregelen worden voorgesteld die wenselijk zijn, hiervoor dient dan een afweging te worden gemaakt of deze wel of (nog) niet worden meegenomen. Geef per maatregel aan wie hiervoor verantwoordelijk is en wanneer de maatregel is geïmplementeerd. Als een maatregel op basis van een risicoafweging toch niet wordt meegenomen dient dit ook vermeld te worden.	De noodzakelijke maatregelen zijn verwerkt in een verbeterplan (Zie bijlage 2 voor een voorbeeld verbeterplan).

Tabel 2 Activiteiten bij het uitvoeren van penetratietesten

33 Zie hiervoor ook het operationele producten met betrekking tot risicoanalyse, zoals de 'baselintoets' en de 'Diepgaande Risicoanalyse'.

34 Bij het oplossen van het beveiligingslek kan (door de gemeente) zelfstandig hergetest worden.

Bevindingen oplossen

Nr.	Activiteit	Omschrijving	Resultaat
1	Analyseren bevindingen met betrekking tot de gemeente.	De bevindingen uit de penetratietest die voor de gemeente als onacceptabel risico kunnen worden bestempeld, vereisen maatregelen om deze risico's in te perken dan wel te voorkomen.	Beschrijving verbeterplan en start uitvoering verbeterplan (Zie bijlage 4 voor een voorbeeld verbeterplan).
2	Analyseren bevindingen met betrekking tot externe organisaties.	Indien (een deel van) de testen bij een of meer externe organisaties heeft plaatsgevonden, vraag dan aan de externe organisatie(s) de noodzakelijke maatregelen te nemen en voor de overige bevindingen uit de penetratietest die op hen van toepassing zijn een verbeterplan op te stellen. Zorg dat de externe organisatie aangeeft per welke datum zij het verbeterplan hebben uitgevoerd.	Overzicht van: • De maatregelen die de betrokken organisatie(s) geïmplementeerd dienen te hebben naar aanleiding van de uitkomsten van de penetratietest. • De afspraken binnen welke termijn de betrokken organisatie(s) de activiteiten uit het opgestelde verbeterplan hebben uitgevoerd.

Tabel 3 Activiteiten met betrekking tot bevindingen penetratietest oplossen

Bijlage 2: Criteria voor selectie van penetratietester

Bij de selectie van een penetratietester kan gebruik gemaakt worden van de criteria zoals in tabel 4 weergegeven.

Criteria	Voorbeelden en aanvullingen
Is de penetratietester onafhankelijk?	Staat de penetratietester buiten het project?
Is de penetratietester extern?	Bijvoorbeeld: is de penetratietester in dienst bij de organisatie en/of leverancier die het object is van de penetratietest?
Is de penetratietester ervaren?	Bijvoorbeeld: zijn er referenties beschikbaar en wordt de penetratietester (h)erkend in de security community? Denk hierbij aan: • Beschikt de penetratietester over uitgebreid curriculum vitae op het gebied van penetratietesten? • Heeft de penetratietester invloedrijke whitepapers gepubliceerd? • Was de penetratietester keynote spreker op security congressen? •
Heeft de penetratietester aantoonbare brede ervaring met niet-standaardtesten in verschillende omgevingen?	Bijvoorbeeld: zijn er referenties beschikbaar waaruit blijkt dat de penetratietester in diverse sectoren actief is geweest? Denk hierbij aan: • Publiek en privaat (financiële, industriële omgeving). • (web)Applicaties die op zichzelf staand of in ketenverband (gemeenschappelijke computernetwerk) functioneren. • Inzet van traditionele en digitale (ICT-) recherchetechnieken. • Penetratietest zowel gericht op mensen (mystery guests of social engineering) als informatie. •
Heeft de penetratietester voldoende capaciteit?	Bijvoorbeeld: heeft de penetratietester schaling- en doorlooptijdmogelijkheden?
Heeft de penetratietester een verzekering tegen schade waar hij toch aansprakelijk voor is?	Bijvoorbeeld: schade die niet is afgedekt door de vrijwaringsverklaring.[35]
Maakt de penetratietester gebruik van gecertificeerd personeel?	Bijvoorbeeld: Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH)[36] of Licensed Penetration Tester (LPT)[37].

