Bijlage 2 - RVICTO 26 marktraadpleging | concept Programma van Eisen Pentesten

1 Algemeen

B2.1 Deelnemers kunnen aan Opdrachtnemer een opdracht verstrekken tot het uitvoeren van een informatiebeveiligingsonderzoek. Deelnemer en Opdrachtnemer bereiken dan overeenstemming over de scope, uitvoering en op te leveren eindresultaat van en eventueel te verlenen nazorg bij dit onderzoek. Het eindresultaat is in beginsel een (onderzoeks)rapportage, al dan niet voorzien van aanvullende documenten en/of toelichting. Het eindresultaat is betrouwbaar, reproduceerbaar en kan (optioneel) door Deelnemer of een derde partij (zoals een auditor) gevalideerd worden. De validatie kan uitgevoerd worden om extra zekerheid te verkrijgen over de kwaliteit van uitvoering en resultaten.

B2.2 Opdrachtnemer zal binnen de opdracht een (mondelinge) toelichting geven op het uitgevoerde onderzoek en hetgeen hij aan Deelnemer (in de vorm van een rapportage of anderszins) heeft opgeleverd, inclusief zijn bevindingen en adviezen. Opdrachtnemer staat hierbij open voor interactie met door Deelnemer aan te wijzen contactpersonen, die belang hebben bij de uitkomsten en eventuele opvolging van het onderzoek.

De onderzoeksrapportage wordt digitaal verstrekt.

B2.3 De (onderzoeks)rapportage wordt digitaal verstrekt. Deelnemer en Opdrachtnemer kunnen na aanvang van de opdracht nadere afspraken maken over zowel opzet van de rapportage, aanvullende te verstrekken documenten als wijze van verstrekking, mits deze rapportagevereisten niet strijdig zijn met dit Programma van eisen (zie eisen xxx e.v.).

Aanwijzing en beschrijving rapporteur, opsteller of hoofdonderzoeker

B2.4 In de op te leveren rapportage is de naam van een persoon (of meerdere personen) genoemd, die de professionele eindverantwoordelijkheid draagt (of dragen) voor de uitvoering van het informatiebeveiligingsonderzoek en de betreffende rapportage. Deze persoon (of personen) is (of zijn) in de rapportage als rapporteur(s) aangemerkt. Hiernaast vermeldt de rapportage de namen van de overige personen die betrokken zijn (geweest) bij de uitvoering van het onderzoek.

Beschrijving van de verplichte certificering, waarover de rapporteur beschikt

B2.5 De rapporteur(s) van het informatiebeveiligingsonderzoek beschikt/beschikken over relevante geldige certificering(en). Een relevante certificering genoemd in de meest recente versie van de lijst kwalificaties voor pentesters, als appendix van het CCV-keurmerk Pentesten, voldoet hieraan, zoals (maar niet uitsluitend):

- OffSec Certified Professional (OSCP)
- OffSec Experienced Pentester (OSEP)
- OffSec Offensive Security Certified Expert (OSCE of OSCE)
- OffSec Web Expert (OSWE)
- Web application Penetration Tester eXtreme (eWPTX)

De eisen die het CCV stelt aan trainingen en examens om erkend te worden als geldige certificering en passende kwalificatie voor pentesters, gelden ook hier:

1. Het certificaat geeft een goede indicatie dat de kandidaat beschikt over uitgebreide kennis en vaardigheden op het gebied van penetratietesten. Instapcertificaten kunnen niet aan deze criteria voldoen.

2. Om het certificaat te behalen, ondergaat de kandidaat een examen waarbij hij/zij minimaal 23 uur zelfstandig hackt in een labomgeving.

3. Na afloop van het examen stelt de kandidaat een rapport op dat daadwerkelijk wordt beoordeeld door een examinator.

4. Er zijn adequate maatregelen genomen om fraude tijdens het examen te voorkomen.

5. Er is minimaal 2 jaar een examen voor persoonscertificering voor pentesters beschikbaar om in aanmerking te komen voor deze lijst (voldoende trackrecord om aan de overige criteria te voldoen).

Proces van de Pentest Execution Standard volgen

B2.6 Het onderzoek wordt uitgevoerd volgens de zeven fasen van de Pentest Execution Standard (PTES) (http://www.pentest-standard.org/index.php/Main_Page) of, na acceptatie door Deelnemer, volgens fasen van een vergelijkbare erkende

