Handreiking Penetratietesten

Colofon

De tekst in deze handreiking is gebaseerd op het document Handreiking Penetratietesten v2.2, die door de Informatiebeveiligingsdienst (IBD) is opgesteld en beschikbaar gemaakt voor gemeenten. De teksten in deze handreiking zijn met toestemming van IBD aangepast en geschikt gemaakt voor de VVT door ActiZ. Voor gebruik en delen van het materiaal, verveelvoudiging, verspreiding en gebruik van dit materiaal verwijzen wij naar de Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) als bronmateriaal van de inhoud.

Inhoudsopgave

[1. Inleiding 4](#_Toc73611720)

[1.1. Aanwijzing voor gebruik 4](#_Toc73611721)

[2. Aandachtspunten Penetratietesten 4](#_Toc73611722)

[3. Uitvoeren penetratietest 5](#_Toc73611723)

[3.1. Stap 1 Penetratietest voorbereiden 5](#_Toc73611724)

[3.2. Stap 2 Penetratietest uitvoeren 5](#_Toc73611725)

[3.3. Stap 3 Bevindingen penetratietest oplossen 5](#_Toc73611726)

[3.4. Checklist uitvoeren penetratietesten 6](#_Toc73611727)

[3.5. Proces penetratietest integreren in de PDCA-cyclus 7](#_Toc73611728)

[4. Vrijwaringsverklaring penetratietest 7](#_Toc73611729)

[Bijlage 1: Draaiboek uitvoeren penetratietest 8](#_Toc73611730)

[Bijlage 2: Voorbeeld overeenkomst uitvoering van een penetratietest 12](#_Toc73611731)

# Inleiding

Met een penetratietest ook wel pentest genoemd, krijg je inzicht in de status en effectiviteit van je beveiligingsmaatregelen. Het resultaat geeft aan wat de aandachtsgebieden zijn en biedt concrete handvatten voor goede maatregelen om de beveiligingsrisico’s te verminderen. Een penetratietest kan ook worden ingezet als onderdeel van een campagne om de bewustwording van de medewerkers te verhogen.

### Voordelen

* Tijdens oplevering of bij grote wijzigingen kan een penetratietest kwetsbaarheden opsporen. Daarmee controleer en verhoog je de kwaliteit en het beveiligingsniveau van je systemen en processen.
* Je controleert hoe goed je gegevens beschermd zijn tegen aanvallen en het geeft een diepgaand en compleet overzicht van het beveiligingsniveau van je ICT-infrastructuur. Penetratietesten zijn dan ook een middel om de kwaliteit van je digitale bescherming aan te tonen.
* Met de resultaten van de penetratietesten kun je je risicomanagement updaten. Daarmee krijg je zicht op de belangrijke risico’s van beveiligingslekken en verminder je deze risico’s.

## Aanwijzing voor gebruik

In deze handreiking geven we je aandachtspunten voor het uitvoeren van penetratietesten. Deze handreiking is geen volledige procesbeschrijving, maar bevat handvatten om goede (beleids)keuzes te maken.

# Aandachtspunten Penetratietesten

Een manier om de kwaliteit van de digitale bescherming van je organisatie te bewijzen is om te proberen in je ICT-omgeving binnen te dringen. Dit heet een penetratietest. Hierbij kan gebruik worden gemaakt van verschillende methoden en technieken. 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 infrastructuur van de organisatie. Externe aanvallen zijn pogingen om binnen te dringen vanaf een willekeurige computer buiten de infrastructuur van de organisatie.

Alle vormen van penetratietesten kunnen worden uitgevoerd op verschillende lagen in het systeem, zowel op de infrastructuur- als op de applicatielaag. De infrastructuurlaag zijn de servers, besturingssystemen, netwerkapparatuur en beveiligingscomponenten (Bijvoorbeeld: firewalls, intrusion detection systems (IDS)[[1]](#footnote-1), 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.