35 Zie ook bijlage 1.

36 https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

37 https://cert.eccouncil.org/licensed-penetration-tester.html

Criteria	Voorbeelden en aanvullingen
Maakt de penetratietester gebruik van 'state-of-the-art' tools en de meest up to date hacktechnieken?	Bijvoorbeeld: IBM Appscan[38], HP Webinspect[39], Acunetix[40], Nessus[41] en NeXpose[42], et cetera.
Maakt de penetratietester gebruik van eigen research en is hij niet afhankelijk van verouderde informatie uit het publieke security domein?	
Voert de penetratietester zelf de test uit, of heeft hij deze uitbesteedt aan een andere organisatie?	

Tabel 4 criteria voor selectie van penetratietester

38 https://en.wikipedia.org/wiki/Security_AppScan

39 https://nl.wikipedia.org/wiki/HP_WebInspect

40 https://www.acunetix.com/

41 https://nl.wikipedia.org/wiki/Nessus_%28software%29

42 https://www.rapid7.com/products/nexpose/

Bijlage 3: Voorbeeld overeenkomst inzake een regeling van aansprakelijkheid met betrekking tot de uitvoering van een penetratietest

De ondergetekenden:

1. <*naam gemeente*>, ingeschreven in het Handelsregister onder nummer *[invullen]* te dezen rechtsgeldig vertegenwoordigd door de heer/mevrouw <*naam verantwoordelijke*>, Hoofd <*naam afdeling>,* hierna te noemen: de Opdrachtgever.

en

2. <*naam Pentest organisatie*>, statutair gevestigd te <*gemeente inschrijving KvK*>, ingeschreven in het Handelsregister onder nummer [*invullen*] te dezen rechtsgeldig vertegenwoordigd door de heer/mevrouw <*naam verantwoordelijke*>, hierna te noemen: de Uitvoerder.

en

3. <*Naam te onderzoeken gemeente en/of eventueel te onderzoeken leverancier (s)*>, (optioneel, indien externe leverancier: gevestigd te <*gemeente inschrijving KvK*>,) ingeschreven in het Handelsregister onder nummer [*invullen*] te dezen rechtsgeldig vertegenwoordigd door de heer/ mevrouw <*naam verantwoordelijke*>, Directeur <*naam leverancier*>, hierna te noemen: de Onderzochte Partij.

Overwegende dat:

- Het beheer van het <naam van het te onderzoeken systeem> is ondergebracht bij de Onderzochte Partij.
- De Opdrachtgever in het kader van de informatiebeveiliging van <naam gemeente> een penetratietest (hierna te noemen: Pentest) wenst uit te laten voeren bij de Onderzochte Partij.
- Het doel van de Pentest is om:
  1. Inzicht te krijgen in de risico's en kwetsbaarheden van de te onderzoeken systemen.
  2. De beveiliging ervan te verbeteren.
- De Uitvoerder voldoende kennis heeft genomen van de behoefte en doelstellingen van Opdrachtgever en de opdracht.
- De in het kader van de pentest door de Uitvoerder te verrichten werkzaamheden mogelijkerwijs schade tot gevolg zouden kunnen hebben.
- De Pentest alleen kan geschieden met toestemming van Opdrachtgever en de Onderzochte Partij.
- Deze overeenkomst een vrijwaring bevat ten behoeve van de Uitvoerder tegen eventuele aansprakelijkheden, anders dan aansprakelijkheid ten gevolge van het niet vakkundig of anderszins verrichten van de overeengekomen werkzaamheden.
- Partijen hun afspraken in verband met de uitvoering van de Pentest in deze overeenkomst wensen vast te leggen.