	industriestandaard voor het uitvoeren van informatiebeveiligingsonderzoeken. De zeven fasen van PTES zijn: 1. Interacties vóór de betrokkenheid (Pre-engagement Interactions) 2. Informatie verzamelen (Intelligence Gathering) 3. Modellering van bedreigingen (Threat Modeling) 4. Kwetsbaarheidsanalyse (Vulnerability Analysis) 5. Exploitatie (Exploitation) 6. Post-exploitatie (Post Exploitation) 7. Rapportage (Reporting)
B2.7	Deelnemer kan, nadat opdrachtnemer het (initiële) onderzoek heeft uitgevoerd en de rapportage heeft opgeleverd, de aanbevelingen opvolgen en maatregelen treffen om de in de rapportage geconstateerde risico's te minimaliseren. Hierna kan Deelnemer aan opdrachtnemer vragen een herhalingsopdracht uit te voeren op eerder gevonden kwetsbaarheden of bevindingen. Hiermee beoogt Deelnemer uitsluitsel te krijgen of de maatregelen doeltreffend zijn doorgevoerd en de risico's tot een volgens Deelnemer acceptabel niveau zijn verminderd. Een herhalingsopdracht doorloopt dezelfde fasering. Opdrachtnemer voert op verzoek van Deelnemer de herhalingsopdracht uit. Een herhalingsopdracht kan als optie bij een initieel onderzoek worden overeengekomen en benut, maar kan ook op basis van een nieuwe Offerte van opdrachtnemer aan hem worden verstrekt.
B2.8	Als de opdracht een optie bevat tot het uitvoeren van een herhalingsopdracht afgesproken en Deelnemer wil daarvan gebruikmaken, dan kan Deelnemer zonder nadere competitie aan opdrachtnemer een timeboxed herhalingsopdracht verstrekken. De toepasselijke uurtarieven van opdrachtnemer op grond van de originele opdracht zijn hierop ook van toepassing, waarbij Deelnemer een maximum aantal te vergoeden uren en zodoende een vaste prijs voor uitvoering van de herhalingsopdracht voorschrijft. Opdrachtnemer mag de uitvoering van de deze herhalingsopdracht weigeren. Alsdan kan Deelnemer de Aanvraag voor het uitvoeren van een herhalingsopdracht gelijktijdig bij alle opdrachtnemers uitzetten met het verzoek hiervoor een (nieuwe) Offerte uit te brengen.
B2.9	Opdrachtnemer dient alle gegevens die hij verwerkt bij het onderzoek aantoonbaar adequaat te beveiligen, conform de relevante maatregelen uit de meest actuele versie van de BIO, ISO 27001/2 of gelijkwaardig. Indien Opdrachtnemer bij het onderzoek in aanraking kan komen met bijzondere (gerubriceerde) informatie die valt onder het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI) 2013 of gevoelige informatie die volgens Deelnemer een vergelijkbaar niveau van veiligheidsclassificatie krijgen, houdt hij zich aan de toepasselijke bindende voorschriften/voorwaarden die Deelnemer of een door Deelnemer aangewezen beveiligingsautoriteit hieraan stelt. Voor de maatregelen van veilige uitwisseling van gerubriceerde of gevoelige informatie zullen Deelnemer en Opdrachtnemer nadere (bindende) voorwaarden overeenkomen.
2 Interacties voor betrokkenheid (pre-engagement)	
B2.10	Opdrachtnemer garandeert dat hij uitsluitend werkzaamheden uitvoert die binnen de reikwijdte van de opdrachtomschrijving/scope van de Offerteaanvraag vallen. De intake die na start van de Nadere Overeenkomst plaatsvindt is niet bedoeld om de scope van de opdracht en de voorwaarden hieraan wezenlijk te wijzigen. In de intake kunnen Deelnemer en Opdrachtnemer nadere werkafspraken maken over de onderwerpen die al in de Aanvraag, de Nadere offerte of Nadere overeenkomst zijn beschreven, dan wel hier nog niet zijn beschreven maar verdere afstemming/detaillering behoeven.
Beschrijving intakegesprek	
B2.11	Het intakegesprek wordt uiterlijk op de 5e werkdag na start van de opdracht uitgevoerd, tenzij specifiek anders overeengekomen tussen Deelnemer en opdrachtnemer. Deze termijn start op de eerste werkdag nadat Deelnemer het verzoek bij opdrachtnemer heeft ingediend. Opdrachtnemer brengt hier geen separate kosten voor in rekening; deze kosten worden opgenomen in de tarieven of aanneemsom voor de uitvoering van de opdracht.
B2.12	Opdrachtnemer maakt een verslag van het intakegesprek. Dit verslag bevat de besproken onderwerpen die nodig zijn om een plan van aanpak te maken voor uitvoering van het onderzoek (zie eis xxx), de datum van het intakegesprek, de deelnemers aan het

intakegesprek en welke informatie er nog verstrekt moet worden voor het informatiebeveiligingsonderzoek.

B2.13 Voorafgaand aan het onderzoek, bijvoorbeeld in het intakegesprek, benoemen Deelnemer en Opdrachtnemer elkaars contactpersonen die met elkaar tijdens de uitvoering van de opdracht kunnen afstemmen, waarover en (indien van toepassing) onder welke voorwaarden. Indien van toepassing benoemt Deelnemer ook contactpersonen van rechthebbende derde partijen die voor het onderzoek relevant zijn.

Opdrachtnemer en Deelnemer bespreken voorafgaand aan het onderzoek eventuele door hen geziene risico's met betrekking tot de beschikbaar en/of deskundigheid en/of bevoegdheid van alle door partijen voorgestelde contactpersonen en kunnen waar gewenst mitigerende maatregelen nemen om beschikbaarheid en/of deskundigheid en/of bevoegdheid beter te borgen.

Deelnemers

Informatieverstrekking

B2.14 Na het intakegesprek levert opdrachtnemer een definitief voorstel plan van aanpak (PvA) op voor het uitvoeren van de gevraagde opdracht. Dit plan van aanpak kan worden gezien als 'rules of engagement'. Het definitieve plan van aanpak omvat ten minste:
- een omschrijving van de scope, doelstelling(en) van de opdracht, te onderzoeken objecten, eigenaarschap en fysieke locaties (land) van objecten inclusief gevolgen voor naleving relevante wet- en regelgeving. Optioneel (indien verzocht door Deelnemer): de locatie(s) van uitvoering van het onderzoek.
- te gebruiken methodiek(en), standaarden, aanvalsscenario's (op grond van eventuele applicatie- of klant specifieke (dreigings)scenario's) en toepassing van het "assume breach" principe
- een planning (w.o. datums/tijden/attack window van onderzoek), verwachte inzet en afspraken hierover
- voorwaarden en garanties van opdrachtnemer en/of deelnemer t.a.v. de planning
- afspraken over hoe om te gaan met eventuele risico's en incidenten die zich tijdens de uitvoering kunnen voordoen.

- overige voorwaarden voor uitvoering onderzoek
- namen van de rapporteur(s) en overige in te zetten professionals
- afspraken over communicatie tussen opdrachtnemer, deelnemer en eventuele derden
- afspraken over het versleutelen en het hashen van documenten/bestanden
- als bijlage het verslag van het intakegesprek

Het definitieve plan van aanpak dient door Deelnemer schriftelijk te worden goedgekeurd. Het plan van aanpak benoemt de uitgangspunten voor uitvoering van het onderzoek.

Scope

B2.15 Er is een beschrijving van de scope van het onderzoek. Deze bevat de relevante selectie van onderdelen en objecten (volgens sub 2.2.1 t/m 2.2.8). Opdrachtnemer verifieert in het intakegesprek of de scopebeschrijving overeenkomt met de behoeftes uit het intakegesprek en past binnen de afgesproken tijdspanne. Opdrachtnemer verwerkt nieuwe inzichten over de scope in het plan van aanpak.