### Wanneer uitvoeren

Het is wenselijk om periodiek een penetratietest uit te voeren. Bijvoorbeeld tweejaarlijks om bestaande systemen te testen op nieuwe inbraaktechnieken en ‘exploits’. En als onderdeel van het Information Security Management System (ISMS). Andere redenen om een penetratietest uit te voeren, zijn wijzigingen in het systeem of maatregelen, en de acceptatiefase van een nieuw systeem of een nieuwe applicatie.

### Ketenpartijen

Denk bij het uitvoeren van een penetratietest ook aan het bijzondere karakter van het werken in ketenverband. Wanneer je in een keten samenwerkt, test je niet alleen de eigen infrastructuur (het eigen computernetwerk) maar ben je ook bedacht op effecten van die test naar de andere ketenpartijen. Bovendien is het nodig dat er specifieke tests worden uitgevoerd, waarin wordt geprobeerd om het gemeenschappelijke computernetwerk te penetreren vanuit, of via, het computernetwerk van een ketenpartij.

### Vulnerability scan

Naast penetratietesten kun je ook gebruik maken van vulnerability scans. Deze scans zijn 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 probeert niet de systemen verder binnen te dringen, waar een security tester dat bij een penetratietest wel zou doen. Dit is handig voor snelheid of wanneer er zeer kritieke objecten onderzocht worden waarbij men niet verder wil testen dan de oppervlakte.

# Uitvoeren penetratietest

De stappen voor penetratietesten staan hier kort toegelicht. In bijlage 1 staat een draaiboek als praktisch hulpmiddel voor degene die verantwoordelijk is voor het uitvoeren van de penetratietest.

## Stap 1 Penetratietest voorbereiden

Zorg bij de voorbereiding dat er toestemming is van de juiste personen, vooral als er ook ketenpartijen betrokken zijn. De whitepaper securitytesten [[2]](#footnote-2) van het Nationaal Cyber Security Centrum (NCSC) biedt een handleiding die tips geeft voor de offerteaanvraag en welke elementen ten minste in de offerteaanvraag te beschrijven.

## Stap 2 Penetratietest uitvoeren

De pentest uitvoerder gaat aan de slag met de test en probeert het systeem te ‘hacken’. Denk eraan dat door alle betrokken partijen een vrijwaringsverklaring getekend is, voordat de penetratietest uitgevoerd wordt. De uitvoerder van de pentest rapporteert de bevindingen van de pentest aan de opdrachtgever.

## Stap 3 Bevindingen penetratietest oplossen

Vervolgens stel je op basis van de bevindingen uit de penetratietest een verbeterplan op. Hierover maak je afspraken met interne en externe partijen. In het verbeterplan met prioriteitenstelling worden acties (maatregelen) naar aanleiding van een penetratietest opgenomen. Enkele voorbeelden:

* Het aanbrengen van configuratieaanpassingen.
* Het inzetten van extra beveiligingsapparatuur of -programmatuur (bijvoorbeeld firewalls).
* Het aanpassen van procedures en werkvoorschriften.
* Et cetera.

## Checklist uitvoeren penetratietesten

Onderstaande vragenlijst kun je gebruiken om het proces van de penetratietesten te checken. Deze vragenlijst is zeker niet volledig, maar geeft ideeën om een eerste inschatting 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 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 zorgorganisatie 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?

## Proces penetratietest integreren in de PDCA-cyclus

De zorgorganisatie (of eventueel een ingehuurde auditor) zal de penetratietest beoordelen. Hierbij dient vastgesteld te worden of de pentest voldoet aan de eisen die vooraf zijn gesteld. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid. De aanpak voor het beoordelen van de resultaten van penetratietesten is gebaseerd op de bekende PDCA-cyclus:

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 en uitgevoerd (Act)?