Zijn het volgende overeengekomen:

Artikel 1 Voorwerp van de overeenkomst

1. Uitvoerder verbindt zich tot het verrichten van de prestaties zoals beschreven in deze overeenkomst, die op hoofdlijnen bestaan uit:

a. Het uitvoeren van een Pentest.
b. Het rapporteren over de resultaten van Pentest.
c. Het verrichten van overige diensten die noodzakelijk zijn in het kader van de onderhavige opdracht.

Deze opdracht heeft het karakter van een resultaatsverbintenis aan de zijde van Uitvoerder.

2. De navolgende stukken maken integraal onderdeel uit van de overeenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerder genoemde stuk boven het later genoemde:

I. Dit document
II. De offerteaanvraag van Opdrachtgever d.d. [datum]
III. [Optioneel: de toepasselijke inkoopvoorwaarden van Opdrachtgever]
IV. De offerte van Uitvoerder d.d. [datum]

3. Indien op grond van een lager gerangschikt document hogere eisen aan de prestaties worden gesteld, gelden steeds die hogere eisen. Tenzij in het hoger gerangschikte document is aangegeven dat, en ten aanzien van welk specifiek onderdeel, van het lager gerangschikte document wordt afgeweken.

4. Partijen voeren de opdracht uit volgens het bepaalde in deze overeenkomst. Uitvoerder zal zijn werkzaamheden, overeenkomstig de in de offerteaanvraag opgenomen planning, verrichten en op de nader door Opdrachtgever aangeduide momenten.

5. De door Opdrachtgever aan Uitvoerder te betalen vergoeding, wijze van factureren en de overige financiële afspraken zijn vastgelegd in de offerte.

Artikel 2 Uitvoering van de opdracht

1. Opdrachtgever zal de Onderzochte Partij vooraf informeren over de periode waarin de Pentest zal plaatsvinden. De Uitvoerder zal pas van start gaan met het uitvoeren van de Pentest na instemming van de Onderzochte Partij. De Uitvoerder zal zich, buiten de in de offerteaanvraag overeengekomen periode, onthouden van onderzoeken bij de Onderzochte Partij.

2. De Uitvoerder zal de Onderzochte Partij benaderen vanaf een IP-nummer dat wordt medegedeeld aan de Onderzochte Partij.

3. De personen die de contacten over de uitvoering van de overeenkomst onderhouden zijn voor:

Opdrachtgever	: [*invullen*]
Onderzochte partij	: [*invullen*]
Uitvoerder	: [*invullen*]

4. Uitvoerder staat ervoor in dat Opdrachtgever en de Onderzochte Partij altijd en onmiddellijk contact kunnen opnemen met de door Uitvoerder in het voorgaande lid aangewezen contactpersoon.

5. Op eerste verzoek van Opdrachtgever of de Onderzochte Partij (gericht aan de contactpersoon van de Uitvoerder) zal de Uitvoerder de uitvoering van de Pentest onmiddellijk staken. De Onderzochte Partij doet dit verzoek aan Uitvoerder niet eerder dan nadat dit, met redenen omkleed, is afgestemd met de Opdrachtgever en Opdrachtgever hiermee heeft ingestemd.

6. De Uitvoerder verklaart dat hij bij het uitvoeren van de Pentest als een professionele, zorgvuldige en vakbekwame dienstverlener te werk zal gaan.
Dit betekent onder meer dat de Uitvoerder gebruik zal maken van gekwalificeerd personeel en enkel geschikte middelen ter uitvoering van de Pentest zal inzetten in overeenstemming met geldende standaarden, zoals:

- Open Web application Security Project (OWASP).
- SysAdmin, Audit, Network, Security (SANS).
- National Institute of Standards and Technology (NIST).
- Information Systems Security Assessment Framework (ISSAF).
- Open Source Security Testing Methodology Manual (OSSTMM)

7. De Uitvoerder handelt in overeenstemming met de schriftelijke opdrachtbeschrijving van Opdrachtgever zoals neergelegd in de offerteaanvraag en in overeenstemming met de geldende ethische standaarden/gedragsregels conform de Code of Ethics van ISC.