Scope - Aanvalsperspectieven

B2.16 In de scopebeschrijving is opgenomen welk aanvalsperspectief is afgesproken, wat gevalideerd wordt door de Deelnemer en Opdrachtnemer. Opdrachtnemer voert op verzoek van Deelnemer een onderzoek uit op basis van blackbox, greybox of whitebox:
1. Black box: er worden vooraf geen gegevens beschikbaar gesteld over of toegang tot het te onderzoeken object. De test wordt uitgevoerd vanuit een ongeautoriseerd perspectief en benadert de realiteit van cyber criminelen het meest.
2. Grey box: er worden beperkte gegevens over de applicatie(s) en infrastructuur beschikbaar gesteld. Ook kunnen er (test) login credentials worden beschikbaar gesteld. De penetratietest wordt uitgevoerd vanuit het perspectief van iemand die normale toegang heeft (bemachtigd), waarbij geprobeerd kan worden buiten de gestelde kaders van dat account te treden.
3. White box: additionele gegevens over de applicatie(s) en infrastructuur worden beschikbaar gesteld. Ook kunnen er (test) login credentials worden beschikbaar gesteld.

	In het intakegesprek kunnen nadere afspraken gemaakt worden over het niveau van voorkennis.
Scope - Objecten	
B2.17	De objecten die onderzocht worden, zijn onderdeel van de scope. Indien een sprake is van een scope object met een specifiek versienummer dient deze te worden vastgelegd als onderdeel van het object. Per scope object wordt aangegeven conform welke bijbehorende kaders/standaarden onderzoek wordt gedaan (zie o.a. eisen XXX). Alle kaders/standaarden die van toepassing kunnen zijn op het betrokken object, zijn in de scopebeschrijving opgenomen.
Scopeonderdeel - Infrastructuur	
B2.18	-
Scopeonderdeel - Webapplicatie	
B2.19	Opdrachtnemer voert zijn opdrachten uit conform de meest recentelijk gepubliceerde standaarden, gerelateerd aan de objecten in de scope: - bij webapplicaties: OWASP Web Security Testing Guide (WSTG); - bij Internet of Things (IoT) apparaten: OWASP IoT Security Testing Guide (ISTG); - bij API: conform de standaard WSTG hoofdstuk 12 API Testing; - bij firmware: OWASP Firmware Security Testing Methodology (FSTM); - bij mobiele applicaties: OWASP Mobile Application Security Testing Guide (MASTG); Hiernaast conformeert Opdrachtnemer zich aan de Penetration Testing Execution Standard (PTES), tenzij anders overeengekomen. In het intakegesprek kunnen Deelnemer en Opdrachtnemer nadere afspraken maken over het gebruik van overige standaarden of referentiebronnen zoals de Google Hacking Database (GHDB), Open Source Security Testing Methodology Manual (OSSTMM), National Institute of Standards and Technology (NIST), Information System Security Assessment Framework (ISSAF), CIS-controls (Center for Internet Security), SOC2, Logius norm (voor DigiD), beveiligings- of beheersingsrichtlijnen van het NCSC.
Scopeonderdeel - IoT	
B2.20	-
Scopeonderdeel - Firmware	
B2.21	-
Scopeonderdeel - API	
B2.22	-
Scopeonderdeel - Mobiele Applicatie	
B2.23	-
Vaststelling scope en objecten	
B2.24	Alle binnen de scope vastgestelde objecten worden getest. Voorafgaand aan het onderzoek verifieert Opdrachtnemer bij Deelnemer of de objecten in een acceptatie-omgeving moeten worden getest en moeten worden gevalideerd in de productie-omgeving of dat direct in de productie-omgeving moet worden getest. De afspraken hierover worden vastgelegd in het plan van aanpak.
Eigenaarschap scope	
B2.25	Voorafgaand aan start van het onderzoek (bijvoorbeeld bij het intakegesprek) heeft opdrachtnemer geverifieerd dat de lijst aan objecten toebehoort aan de opdrachtgever (deelnemer) of toestemming is gegeven door de rechthebbende derde partij voor het uitvoeren van het onderzoek. Het proces en de verantwoordelijkheid om tijdig tot toestemming van de rechthebbende derde partij te komen, stemmen opdrachtnemer, deelnemer en eventueel deze derde partij indien nodig nader af, voorafgaan aan de uitvoering van het onderzoek. Indien deze rechthebbende derde partij nadere voorwaarden stelt, die noodzakelijk zijn om het onderzoek te kunnen uitvoeren, stemmen deelnemer, opdrachtnemer en deze derde partij af of en in hoeverre hieraan voldaan kan worden bij de uitvoering van het onderzoek. De afspraken hierover worden opgenomen in het plan van aanpak en de rapportage. Indien

opdrachtnemer en/of deelnemer besluiten zich niet aan deze nadere voorwaarden van de rechthebbende derde partij te kunnen of willen committeren, geeft dit het recht aan Deelnemer en opdrachtnemer om de betreffende opdracht eenzijdig te beëindigen.

Jurisdictie scope-objecten

B2.26 Voorafgaand aan start van het onderzoek (bijvoorbeeld bij het intakegesprek) stelt opdrachtnemer vast wat de fysieke locaties zijn van de te onderzoeken objecten en welke relevante wet- en regelgeving hier van toepassing is. De pentest wordt uitgevoerd volgens de aldaar van toepassing zijnde wet- en regelgeving.

B2.27 Opdrachtnemer voert op verzoek van Deelnemer het onderzoek uit vanaf een nader te benoemen externe en/of interne locatie (een door Deelnemer gebruikte locatie of vanaf een locatie van een rechthebbende derde partij).

Accordering scope

B2.28 Er is schriftelijke overeenstemming tussen een bevoegde functionaris van de opdrachtgever (deelnemer) en opdrachtnemer over het plan van aanpak, waaronder de uit te voeren scope van onderzoek.