# Vrijwaringsverklaring penetratietest

In bijlage 2 staat een voorbeeld overeenkomst om de vrijwaringsverklaring te regelen. De penetratietester voert een penetratietest uit op verzoek van een organisatie. Omdat de penetratietester werkzaamheden verricht die strikt genomen niet legaal zijn (binnendringen van ICT-systemen) en tot aansprakelijkheid kunnen leiden, moet de opdrachtgever de tester vrijwaren. De Overeenkomst bevat een vrijwaringsverklaring (artikel 6, lid 5).

De pentest wordt uitgevoerd bij jouw organisatie, daarom ben je zowel ‘opdrachtgever’ als ‘onderzochte partij’. De zorgorganisatie moet in dit geval dus vanuit beide rollen tekenen voor de vrijwaring. Als de pentest ook bij externe partijen wordt uitgevoerd, zoals een SaaS-dienstverlener, 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).

# Bijlage 1: Draaiboek uitvoeren penetratietest

Dit voorbeeld draaiboek biedt handvatten voor een planning van de te ondernemen acties en de monitoring van de voortgang van de test. Het doel van dit voorbeeld is om ideeën te geven per stap waaraan de denken.

**Voorbereiding**

| **Nr.** | **Activiteit** | **Omschrijving** | **Beoogde resultaat** |
| --- | --- | --- | --- |
| 1 | Scope vaststellen | 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 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 worden: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.
1. 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.
1. Een omschrijving van de informatie die de opdrachtgever aan de pentester ter beschikking zal stellen voorafgaand aan de pentest (blackbox-, whitebox-, greybox-test).
* 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.
1. Welke technieken bij de penetratietest zullen worden gebruikt. Bijvoorbeeld: phishing[[3]](#footnote-3), systeem en/of protocol hacks, database aanvallen (bijvoorbeeld: SQL-injectie[[4]](#footnote-4)), trojaanse paarden[[5]](#footnote-5), backdoors[[6]](#footnote-6), sniffers[[7]](#footnote-7), Denial of Service (DoS)[[8]](#footnote-8), hijacking (bijvoorbeeld: sessie[[9]](#footnote-9) of browser[[10]](#footnote-10)), privilege escalatie[[11]](#footnote-11) en bufferoverflows[[12]](#footnote-12).[[13]](#footnote-13)
2. Een planning, inclusief de momenten waarop er niet getest mag worden.
3. 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)[[14]](#footnote-14).
4. De offerteaanvraag dient op het juiste niveau goedgekeurd te worden. Bijvoorbeeld door een bestuurder of manager.
 | De offerteaanvraag is opgesteld en goedgekeurd. |
| 3 | Communicatie vaststellen | Bepaal wie binnen de organisatie geïnformeerd moet worden over deze pentest. Bedenk of het noodzakelijk is om de afdeling communicatie te betrekken. 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. Over het algemeen wil je zo weinig mogelijk mensen op de hoogte brengen van de pentest om deze realistisch te houden. Het voordeel is dat er 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. | Er is een vastgesteld wie geïnformeerd dienen te worden over deze 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 | Zorg voor een vrijwaringverklaring die door betrokken partijen is ondertekend.  | De vrijwaringsverklaring(en) zijn ondertekend door alle juiste partijen (Zie bijlage 1: Voorbeeld overeenkomst) |

**Uitvoeren**

| **Nr.** | **Activiteit** | **Omschrijving** | **Resultaat** |
| --- | --- | --- | --- |
| 1 | Voer de pentest uit. | Voer de pentest uit volgens alle gemaakte afspraken en houdt tijdens de uitvoering de verantwoordelijk bestuurder of manager en de CISO op de hoogte 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 moeten vastgelegd worden. Vervolgens ga je op basis van een risicoafweging vaststellen welke bevindingen wel en welke bevindingen niet acceptabel zijn. Deze risicoafweging maak je volgens de afgesproken werkprocessen met de systeemeigenaar (de verantwoordelijke) van het te onderzoeken object en de CISO.In de rapportage staan de volgende onderdelen:* Beschrijving beveiligingslek en risicoclassificatie.
* Hoe is de constatering van het beveiligingslek gedaan.
* Hoe kan het beveiligingslek gereproduceerd worden.
* Details beveiligingslek, niet alleen technisch maar ook in begrijpbare taal.
* Indien bekend, verbetervoorstellen. Bijvoorbeeld oplossing of workaround.