Artikel 3 Verwerkersovereenkomst
1. Bij de uitvoering van de Pentest zal de Uitvoerder zoveel als mogelijk vermijden om persoonsgegevens te verwerken. Dit kan echter niet worden uitgesloten door de Uitvoerder.

2. De Opdrachtgever is de verantwoordelijke voor de gegevensverwerking in de zin van de Wet Algemene Verordening Gegevensbescherming (AVG)

3. De Uitvoerder verbindt zich, om in het kader van de verwerking van persoonsgegevens alsook andere gegevens waarmee hij in aanraking komt, de Wbp na te leven en onder meer de (persoons)gegevens van de Onderzochte Partij, als verwerker in de zin van de Wbp behoorlijk en zorgvuldig te verwerken. In dit kader zal de Uitvoerder de (persoons)gegevens slechts in opdracht van de Opdrachtgever verwerken en deze adequaat beveiligen en technische en organisatorische maatregelen treffen tegen enige vorm van onrechtmatige verwerking.

4. Uitvoerder stelt Opdrachtgever in staat te controleren dat de verwerking van de (persoons)gegevens door Uitvoerder plaatsvindt zoals overeengekomen. Uitvoerder zal eventuele beveiligingsincidenten onverwijld schriftelijk aan Opdrachtgever melden.

5. De Opdrachtgever en de Onderzochte Partij zullen zorgdragen voor een volledige back-up van alle gegevens die op haar computernetwerken en/of systemen zijn opgeslagen.

6. Het personeel van de Opdrachtgever en de Onderzochte Partij zal over een procedure en middelen beschikken om de back-up gegevens, in het geval van calamiteiten, zo snel mogelijk op de desbetreffende systemen terug te zetten.

7. De Uitvoerder stelt de Opdrachtgever en Onderzochte Partij te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp.

8. De Uitvoerder zal te allen tijde op eerste verzoek van de Opdrachtgever onmiddellijk alle van de Onderzochte Partij, afkomstige en/of in opdracht van de Onderzochte Partij verwerkte gegevens met betrekking tot deze overeenkomst aan de Opdrachtgever ter hand stellen.

9. De Uitvoerder zal te allen tijde op eerste verzoek van de Opdrachtgever onmiddellijk alle afschriften en kopieën van de Onderzochte Partij, afkomstige en/of in opdracht van de Onderzochte Partij verwerkte gegevens met betrekking tot de Onderzochte Partij vernietigen.

10. De Uitvoerder zal bij het decharge verlenen van de opdracht door de Opdrachtgever onmiddellijk alle afschriften en kopieën van de Onderzochte Partij afkomstige en/of in opdracht van de Onderzochte Partij verwerkte gegevens met betrekking tot de Onderzochte Partij vernietigen.

11. Alle informatie en gegevens die tussen de Uitvoerder, Opdrachtgever en Onderzochte Partij worden uitgewisseld, of waarvan kennis genomen wordt, worden als vertrouwelijk behandeld door alle partijen. De partij die vertrouwelijke informatie ontvangt, zal van deze informatie slechts gebruik maken voor het doel waarvoor deze verstrekt is en deze informatie niet aan derden verstrekken of kenbaar maken. Tenzij schriftelijk anders overeengekomen wordt tussen partijen dan wel dat er een wettelijke verplichting tot openbaarmaking van deze informatie is.

Artikel 4 Beschikbaar stellen van onderzoeksresultaten
1. De resultaten van de Pentest worden door de Uitvoerder, door middel van een rapportage, na afstemming van de concept rapportage door de Opdrachtgever met de Onderzochte Partij en de Uitvoerder, ter beschikking gesteld aan de Opdrachtgever. Opdrachtgever is gerechtigd het rapport aan derden ter beschikking te stellen, waaronder auditors. Op verzoek van Opdrachtgever zal Uitvoerder ten behoeve van auditors inzicht bieden in scoping, aanpak, tooling, diepgang en uitkomsten van het rapport.