Taal

B2.29 Voorafgaand aan start van het onderzoek (bijvoorbeeld bij het intakegesprek) heeft opdrachtnemer geverifieerd wat de taal van de rapportage moet zijn. De standaard is Nederlands.

Doel

B2.30 -

Vrijwaringsverklaring

B2.31 Opdrachtnemer, Deelnemer en eventueel nog derden (voor zover te onderzoeken objecten niet in eigendom van Deelnemer zijn) komen per Nadere overeenkomst een vrijwaringsverklaring overeen voor het uitvoeren van het informatiebeveiligingsonderzoek. Partijen kunnen hierbij gebruikmaken van het model in bijlage xx. In de vrijwaringsverklaring worden de risico's beschreven die het uitvoeren van het onderzoek met zich meebrengt, wordt toestemming gegeven voor aanval op / toegang tot bepaalde objecten en wordt vrijwaring van aansprakelijkheid met betrekking tot de uitvoering van het onderzoek nader geregeld. De Deelnemer draagt zorg voor afstemming met eventuele derden en ondertekening en retournering van de vrijwaringsverklaring aan opdrachtnemer voordat het onderzoek start. Een door bevoegde functionaris(sen) ondertekende vrijwaringsverklaring wordt dan onderdeel van de betreffende Nadere overeenkomst. Opdrachtnemer vangt niet aan met uitvoering van het onderzoek zonder schriftelijke goedkeuring door Deelnemer van genoemde documenten dan wel een afwijking hierop.

B2.32 In de Aanvraag kan Deelnemer eisen dat een door betrokken partijen getekende Verwerkersovereenkomst een noodzakelijke voorwaarde is voor het starten van de opdracht. Dat zal geëist worden als Opdrachtnemer bij de uitvoering van het onderzoek toegang kan krijgen tot persoonsgegevens.
Opdrachtnemer vangt dan niet aan met uitvoering van het onderzoek zonder een door betrokken partijen getekende Verwerkersovereenkomst.

B2.33 Deelnemer en opdrachtnemer kunnen voorafgaande aan het onderzoek overeenkomen hoe opdrachtnemer tijdens het uitvoeren van het onderzoek dient om te gaan met bevindingen die boven een nader te bepalen risiconiveau komen (wie dient waarover geïnformeerd te worden, wordt het onderzoek vervolgd of gestaakt). Dit wordt besproken in het intakegesprek en vastgelegd in het plan van aanpak. Opdrachtnemer adviseert Deelnemer hierbij desgewenst al direct (voorafgaand aan de rapportage) over effectieve maatregelen om de risico's (al dan niet tijdelijk) te mitigeren. Ook benoemt Opdrachtnemer welke risico's niet tijdelijk gemitigeerd kunnen worden.

3. Executieonderzoek

B2.34 Opdrachtnemer voert het onderzoek uit conform het definitieve plan van aanpak, waarbij een wederzijds overeengekomen latere versie bij tegenstrijdigheid prevaleert boven een eerdere versie. Deelnemer en Opdrachtnemer kunnen tijdens de uitvoering van het onderzoek aanpassingen op het plan van aanpak overeenkomen, mits deze ook expliciet worden vastgelegd en beargumenteerd in de rapportage. De aanpassingen mogen geen

wezenlijke wijzigingen zijn.
Kosten voor voorbereiding, uitvoering van het onderzoek conform een plan van aanpak, inclusief eventuele aanpassingen, en rapportage, zijn in redelijkheid en billijkheid integraal opgenomen in de in de Offerte voorgestelde prijs.

B2.35 Indien in het plan van aanpak is overeengekomen, informeert Opdrachtnemer vlak voordat het attack window van het onderzoek begint de hiervoor aangewezen contactpersoon/contactpersonen van Deelnemer.

Er wordt getest ervan uitgaande dat een aanvaller op reeds toegang tot een netwerkomgeving heeft (assume breach)

B2.36 De standaard bij een onderzoek is dat er getest wordt op basis van het "assume breach" principe, waarbij ervan uit wordt gegaan dat een aanvaller/uitvoerder reeds toegang heeft tot de netwerkomgeving/objecten. Hierdoor kan de robuustheid/kwetsbaarheid van het object 'as is' beter worden getest, zonder invloed van andere mitigerende maatregelen (zoals firewalls etc.). Partijen stemmen dan af welke maatregelen nodig zijn om dat mogelijk te maken.
Deelnemer en opdrachtnemer kunnen ook nader overeenkomen dat/wanneer er niet wordt getest op basis van het "assume breach" principe.

Gebruik CVSS-scores

B2.37 Aan iedere bevinding wordt een score toegekend volgens de standaard van het Common Vulnerability Scoring System (CVSS). De CVSS-scores dienen te worden berekend op basis van de relevante metriekgroepen: Base Metrics, aangevuld met de Supplemental Metrics, Environmental (Modified Base Metrics - Vulnerable System Impact Metrics, Subsequent System Impact Metrics) en Threat Metrics.

Berekening CVSS-score

B2.38 -

Bewijslast

B2.39 Opdrachtnemer dient de rapportage versleuteld op te slaan. Indien dat in het Plan van Aanpak is overeengekomen, dient Opdrachtnemer ook de scanresultaten, producties en andere resultaten versleuteld op te slaan en op eerste verzoek van Deelnemer ter beschikking te stellen.
De integriteit van alle scanresultaten, producties en overige resultaten is gewaarborgd. Indien dat in het Plan van Aanpak is overeengekomen, heeft Opdrachtnemer alle resultaten gehasht, zodat de inhoud en integriteit van de bestanden geverifieerd kan worden.
Er geldt een minimale bewaartermijn van 3 maanden, berekend vanaf datum van het definitieve eindrapport. Voor informatie die te beschermen belangen (TBB's) raakt met een rubricering TBB1, 2 of 3 (staatsgeheim) geldt een minimale bewaartermijn van 6 maanden. Partijen maken afspraken over eventueel langere bewaartermijnen.