Stel de rapportage zo op dat deze met één of meer ketenpartijen kan worden besproken als dat nodig is. 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, waarvoor je een afweging maakt of deze wel of (nog) niet worden meegenomen. Geef per maatregel aan wie hiervoor verantwoordelijk is en wanneer de maatregel wprdt geïmplementeerd. Als een maatregel op basis van een risicoafweging toch niet wordt meegenomen vermeld je dit ook. | De noodzakelijke maatregelen zijn verwerkt in een verbeterplan.  |
| 4 | 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. |

Bijlage 2: Voorbeeld overeenkomst uitvoering van een penetratietest

Hieronder een voorbeeld voor een overeenkomst voor uitvering van een penetratietest. Hierin staan ook artikelen opgenomen over de vrijwaringsverklaring. Let op! Dit is geen voorbeeld om kant en klaar te gebruiken, maar dient als voorbeeld om aandachtspunten te zien.

**De ondergetekenden:**

**1.** *<naam organisatie>*, 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 organisatie 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 zorgorganisatie> 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:

1. Het uitvoeren van een Pentest.
2. Het rapporteren over de resultaten van Pentest.
3. 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:

1. Dit document
2. De offerteaanvraag van Opdrachtgever d.d. [datum]
3. [Optioneel: de toepasselijke inkoopvoorwaarden van Opdrachtgever]
4. 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.

Aansprakelijkheid Opdrachtgever en Onderzochte Partij

4. De aansprakelijkheid van Opdrachtgever en de Onderzochte Partij is uitgesloten voor de duur van de overeenkomst.

Aansprakelijkheid Uitvoerder

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:

1. De Uitvoerder het feit dat hij door een derde in of buiten rechte is aangesproken onverwijld bij aangetekende brief meedeelt aan Opdrachtgever.
2. 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.
3. 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:

1. 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.
2. 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 als er meerdere te onderzoeken partijen zijn, dan kunnen deze hier meetekenen]

**Namens de Onderzochte Partij, genoemd onder 3,**

Naam : [*invullen*]

Functie : [*invullen*]

Datum : [*invullen*]

Plaats : [*invullen*]

1. <https://nl.wikipedia.org/wiki/Intrusion_Detection_System> [↑](#footnote-ref-1)
2. <https://www.ncsc.nl/documenten/publicaties/2020/maart/30/whitepaper-securitytesten> [↑](#footnote-ref-2)
3. <https://nl.wikipedia.org/wiki/Phishing> [↑](#footnote-ref-3)
4. <https://nl.wikipedia.org/wiki/SQL-injectie> [↑](#footnote-ref-4)
5. <https://nl.wikipedia.org/wiki/Trojaans_paard_%28computers%29> [↑](#footnote-ref-5)
6. <https://nl.wikipedia.org/wiki/Achterdeurtje> [↑](#footnote-ref-6)
7. <https://nl.wikipedia.org/wiki/Packet_sniffer> [↑](#footnote-ref-7)
8. <https://nl.wikipedia.org/wiki/Denial-of-service> [↑](#footnote-ref-8)
9. <https://nl.wikipedia.org/wiki/Session_hijacking> [↑](#footnote-ref-9)
10. <https://en.wikipedia.org/wiki/Browser_hijacking> [↑](#footnote-ref-10)
11. <https://en.wikipedia.org/wiki/Privilege_escalation> [↑](#footnote-ref-11)
12. <https://nl.wikipedia.org/wiki/Bufferoverloop> [↑](#footnote-ref-12)
13. 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. [↑](#footnote-ref-13)
14. 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>). [↑](#footnote-ref-14)