2. De rapportage bevat minimaal de informatie zoals benoemd in de offerteaanvraag en minimaal die informatie die noodzakelijk is in het kader van <*naam assessment*>.

3. Indien tijdens de uitvoering van de Pentest blijkt dat sprake is van beveiligingsincidenten, meldt de Uitvoerder deze onmiddellijk bij de contactpersoon van Opdrachtgever, vergezeld van een voorgestelde oplossing om het incident zo spoedig mogelijk te kunnen verhelpen. Van een incident is ook sprake indien Uitvoerder constateert dat hij data of settings kan aanpassen.

Artikel 5 Toestemming
1. De Opdrachtgever en Onderzochte Partij geven de Uitvoerder hierbij toestemming tot het uitvoeren van een Pentest op de ICT-systemen, zoals nader omschreven in de offerteaanvraag.

2. De reikwijdte en het object van de Pentest zijn beschreven in de offerteaanvraag. Opdrachtgever en Onderzochte Partij laten Uitvoerder vrij in de wijze waarop deze zal proberen de in de offerteaanvraag beschreven computernetwerken en/of systemen binnen te dringen, dan wel gegevens aan deze computernetwerken en/of systemen te onttrekken. Met uitzondering van methoden die de voornoemde systemen en aangeboden diensten onbereikbaar maken zoals denial of service-attacks. Evenmin is het de Uitvoerder toegestaan om wijzigingen aan te brengen in de systemen en data die hij aantreft, zodra hij in de systemen is binnengedrongen.

3. Uitvoerder garandeert dat hij enkel werkzaamheden uitvoert die binnen de reikwijdte van de opdrachtomschrijving vallen. De Uitvoerder zal alleen gegevens vastleggen of verwerken als dat voor bewijsvoering van de Pentest nodig is.

4. De Onderzochte Partij is zich ervan bewust dat de werkzaamheden van de Uitvoerder zijn gericht op het identificeren van kwetsbaarheden in de beveiliging van het geautomatiseerde werk, de gegevens, bedrijfsgebouwen of enig ander goed dat aan de Onderzochte Partij toebehoort. Met het oogmerk om doeltreffende maatregelen te kunnen treffen ten aanzien van deze kwetsbaarheden.

Artikel 6 Aansprakelijkheid Algemeen
1. Indien één der partijen tekort schiet in de nakoming van zijn verplichtingen uit deze overeenkomst, kan de andere partij hem in gebreke stellen. De nalatige partij is echter onmiddellijk in verzuim als nakoming van de desbetreffende verplichtingen anders dan door overmacht binnen de overeengekomen termijn reeds blijvend onmogelijk is. De ingebrekestelling geschiedt schriftelijk, waarbij aan de nalatige partij een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen.
Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is de nalatige partij in verzuim.

2. De partij die toerekenbaar tekort schiet in de nakoming van zijn verplichtingen en/of onrechtmatig handelt jegens de andere partij, is tegenover de andere partij aansprakelijk voor de door de andere partij geleden dan wel te lijden schade.

3. De hierna genoemde beperkingen en uitsluitingen van aansprakelijkheid vinden geen toepassing, in geval van aanspraken van derden op schadevergoeding ten gevolge van dood of letsel, of indien sprake is van opzet of grove schuld aan de zijde van een partij en/of diens personeel.

<u>Aansprakelijkheid Opdrachtgever en Onderzochte Partij</u>
4. De aansprakelijkheid van Opdrachtgever en de Onderzochte Partij is uitgesloten voor de duur van de overeenkomst.