Validatie scanresultaten

B2.40 Opdrachtnemer levert voor zover redelijkerwijs mogelijk, op eerste verzoek van Deelnemer, bewijs aan waaruit blijkt dat alle scans/testen zijn uitgevoerd tegen de scope objecten en niet tegen andere beschermende maatregelen (zoals firewalls), die buiten werking gesteld hadden moeten om een verstorende werking op de scanresultaten te voorkomen. Opdrachtnemer levert dan ook bewijs aan dat met andere parameters (bijvoorbeeld IP-adres of intensiteit van scanning) is gevalideerd dat extra beschermende maatregelen voor het onderzoek niet functioneerden tijdens het onderzoek.

Documenteren toegangswegen

B2.41 Opdrachtnemer dient op eerste verzoek van Deelnemer bewijs te kunnen leveren van de gedetecteerde en geïdentificeerde toegangswegen waarmee verbonden kan worden met een onderzocht scope object, ook indien deze niet direct tot een kwetsbaarheid hebben geleid.

B2.42 De rapporteur(s) en overige bij het onderzoek in te zetten professionals van opdrachtnemer handelen tijdens het onderzoek integer en zoals van een bekwaam beroepsbeoefenaar verwacht mag worden. Als dat niet het geval is, heeft Deelnemer het recht verdere inzet van deze de persoon te weigeren en vervanging te verlangen, zonder dat de opdrachtnemer aanspraak kan maken op enigerlei schadevergoeding in de

breedste zin des woords. De rapporteurs en overige in te zetten professionals voorkomen onderbrekingen of verstoringen die het gevolg zijn van hun handelen, met ongewenst gevolgen voor de Deelnemer.

B2.43 Wanneer opdrachtnemer tijdens het onderzoek een onvoorziene onderbreking of verstoring veroorzaakt op een scope-object als gevolg van zijn handelen, met ongewenste gevolgen voor de productie-omgeving, staakt hij het onderzoek en maakt hij hiervan direct melding bij de voor dit onderzoek aangewezen contactpersoon van Deelnemer onder vermelding van alle relevante informatie. De contactpersoon van Deelnemer verzorgt de interne communicatie, opdrachtnemer herstelt de situatie zo spoedig mogelijk. Opdrachtnemer stemt met Deelnemer af of en onder welke voorwaarden het onderzoek kan worden vervolgd.

B2.44 Het is opdrachtnemer bij een onderzoek niet toegestaan om wijzigingen aan te brengen in de scope-objecten en data die hij aantreft, tenzij Deelnemer hiervoor expliciete schriftelijke toestemming heeft verleend.

B2.45 Opdrachtnemer laat alle bevindingen die uit geautomatiseerde tests volgen nog handmatig verifiëren of reviewen door de rapporteur(s) of door overige bij het onderzoek in te zetten professionals.

B2.46 Opdrachtnemer stemt met Deelnemer of en welke bevindingen van kwetsbaarheden gemeld worden bij het NCSC via een Coordinated Vulnerability Disclosure (CVD) formulier. Opdrachtnemer ondersteunt Deelnemer op verzoek bij deze CVD-melding. Als de kwetsbaarheid gevonden is in een systeem of product dat niet van Deelnemer maar een rechthebbende derde is, dan stemt Opdrachtnemer met Deelnemer af en ondersteunt hij op verzoek van Deelnemer bij het melden van deze kwetsbaarheid bij deze derde.

4. Rapportage

Aanwijzing en beschrijving rapporteur, opsteller of hoofdonderzoeker

B2.47 In de op te leveren rapportage is de naam van een persoon (of meerdere personen) genoemd, die de professionele eindverantwoordelijkheid draagt (of dragen) voor de uitvoering van het informatiebeveiligingsonderzoek en de betreffende rapportage. Deze persoon (of personen) is (of zijn) in de rapportage als rapporteur(s) aangemerkt. Hiernaast vermeldt de rapportage de namen van de overige personen die betrokken zijn (geweest) bij de uitvoering van het onderzoek.

Beschrijving van de verplichte certificering, waarover de rapporteur beschikt

B2.48 In de rapportage wordt bij de rapporteur(s) benoemd over welke relevante en geldige certificeringen deze persoon/personen beschikken. Datzelfde wordt gedaan voor de overige professionals die betrokken zijn bij de uitvoering van het onderzoek.

Bewijs certificering

B2.49 De rapportage geeft aan hoe opdrachtgever de aanwezigheid van geclaimde geldige certificering middels inzage in bewijsstukken kan vaststellen. Dat kan door vermelding van (1) een digitale vindplaats met link naar een platform/portaal of bestand of (2) contactgegevens van een persoon die op fysieke of digitale wijze inzage kan geven.

Benoemen van de versie van de rapportage

B2.50 De rapportage beschikt over een versienummer.

Handtekening voor waarheidsgetrouwe rapportage

B2.51 De rapportage wordt voorzien van een tekst, waaruit blijkt dat de rapportage:
1. accuraat en naar waarheid is opgesteld;
2. er een review op deze versie van het document heeft plaatsgevonden door andere een niet bij het onderzoek betrokken persoon.
Deze tekst voorzien van een handtekening van de rapporteur. Deze handtekening kan een fysiek gezette handtekening zijn of een digitale handtekening.

Vertrouwelijkheid

B2.52 Opdrachtnemer legt in beginsel aan de op te leveren rapportage en onderliggende documenten geen belemmeringen aan Deelnemer op met betrekking tot het beschikbaar stellen, verspreiden, opslaan en distribueren. Bijvoorbeeld aan rechthebbende derde partijen die eigenaar zijn van onderzochte systemen of applicaties of door Deelnemer

ingeschakelde auditors. Deelnemer draagt in zo'n geval de verantwoordelijkheid voor het verder verspreiden van deze informatie en de vertrouwelijkheid hiervan. Eventuele door Deelnemer en Opdrachtnemer gemaakte afspraken over vertrouwelijkheid worden in de rapportage benoemd en gerespecteerd. Opdrachtnemer accepteert dat Deelnemer de intellectuele eigendomsrechten heeft op de data die afkomstig is van Deelnemer en door opdrachtnemer opgestelde rapportages. Opdrachtnemer deelt de rapportage niet zonder expliciete toestemming van de contactpersoon van Deelnemer met anderen.

B2.53 Indien van toepassing, vernietigt Opdrachtnemer de gegevens van de rapportage en/of onderliggende bestanden na een bepaalde bewaartermijn, volgens de specifieke afspraken die Deelnemer en Opdrachtnemer daarover hebben gemaakt. Anders gelden hiervoor de wettelijke bewaartermijnen.

Verspreiding

B2.54 Deelnemer kan verlangen dat opdrachtnemer de rapportage in (laatste) conceptvorm aan een of meerdere contactpersonen van Deelnemer ter review aanbiedt, om vast te stellen of rapportage voldoet aan rapportagevereisten en de afspraken in het plan van aanpak. Deelnemer onthoudt zich van commentaar waarmee de onafhankelijkheid en integriteit van de rapportage kan worden aangetast. Zolang het commentaar niet ziet op het nakomen van eerder overeengekomen rapportagevereisten of afspraken in het plan van aanpak, is de rapporteur(s) eindverantwoordelijk voor de keuze welk commentaar wel of niet overgenomen wordt in de rapportage. Na review en verwerking van noodzakelijke aanpassingen kan het rapport worden opgeleverd als definitief.

Hoofdstukindeling

Inhoudsopgave

B2.55 Opdrachtnemer levert op basis van het uitgevoerde onderzoek een rapportage op, conform het door opdrachtgever vastgestelde model(rapportage) met standaard hoofd- en paragraafindeling. Dit model moet zorgen voor uniformiteit, transparantie, compleetheid van de rapportage en reproduceerbaarheid van het onderzoek. De Opdrachtgever kan nieuwe versies van dit model vaststellen, die opdrachtnemer daarna dient toe te passen. Opdrachtnemer heeft de mogelijkheid suggesties aan opdrachtgever te geven voor verbetering van het model. Afwijking van dit model is alleen toegestaan na schriftelijke goedkeuring van Deelnemer, overeen te komen in het plan van aanpak (pre-engagement).

Methodologie

B2.56 De rapportage bevat een hoofdstuk methodiek waarin beschreven wordt langs welke fasen en lijnen het onderzoek uitgevoerd is. De fasering van de Pentest Execution Standard (PTES) wordt hierbij als standaard gebruikt, tenzij Deelnemer en Opdrachtnemer expliciet in het Plan van Aanpak een andere, vergelijkbare industriestandaard zijn overeengekomen, welke in de methodiek beschreven is.

Methodologie - CVSS

B2.57 De rapportage bevat een subhoofdstuk binnen het hoofdstuk methodiek - waarin beschreven wordt dat de bevindingen welke door onderzoekers gedaan worden, geclassificeerd worden middels het Common Vulnerability Scoring System en worden voorzien van een zogenoemde CVSS-vector string teneinde terug te kunnen leiden hoe de calculatie van de score tot stand gekomen is.

Documentbeheer

B2.58 De rapportage bevat een (sub)hoofdstuk over het document (documentbeheer) - in dit hoofdstuk wordt tenminste gedefinieerd: Opdrachtgever, projectnummer/naam, start- en einddatum van project, rapporteurs, reviewers, document classificatie, versie-nummer van het document en de handtekening van de verantwoordelijke rapporteur

Versiebeheer

B2.59 De rapportage bevat een (sub)hoofdstuk over versie-beheer - in dit hoofdstuk wordt tenminste gedefinieerd (per versie): Versie, Datum, Auteur en Versie-omschrijving

Distributielijst

B2.60	De rapportage bevat een (sub)hoofdstuk inzake de distributielijst - in dit hoofdstuk wordt tenminste gedefinieerd: Versie, datum, naam, organisatie en verspreidingsmethode
Aanleiding	
B2.61	De rapportage bevat een (sub)hoofdstuk waarin de aanleiding van het onderzoek beschreven is, hierbij wordt minimaal beschreven: of er sprake is van een time-boxed test en indien dit het geval is, wat de maximering van de uren betreft, welke onderdelen niet (volledig) konden worden getest en waarom niet, een algemene beschrijving van de te testen omgevingen van opdrachtgever
Doelstelling	
B2.62	De rapportage bevat de doelstelling(en) die overeenkomt (overeenkomen) met wat tijdens de intake is besproken en is opgenomen in het definitieve plan van aanpak.
Bevindingenlijst	
B2.63	De rapportage bevat een genummerde lijst van bevindingen en verwijst naar de individuele bevindingen
Managementsamenvatting	
B2.64	De rapportage bevat een managementsamenvatting
Start/einddatum	
B2.65	De managementsamenvatting bevat een start- en einddatum van het onderzoek
Overzicht gebruikte standaarden	
B2.66	De managementsamenvatting bevat een overzicht van de gebruikte standaarden tijdens het onderzoek
CIA-scores	
B2.67	De managementsamenvatting bevat een overzicht van de door opdrachtgever aangeleverde CIA-scores per scope-object indien deze door opdrachtgever zijn opgeleverd
Root-cause analyse	
B2.68	De managementsamenvatting bevat een root-cause analyse op basis van de informatie verkregen uit het onderzoek en de bevindingen
Overzicht bevindingen	
B2.69	De managementsamenvatting bevat een overzicht van de door rapporteur aangetroffen kwetsbaarheden (aantal bevindingen per risico-categorie) - op basis van het Common Vulnerability Scoring System - CVSS - waarbij de volgende categorieën worden gehanteerd: Kritiek, Hoog, Gemiddeld, Laag en Informatief (zoals gedefinieerd door FIRST)
Scope	
B2.70	De rapportage bevat een overzicht van de scope-objecten, waarbij per scope-object aangegeven wordt of deze getest is en indien er afwijkingen zijn wordt er per scope-object beschreven wat deze afwijkingen behelzen.
Overeenkomst met Plan van Aanpak	
B2.71	De rapportage bevat de scope die is besproken in het intakegesprek en is vastgelegd in het definitieve plan van aanpak
Assume Breach principe	
B2.72	De rapportage bevat een (sub)hoofdstuk waarin beschreven is of er middels het assume breach principe getest wordt en hoe de validatie van het toepassen van het principe vastgesteld is door opdrachtnemer. De rapportage bevat de fysieke locaties (land) van de onderzochte objecten, de fysieke locaties van uitvoering van het onderzoek en vaststelling dat het onderzoek volgens de aldaar van toepassing zijnde wet- en regelgeving is uitgevoerd.
Tijdslijn (verloop van penetratietest) - reproduceerbaarheid	