<u>Aansprakelijkheid Uitvoerder</u>
5. De Uitvoerder is niet aansprakelijk voor schade die ontstaat als gevolg van diens werkzaamheden op grond van deze overeenkomst, mits de desbetreffende aanspraak betrekking heeft op werkzaamheden die vallen binnen de reikwijdte van de Pentest, en de desbetreffende werkzaamheden zijn verricht conform het bepaalde in deze Overeenkomst. Opdrachtgever en de Onderzochte Partij vrijwaren de Uitvoerder tegen aansprakelijkheden dienaangaande, met name ingeval een derde zich beroept op de artikelen 161sexies, 161septies, 351, 351bis, 138ab en 138b van het Wetboek van Strafrecht.

6. De vrijwaring als omschreven in het voorgaande artikellid geldt slechts indien, en voor zover is voldaan aan de daar genoemde voorwaarden en:

a. De Uitvoerder het feit dat hij door een derde in of buiten rechte is aangesproken onverwijld bij aangetekende brief meedeelt aan Opdrachtgever.
b. De Uitvoerder geen aansprakelijkheid jegens de derde erkent, niet afziet van verweer en ter zake van de aanspraak geen schikking aangaat, anders dan met de voorafgaande schriftelijke toestemming van Opdrachtgever.
c. De Uitvoerder het verweer tegen de aanspraak van de derde geheel overlaat aan Opdrachtgever en alle medewerking verleent om dat verweer te voeren.

7. Voor zover Uitvoerder wel aansprakelijk is, is de hoogte daarvan beperkt tot EUR [*invullen*] voor de duur van de overeenkomst.

Artikel 7 Geen vrijwaring voor wanprestatie

1. De vrijwaring als omschreven in artikel 6 lid 5 ziet niet op schade die is ontstaan door een toerekenbare tekortkoming bij het uitvoeren van deze Overeenkomst c.q. de pentest door de Uitvoerder dan wel bij opzet, bewuste roekeloosheid, ernstige verwijtbaarheid of een beroepsfout bij Uitvoerder.

Artikel 8 Looptijd en beëindiging van de overeenkomst

Looptijd

1. Deze overeenkomst treedt in werking op het moment van ondertekening door alle partijen en duurt voort totdat partijen aan hun, uit onderhavige overeenkomst voortvloeiende, verplichtingen hebben voldaan.

Tussentijdse opzegging

2. Opdrachtgever is gerechtigd door middel van een aangetekend schrijven aan Uitvoerder de overeenkomst tussentijds op te zeggen, met inachtneming van een opzeggingstermijn van een week. Opdrachtgever zal in geval van tussentijdse opzegging een redelijke vergoeding aan Uitvoerder voldoen.

3. De Uitvoerder en de Onderzochte Partij zijn niet gerechtigd tot tussentijdse opzegging van de overeenkomst.

Ontbinding

4. Buiten hetgeen elders in deze overeenkomst is bepaald is:

a. Ieder der partijen gerechtigd de overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang, zonder rechterlijke tussenkomst, geheel of gedeeltelijk te ontbinden. Dit indien de andere partij ook na een aangetekende schriftelijke sommatie waarin een redelijke termijn is gesteld (welke nooit meer zal bedragen dan 30 dagen), in gebreke blijft aan zijn verplichtingen uit de overeenkomst te voldoen.
b. Opdrachtgever gerechtigd zonder dat enige sommatie of ingebrekestelling en zonder dat rechterlijke tussenkomst zal zijn vereist, de overeenkomst door middel van een aangetekend schrijven geheel of gedeeltelijk te ontbinden. Dit indien Uitvoerder (voorlopige) surseance van betaling aanvraagt of hem (voorlopige) surseance van betaling wordt verleend, Uitvoerder zijn faillissement aanvraagt of in staat van faillissement wordt verklaard, de onderneming van Uitvoerder wordt geliquideerd, Uitvoerder zijn huidige onderneming staakt, op een aanmerkelijk deel van het vermogen van Uitvoerder beslag wordt gelegd, dan wel dat Uitvoerder anderszins niet langer in staat moet worden geacht de verplichtingen uit deze overeenkomst na te kunnen komen.