B2.73	De rapportage bevat een tijdlijn waarin aangegeven wordt welke acties er op welk moment in de tijd (tijdens de testperiode) uitgevoerd zijn.
Hoofdstuk - Bevindingen	
B2.74	De rapportage bevat een hoofdstuk waarin de bevindingen van het onderzoek zijn beschreven.
Scope-object	
B2.75	In de rapportage dient er per opgenomen bevinding een scope-object te worden gedefinieerd - dit scope-object dient direct herleidbaar te zijn naar het systeem, de omgeving of applicatie (of directe URL) waarbinnen de kwetsbaarheid zich bevindt.
CVSS-score	
B2.76	In de rapportage dient er per opgenomen bevinding een CVSS-score te worden gedefinieerd, tezamen met een CVSS-classificatie, bij voorkeur volgens de meest recente standaard (https://www.first.org/cvss/v4.0/specification-document - 6. Qualitative Severity Rating Scale) en indien van toepassing wordt in de berekening de weging meegenomen vanuit de door opdrachtgever verstrekte CIA-scores.
CVSS Vector string	
B2.77	In de rapportage dient er per opgenomen bevinding een CVSS-vector string te worden verstrekt, bij voorkeur volgens de meest recente standaard (https://www.first.org/cvss/v4.0/specification-document - 7 Vector String). Indien van toepassing wordt in de berekening de weging meegenomen vanuit de door opdrachtgever verstrekte CIA-scores.
Beschrijving kwetsbaarheid	
B2.78	In de rapportage dient er per opgenomen bevinding een beschrijving van de kwetsbaarheid te worden opgenomen, waarbij indien beschikbaar gerefereerd wordt naar externe bronnen (zoals bijvoorbeeld CVE-nummers, public advisories)
Bevestiging kwetsbaarheid	
B2.79	In de rapportage dient er per opgenomen bevinding een bevestiging van de kwetsbaarheid te worden opgenomen, waarbij expliciet opgenomen staat hoe de kwetsbaarheid kan worden gereproduceerd, of er gebruik gemaakt is van een publieke exploit, of er door middel van misbruik van de kwetsbaarheid toegang is verkregen tot het systeem en/of beschikbare informatie
Mogelijke impact	
B2.80	In de rapportage dient er per opgenomen bevinding een mogelijke impact te worden beschreven. Daarbij dient ook rekening te worden gehouden met de impact op omliggende omgevingen/systemen welke een relatie hebben tot het scope-object
Aanbeveling	
B2.81	In de rapportage dient er per opgenomen bevinding een aanbeveling te worden geschreven inzake hoe een kwetsbaarheid kan worden opgelost. Daarbij dient er (indien deze van toepassing is) een klikbare (link) te worden opgenomen naar een individuele toevoeging in de Common Weakness Enumaration (CWE) database welke bij de kwetsbaarheid hoort.
Bijlagen	
B2.82	De rapportage bevat een hoofdstuk waarin bijlages opgenomen worden
Verklarende woordenlijst	
B2.83	De rapportage bevat (bij voorkeur in de bijlagen) een verklarende woordenlijst.
Hulpmiddelen	
B2.84	De rapportage bevat (bij voorkeur in de bijlagen) een opsomming van gebruikte hulpmiddelen tijdens het onderzoek.
Hulpmiddelen - Beschrijving	

B2.85	Per gebruikt hulpmiddel wordt een beschrijving opgenomen.
Hulpmiddelen - Versie-nummer	
B2.86	Per gebruikt hulpmiddel wordt een specifiek versienummer opgenomen welke overeenkomt met de versie van het ingezette hulpmiddel
Hulpmiddelen - Publieke referentie (URL)	
B2.87	Per gebruikt hulpmiddel wordt een publieke referentie (URL) opgenomen waar het specifieke hulpmiddel kan worden verkregen (download/informatie website)
Ontvangen documenten	
Ontvangen documenten – Beschrijving	
B2.88	De rapportage bevat (bij voorkeur in de bijlagen) een lijst met ALLE door opdrachtnemer ontvangen documenten (inclusief bestandsnaam). Per ontvangen document wordt een beschrijving opgenomen van het specifieke document
Ontvangen documenten - SHA1-hashes	
B2.89	Per ontvangen document wordt een SHA1-hash berekend en opgenomen (als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak waren overeengekomen)
Ontvangen bestanden	
B2.90	De rapportage bevat (bij voorkeur in de bijlagen) een lijst met ALLE door opdrachtnemer ontvangen bestanden (inclusief bestandsnaam).
Ontvangen bestanden - Beschrijving	
B2.91	Per ontvangen bestand wordt een beschrijving opgenomen van het specifieke bestand
Ontvangen bestanden - SHA1-hashes	
B2.92	Per ontvangen bestand wordt een SHA1-hash berekend en opgenomen (als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak waren overeengekomen)
Gebruikte accounts	
B2.93	De rapportage bevat (bij voorkeur in de bijlagen) een lijst met de door opdrachtgever verstrekte accounts
Gebruikte accounts - Scope-object	
B2.94	Per opgenomen account wordt het bijbehorende scope-object beschreven
Gebruikte accounts - Beschrijving	
B2.95	Per opgenomen account wordt een beschrijving en rol/een korte beschrijving van permissies opgenomen
Uitgevoerde scans	
B2.96	De rapportage bevat (bij voorkeur in de bijlagen) de scan-output (scan-resultaten) van de uitgevoerde scans
Uitgevoerde scans - Scan-resultaat - Scope-object	
B2.97	Per scan-resultaat wordt het scope-object gedefinieerd
Uitgevoerde scans - Scan-resultaat - Output	
B2.98	Per scan-resultaat wordt de ruwe scan-output opgenomen
Bewijsmateriaal	
B2.99	De rapportage bevat (bij voorkeur in de bijlagen) een lijst met alle door opdrachtnemer gecreëerde/gegenereerde informatie, welke dient als bewijsmateriaal. Voorbeelden hiervan zijn state-files (Burp), Nessus scans, map scans, testssl.sh scans en elke andere output behorende tot het onderzoek
Bewijsmateriaal - SHA1-hashes	

B2.100	Per bestand dat behoort tot het bewijsmateriaal wordt een SHA1-hash berekend en opgenomen (als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak waren overeengekomen)
Checklists	
B2.101	De rapportage bevat (bij voorkeur in de bijlagen) de checklists voor de standaarden die van toepassing zijn op het onderzoek
Checklists - Per standaard	
B2.102	Binnen deze checklist dient elke test te worden afgevinkt, waarbij er drie verschillende statussen mogelijk zijn: 1. Getest. 2. Niet getest. 3. Valt niet te testen (functionaliteit afwezig). Indien er een bevinding is, dient deze bij de individuele check te worden opgenomen als afwijking. Indien een check niet getest is, dient dit als rood te worden gemarkeerd en dient toelichting te worden gegeven waarom een test niet uitgevoerd is.
Lijst van onbenaderbare/onbereikbare scope-objecten	
B2.103	In de rapportage (bij voorkeur in de bijlagen) wordt beschreven of er scope-objecten ten tijden van het onderzoek technisch niet bereikbaar waren. Daarbij wordt beschreven welke scope-objecten dit betroffen en hoe is vastgesteld dat deze objecten technisch niet benaderbaar/bereikbaar waren.

Modelrapportage Penetratietest - te rapporteren onderwerpen per hoofdstuk

1. Documentbeheer

Opdrachtgever:

Projectnummer/-naam:

Start- en einddatum onderzoek

Versienummer:

Versiedatum:

Versienaam en -omschrijving:

Verantwoordelijke rapporteur/auteur:

Bij de uitvoering ingezette professionals:

Distributielijst en reviewers:

Review en accordering:

Tekst waarin wordt bevestigd dat de rapportage accuraat en naar waarheid is opgesteld

Bevestiging dat een review is uitgevoerd door een onafhankelijke persoon

Handtekening rapporteur (fysiek of digitaal)

Voorwaarden gebruik rapportage en vertrouwelijkheid

2. Managementsamenvatting

Start- en einddatum onderzoek

Overzicht gebruikte standaarden

Aangeleverde CIA-scores per scope-object

Root-cause analyse

Overzicht aangetroffen kwetsbaarheden per CVSS-risicocategorie

Fysieke locaties (land) van onderzochte objecten en naleving wet- en regelgeving

Samenvatting van belangrijkste bevindingen

Samenvatting van aanbevelingen voor verbetering

3. Inleiding

Doel en reikwijdte van de test

Achtergrondinformatie over de organisatie

Assumpties en beperkingen

Relevante standaarden en methodologieën

Personele certificering en verantwoordelijkheden

Naam rapporteur en zijn/haar certificeringen

Certificeringen van overige betrokken professionals

Informatie over validatie van certificeringen

4. Scope

Scope-objecten en afbakening

Overzicht van afwijkingen ten opzichte van het Plan van Aanpak

Fysieke locaties (land) van onderzochte objecten en naleving wet- en regelgeving

5. Methodiek

Toegepaste testmethodiek (incl. assume breach principe)

Uitvoering volgens PTES (Pentest Execution Standard) of andere standaard

Interacties vóór de betrokkenheid

Informatie verzamelen

Modellering van bedreigingen

Kwetsbaarheidsanalyse

Exploitatie

Post-exploitatie

Rapportage

Toegepaste classificatiemethodiek van bevindingen: CVSS

Tijdlijn met uitgevoerde acties

Aanvalsperspectief en gebruikte technieken

6. Bevindingen

Indeling per scope-object

Beschrijving kwetsbaarheden (incl. referenties naar CVE-nummers)

CVSS-score, classificatie en vectorstring

Impactanalyse (incl. impact op omliggende systemen)

Reproductiestappen en gebruikte exploits

Aanbevelingen met verwijzing naar CWE-database

Optioneel: Bewijs van gedetecteerde en geïdentificeerde toegangswegen

Optioneel: Bewijsvoering dat tests op scope-objecten zijn uitgevoerd en niet op beschermende maatregelen

7. Conclusie en aanbevelingen

Samenvatting van de belangrijkste bevindingen

Aanbevelingen voor verbeteringen, inclusief een advies over de prioritering van de aanbevelingen

Bijlagen

Begrippenlijst / Verklarende woordenlijst

Hulpmiddelen

Beschrijving hulpmiddelen

Versienummer per hulpmiddel

URL naar download/informatiepagina hulpmiddel

Overzicht van ontvangen documenten en bestanden

Documenten, beschrijvingen en SHA1-hashes

Bestanden, beschrijvingen en SHA1-hashes

Overzicht verstrekte accounts (inclusief rollen en permissies)

Accounts, bijbehorende scope-objecten, rollen en permissies

Uitgevoerde scans

Scanresultaten en scope-objecten

Ruwe scanoutput

Volledige CVSS-berekeningen en vectorstrings

Bewijsmateriaal

Optioneel: SHA1-hashes voor bewijsmateriaal

Optioneel: Bewijsvoering van scope-controle en beschermende maatregelen

Checklists

Overzicht van gebruikte standaarden en frameworks

Checklist per standaard
Status (Getest/Niet getest/Valt niet te testen)
Toelichting bij niet-geteste onderdelen
Afwijkingen en bevindingen gekoppeld aan specifieke tests
Beheer van testresultaten
Afspraken over versleutelde opslag van resultaten
Optioneel: Afspraken over hashing ter verificatie van integriteit
Afspraken over bewaartermijnen
Lijst van onbenaderbare/onbereikbare scope-objecten
Scope-objecten die niet bereikbaar waren
Hoe bereikbaarheid is vastgesteld
Impact op de testresultaten