5. Beëindiging van de overeenkomst ontslaat partijen niet van verplichtingen daaruit, die naar hun aard doorlopen. Tot deze verplichtingen behoren in ieder geval: garanties, aansprakelijkheid en vrijwaring, geheimhouding, vernietiging van verzamelde gegevens, geschillen en toepasselijk recht.

Artikel 9 Algemeen

1. De toepasselijkheid van algemene en bijzondere voorwaarden van Uitvoerder of de Onderzochte Partij dan wel derden, is uitgesloten, tenzij partijen expliciet schriftelijk anders overeenkomen.

2. Partijen maken het bestaan en de inhoud van de overeenkomst alsmede hetgeen hen bij de uitvoering van de overeenkomst ter kennis komt en waarvan zij het vertrouwelijk karakter kennen of redelijkerwijs kunnen vermoeden op geen enkele wijze verder bekend. Tenzij enig wettelijk voorschrift of een onherroepelijke uitspraak van de rechter hen tot bekendmaking daarvan verplicht. Bekendmaking vindt in laatstgenoemd geval plaats in overleg met de andere partij en op een zodanig manier dat de belangen van die andere partij daardoor zo min mogelijk worden geschaad.

3. Uitvoerder is niet gerechtigd rechten en verplichtingen uit de overeenkomst zonder voorafgaande schriftelijke toestemming van Opdrachtgever aan een derde over te dragen.

4. Indien Uitvoerder bij de uitvoering van de opdracht gebruik wil maken van (de diensten van) derden, hetzij in onderaanneming, hetzij door tijdelijke inhuur van personeel. Dan is hij daartoe slechts bevoegd na daartoe verkregen schriftelijke goedkeuring van Opdrachtgever, welke goedkeuring niet op onredelijke gronden zal worden onthouden.

5. Uitvoerder zal zich voor de duur van de overeenkomst adequaat verzekeren en zich adequaat verzekerd houden ter zake van contractuele en wettelijke aansprakelijkheidsrisico's die voortvloeien uit de overeenkomst.

Artikel 10 Toepasselijk recht en geschillen
1. Op deze overeenkomst en alle daaruit voortvloeiende gevolgen is Nederlands recht van toepassing. Geschillen inzake deze overeenkomst en de uitvoering daarvan worden voorgelegd aan de bevoegde rechter te Den Haag.

Aldus op de laatste van de 3 hierna genoemde data overeengekomen en in drievoud ondertekend:

Namens de Opdrachtgever, genoemd onder 1,
Naam : [*invullen*]
Functie : [*invullen*]
Datum : [*invullen*]
Plaats : [*invullen*]

Namens de Uitvoerder, genoemd onder 2,
Naam : [*invullen*]
Functie : [*invullen*]
Datum : [*invullen*]
Plaats : [*invullen*]

[Optioneel indien de gemeente niet tevens de onderzochte partij is. NB: indien er meerdere te onderzoeken partijen zijn, dan kunnen deze hier meetekenen (nr. 4 en verder)]

Namens de Onderzochte Partij, genoemd onder 3,
Naam : [*invullen*]
Functie : [*invullen*]
Datum : [*invullen*]
Plaats : [*invullen*]

Bijlage 4: Voorbeeld verbeterplan

Nr.	Beschrijving	Prioriteit	Doelstelling	Bewijsvoering	Wie is verantwoordelijk	(verwachte) Datum klaar	Status
1	Bijvoorbeeld: Inzicht krijgen en houden in de mate waarin een (web)applicatie weerstand kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van een webapplicatie).	Bijv. • High • Medium • Low	Bijvoorbeeld: • Planning • Opdrachtomschrijving(en) met daarin een heldere onderzoeksvraag • Scopedefinitie(s) met daarin het object van onderzoek • Rapportageformat met daarin duidelijk vastgelegd welke informatie de rapportage moet bevatten • Rapportages met de resultaten van de penetratietest(s)	Bijvoorbeeld: • Tijd tussen penetratietesten op dezelfde server • Tijd tussen resultaten penetratietest en oplossen bevindingen • Risico acceptatie overzicht	Bijvoorbeeld: Gemeente en/of software ontwikkelaar en/of hostingpartij	Bijvoorbeeld: 1-1-2015	Bijvoorbeeld: Open of afgerond
2							
3							

Tabel 5 voorbeeld verbeterplan

Bijlage 5: Definities

Blackbox:

Bij een blackboxtest krijgt het penetratietestteam geen informatie en geen toegang tot het interne computernetwerk zodat deze test de aanval van een Hacker of Cracker zoveel mogelijk benaderd. Het penetratietestteam moet alles zelf ontdekken. Hierdoor neemt de test ook veel meer tijd in beslag en levert waarschijnlijk minder resultaten op.

Greybox:

Een greyboxtest is een mix van een blackbox en een whitebox penetratietest. Bij deze test krijgt het penetratietestteam toegang tot het interne computernetwerk, informatie over de infrastructuur en de applicaties.

Hacken:

Met een hack wil een persoon zwakke plekken aantonen dat computerprogramma's en –computernetwerken (nog) niet veilig zijn. Dit kan met kwade (criminele) bedoelingen of zonder er verder misbruik van te maken.

Pentest:

Een penetratietest of pentest is een check van één of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om op deze systemen in te breken (mits er een representatieve testomgeving beschikbaar is om dit inbreken op uit te voeren zonder risico voor de productieomgeving). Een penetratietest vindt normaal gesproken om legitieme redenen plaats, met toestemming van de eigenaars van de systemen die gecheckt worden. Met als doel de systemen (nog) beter te beveiligen.

Vrijwaringsverklaring:

Een vrijwaringsverklaring is een document dat de betrokken partijen bij de penetratietest moeten ondertekenen. In dit document wordt vastgelegd dat de partijen de pentester toegang verlenen tot hun systemen. Het document vrijwaart de pentester van juridische aansprakelijkheid op eventueel aangebrachte schade.

Vulnerability scan:

Dit is een scan die zich richt op het checken van de hardening en patching van systemen en het detecteren van mogelijke kwetsbaarheden van deze systemen.

Whitebox:

Bij een whiteboxtest krijgt het penetratietestteam alle informatie over applicaties en infrastructuur voor aanvang van de penetratietest. Ook gebruikersnamen en wachtwoorden worden aan het testteam gegeven. Onderdeel van de afspraak kan zelfs zijn dat inzicht in de source code van applicaties wordt gegeven. Bij dit soort testen wordt nauw samen gewerkt met de opdrachtgever om dieper inzicht te krijgen in de logica van de infrastructuur en applicaties. Deze test wordt uitgevoerd vanaf het interne computernetwerk en de testresultaten zijn meestal meeromvattend dan bij de andere tests

Bijlage 6: Literatuur / bronnen

Voor deze publicatie is gebruik gemaakt van onderstaande bronnen:

Titel: Whitepaper Securitytesten
Wie: Nationaal Cyber Security Centrum (NCSC)
Datum: 30 maart 2020
Link https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten

Titel: Whitepaper Pentesten doe je zo
Wie: Nationaal Cyber Security Centrum (NCSC)
Datum: 15 juni 2010
Link: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/pentesten-doe-je-zo

Titel: Diverse documenten met betrekking tot de ondersteuning ICT-Beveiligingsassessment DigiD
Wie: Informatiebeveiligingsdienst voor gemeenten (IBD)
Datum: 2013
Link: https://www.informatiebeveiligingsdienst.nl/ en https://community.informatiebeveiligingsdienst.nl/

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie