PENTESTEN DOE JE ZO

Een handleiding voor opdrachtgevers

WWW.GOVCERT.NL

POSTADRES
Postbus 84011
2508 AA Den Haag
BEZOEKADRES
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
TELEFOON
070 888 75 55
FAX
070 888 75 50
E-MAIL
info@govcert.nl

Auteurs : GOVCERT.NL in samenwerking met Fox-IT
Versie : 1.1
Den Haag : 15 juni 2010
Publieke uitgave : 20 september 2010

GOVCERT.NL

GOVCERT.NL is het Computer Security Incident Response Team van de Nederlandse overheid.

GOVCERT.NL heeft in de loop der jaren veel vragen en ervaringen van haar deelnemers over pentests verzameld. Door deze ervaringen in dit document te delen hoopt GOVCERT te helpen veel voorkomende vragen rondom dit onderwerp te beantwoorden. Dit whitepaper is opgesteld samen met Fox-IT.

Fox-IT is een gerenommeerd Europees IT-beveiligingsbedrijf gevestigd in Delft. Fox-IT levert wereldwijd bijzondere beveiliging- en intelligence-oplossingen voor overheden en maatschappelijk belangrijke organisaties. De kernactiviteiten zijn het ontwikkelen van oplossingen voor het beschermen van staatsgeheimen, het uitvoeren van digitale rechercheonderzoeken en het leveren van beveiligingsexpertise in de vorm van audits, consultancy en trainingen.

Fox-IT voert jaarlijks tientallen pentests uit voor (semi-) overheidsorganisaties in binnen- en buitenland op een breed scala aan informatiesystemen; van internetstemsystemen tot beveiligde USB-sticks en van Blackberries tot complete kantoorgebouwen.

GOV  CERT.NL

SAMENVATTING / SUMMARY

Nederlands

Penetratietests zijn een waardevolle aanvulling op de beveiliging van informatiesystemen. Een penetratietest (ook pentest genoemd) uitvoeren kan echter een uitdaging zijn. Risico's moeten minimaal zijn, de kwaliteit van de test optimaal en resultaten moeten bruikbaar zijn om kwetsbaarheden efficiënt te verhelpen.

Niet alle organisaties beschikken over gedetailleerde kennis om zelf een pentest uit te voeren en dit wordt dan ook vaak uitbesteed. De opdrachtgever moet echter wel een aantal keuzes maken bij uitbesteding. Om die keuzes te kunnen maken is ook weer bepaalde kennis over pentests nodig.

Alle informatie die u nodig heeft om een penetratietest uit te besteden, is samengevat in dit white paper.

Na een introductie over penetratietests gaan we in op de offerteaanvraag, de leverancierselectie en de uitvoering en het verwerken van de resultaten. Het gehele traject van het inkopen van een penetratietest is hiermee onderverdeeld is duidelijk te scheiden fasen.

English

Penetration testing is an invaluable complement to the safeguarding of information systems. However, the process of carrying out a penetration test (also known as a pen test) can be challenging. Risks must be minimal, testing quality optimal, and results must be usable so that vulnerabilities can be repaired efficiently.

Not all organizations have the detailed knowledge required to carry out a pen test, so this process is often contracted out. However, in the event of contracting out, the instructing party must make a number of choices. In order to make these choices, a certain level of knowledge with regard to pen testing is required.

All of the information you need in order to contract out penetration testing is summarized in this white paper.

Following an introduction on penetration testing we explore the following: requesting a quotation, selecting a supplier, carrying out the test and processing the results. The entire process of purchasing a penetration test is thus divided into clearly defined phases.

GOVCERT.NL

INHOUD

1 INLEIDING

Steeds vaker ontstaat bij (overheids)organisaties de behoefte om hun IT-systemen te onderwerpen aan een zogenaamde *penetratietest* (afgekort: pentest). Het laten uitvoeren van zo'n test is echter geen sinecure. Het kan een lange weg zijn van het vinden van een goede leverancier tot aan het zorgen voor opvolging van de resultaten. Dit document geeft u als opdrachtgever inhoudelijke hulp door te illustreren hoe een pentesttraject kan verlopen.

1.1 Leeswijzer

Dit whitepaper neemt u mee door een pentestingproject. In hoofdstuk 2 wordt eerst gedefinieerd wat een pentest precies is en welke begrippen daarbij belangrijk zijn. Hoofdstuk 3 geeft informatie over het opstellen van een offerteaanvraag, waarna de leverancierselectie in het hoofdstuk 4 aan bod komt. Hoofdstuk 5 beschrijft wat te doen en waar op te letten tijdens de daadwerkelijke uitvoering van de test en hoofdstuk 6 gaat over het verwerken van de resultaten.

NOOT 1 Indien in dit document de naam van een product, dienst, fabrikant of leverancier wordt genoemd, betekent dit niet dat GOVCERT.NL deze op enige wijze goedkeurt, afkeurt, aanraadt, afraadt of anderszins hiermee verbonden is.

NOOT 2 Dit document is niet uitputtend en zal regelmatig bijgewerkt worden. Aanvullingen, opmerkingen of eigen ervaringen ontvangen wij graag via info@govcert.nl.

2 WAT IS EEN PENTEST?

Een pentest is een geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken, om zo inzicht te krijgen in de effectiviteit van dat systeem en om verbeterpunten te definiëren.

In de praktijk betekent het dat een team beveiligingsspecialisten (ook wel *ethical hackers* genoemd) met toestemming van de systeemeigenaar probeert om informatie uit het beveiligde systeem te benaderen zonder de vereiste toegangsgegevens.

Het doel van de pentest is om:

1. Inzicht te krijgen in de risico's en kwetsbaarheden van het onderzochte systeem.
2. De beveiliging te verbeteren – met andere woorden, de risico's en kwetsbaarheden te bestrijden.

Let op: soms kan een pentest problemen blootleggen die inherent blijken te zijn aan een bepaalde ontwerpbeslissing, waardoor het oplossen van het probleem veel werk kost. Het is dan ook erg belangrijk om ook beveiligingsexpertise bij de ontwerpfase van een systeem te betrekken.

2.1 Andere termen voor pentesting

Andere termen die voor penetratietests gebruikt worden zijn *ethical hacking test, legal hacking test*, *hacktest*, *security scan*, *vulnerability assessment* en diverse samenstellingen van deze termen. De termen komen min of meer op hetzelfde neer. In dit paper gebruiken we alleen de term pentest.

2.2 Soorten pentest

Bij penetratietests hoort nogal wat jargon. Vooral de *boxen* zullen bij een gesprek over pentesting snel op tafel komen: men spreekt van *black box tests*, *grey box*, *white box* en soms zelfs van *crystal box* en *time/budget box tests*. Het verschil zit onder meer in de hoeveelheid kennis en achtergrondinformatie die de tester krijgt.

Als een tester minimale voorkennis heeft, is er sprake van *black box*; krijgt een tester van tevoren inzicht in alle aspecten van de systeemarchitectuur, dan heet die *white box*. Beschikt een tester over gedeeltelijke informatie, dan heet dit *grey box*. Dat kan een inlogaccount zijn om te testen of het voor gebruikers met een werkend wachtwoord mogelijk is om misbruik te maken. Denk ook aan een test van een internetbank: het is zinvol om, als de testers niet voorbij het inlogscherm komen, ook te proberen om met geldige inloggegevens geld over te maken van een rekening van iemand anders. In een pure *black box* komt de aanvaller wellicht niet langs het inlogscherm en heeft dan niet de gelegenheid of de tijd om ook dit soort aspecten nog te testen.

Met *crystal box* wordt meestal bedoeld dat de testers ook de broncode van de applicatie hebben en toegang hebben tot alle mogelijke configuratie-informatie.

Met *time box* of *budget box* wordt eigenlijk iets heel anders bedoeld, namelijk een test waarbij de doorlooptijd of de kosten bepalen wanneer de test ophoudt. Bijvoorbeeld: hoe ver kan een team ervaren pentesters in drie dagen komen? Dat kan soms een zinvolle vraag zijn om te stellen. In de fysieke beveiligingswereld weet men immers al veel langer dat 100% veiligheid niet bestaat en verkoopt men kluizen met een tijdsaanduiding: “een aanvaller met de juiste kennis en gereedschap heeft minstens *x* uur nodig om deze kluis open te krijgen”.

Naast de hoeveelheid informatie die de aanvallers ter beschikking hebben, moet er ook een keuze worden gemaakt over de informatie die het eigen personeel krijgt: worden ze op de hoogte gebracht dat een penetratietest uitgevoerd gaat worden of blijven ze in het ongewisse? Bij dat laatste geeft de penetratietest ook inzicht in de manier waarop incidentdetectie en afhandeling wordt uitgevoerd. Het is dan wel van belang dat wordt ingegrepen voordat het personeel vervolgacties (zoals aangifte) gaat ondernemen.

Voor het verkrijgen van informatie kunnen de testers publiekelijk beschikbare bronnen raadplegen (zoals Internetpagina’s), maar het is ook mogelijk om ‘social engineering’ toe te passen. Hierbij wordt geprobeerd om informatie te krijgen van medewerkers, door bijvoorbeeld de helpdesk te bellen, door een medewerker om zijn wachtwoord te vragen of door de portier om te praten om het gebouw binnen te komen. Afhankelijk van de doelstelling van de penetratietest kan social engineering binnen de scope vallen.

2.3 Wanneer pentesten?

Er kunnen meerdere momenten zijn waarop een pentest zinvol is:

1. In de acceptatiefase van een nieuw systeem of een nieuwe applicatie.
2. Bij significante wijzigingen van een belangrijk systeem of een belangrijke applicatie.
3. Periodiek (jaarlijks/tweejaarlijks), om bestaande systemen te testen op nieuwe inbraaktechnieken en/of als onderdeel van de ‘Plan, Do, Check, Act’-cyclus van het Information Security Management System (ISMS)[1].
4. Als er een andere reden is om te denken dat de beveiliging van een systeem minder goed is dan gedacht. Het bekend worden van de kwetsbaarheid van de beveiliging van sommige gebouwen zou bijvoorbeeld aanleiding kunnen zijn voor een pentest op het eigen toegangspassensysteem.

[1] ISO-standaard 27002 (voorheen 17799)

2.4 Audit, code review en risicoanalyse

In deze paragraaf behandelen we voor de duidelijkheid kort enkele termen die soms in combinatie met of zelfs in plaats van de term penetratietest worden gebruikt. Het gaat om de termen audit, code review en risicoanalyse.

Hoewel de term audit ook wel wordt gebruikt om penetratietests aan te duiden, is dat toch iets anders. Een audit is een formeel proces, dat start met een bepaald normenkader waarvan de auditor opzet, bestaan en werking kan toetsen. Een audit levert dan ook een volledig beeld op – ten aanzien van het vooraf overeengekomen normenkader. De betekenis van een audit hangt dan ook sterk samen met de kwaliteit van het normenkader.

Bij een penetratietest hoort geen normenkader; wel zal een volwassen aanbieder een methodiek hebben volgens welke een penetratietest van een bepaald soort besturingssysteem of applicatie wordt aangepakt, maar er wordt niet getoetst aan de hand van een normenkader. Creativiteit en vakkennis van de individuele tester speelt een veel grotere rol.

Bij een code review wordt de broncode van een applicatie onderzocht. Een code review is een goed middel kwetsbaarheden in een applicatie te vinden. Omdat een code review en een penetratietest vanuit verschillende perspectieven werken en geen overlap hebben, worden ze soms tegelijkertijd uitgevoerd.

Een risicoanalyse brengt dreigingen in kaart. Daarbij wordt een inschatting gemaakt van de dreigingskans en de impact ervan. Een risicoanalyse heeft bijna altijd een hoger abstractieniveau dan een penetratietest. Meestal wordt daarom eerst een risicoanalyse uitgevoerd waaruit blijkt dat kwetsbaarheden in een systeem een groot risico zijn en vervolgens wordt een penetratietest uitgevoerd om in kaart te brengen welke kwetsbaarheden er zijn en hoe ze opgelost kunnen worden.

3 OFFERTEAANVRAAG

Ter voorbereiding op een pentest, moet een aantal acties ondernomen worden. Dit hoofdstuk gaat in op de offerteaanvraag, de opdrachtomschrijving, scopedefinitie, planning, kosten, kwaliteit en overige randvoorwaarden.

3.1 Opdrachtomschrijving

Essentieel in de offerteaanvraag is de opdrachtomschrijving met daarin een heldere onderzoeksvraag. Welke informatie moet de pentest opleveren; welke vraag moet beantwoord worden? Het moet voor aanbieders duidelijk zijn wat er van hen wordt verwacht. Het belangrijkste aspect dat u bij het maken van de opdrachtomschrijving voor ogen moet houden is die van de heldere onderzoeksvraag. Welke vraag wilt u beantwoord hebben met deze test? – met andere woorden, naar welke informatie bent u uiteindelijk op zoek, welk doel heeft u voor ogen?

Voorbeelden van onderzoeksvragen zijn:

- *Welke kwetsbaarheden kunnen worden gevonden in de configuratie en implementatie van systeem x?*
- *Zijn er naast de dreigingen die wij al geïdentificeerd hebben nog onvoorziene dreigingen bij het gebruik van applicatie y?*
- *Hoe ver kan een ervaren hacker binnendringen via het internet via website z als hij daarvoor maximaal 2 weken de tijd heeft?*

Als u al weet hoe de test er inhoudelijk in grote lijnen uit moet zien, kan het helpen om dat ook te schetsen. Besef wel dat u daarmee het risico loopt dat u een test schetst die misschien niet het juiste of efficiëntste middel is om de uiteindelijke vraag te beantwoorden.

Als een aanbestedings- of inkooptraject ook voor kleine pentests in uw organisatie veel tijd kost, kunt u ook bij de initiële offerteaanvraag ook alvast een latere hertest aanvragen. Een hertest wordt vaak gebruikt om te controleren of eerder geconstateerde kwetsbaarheden daadwerkelijk zijn opgelost (zie verder paragraaf 5.2, “wat doet u ermee?”)

Maak in de offerteaanvraag ook duidelijk welke informatie u de leveranciers ter beschikking zult stellen voorafgaand aan de test. U kunt de aanbieders ook vragen om zelf te specificeren welke achtergrondinformatie zij zinvol achten om van tevoren te hebben. Gebruik in de offerteaanvraag bij voorkeur niet termen als *black box* of *grey box*. De betekenis van deze termen is niet eenduidig en de aanbieder kan er een eigen draai aan geven. Dit maakt de offertes moeilijk vergelijkbaar en kan later leiden tot discussies.

3.2 Scopedefinitie

Een ander belangrijke aspect is de inkadering van de test. Wat is het object van onderzoek?

1. Geef goed aan om welke omgeving het gaat; hoeveel systemen, apparaten, gebouwen en dergelijke moeten er worden getest en zijn ze vergelijkbaar? Als alle 100 werkstations er in principe hetzelfde uitzien kan een steekproef van 2 of 3 systemen om te testen efficiënter zijn.
2. Als u van het te testen object een ontwikkel-, test- en/of acceptatieomgevingen heeft, dan kan het verstandig zijn om één van die omgevingen voor de duur van de pentest precies zo in te richten als de productieomgeving en de test daarop laten plaatsvinden.
3. Geef vooraf de diepgang van de penetratietest aan. Valt bijvoorbeeld het gebruiken van exploits binnen scope of niet? Exploits kunnen enerzijds dienen als ‘bewijs’ dat een gevonden kwetsbaarheid echt te misbruiken valt, maar kunnen ook de integriteit en beschikbaarheid van een systeem in gevaar brengen. Als het gebruik van een exploit weinig toegevoegde waarde biedt, is het beter om het gebruik ervan expliciet uit te sluiten.

3.3 Planning

Een pentest moet ruim van tevoren gepland worden. Houd rekening met de volgende aspecten:

1. Zijn er momenten waarop er niet getest mag worden?
2. Vermijd kritieke periodes, zoals een pentest van een salarisverwerkend systeem aan het eind van de maand;
3. Doe geen pentest als een systeem tijdens de test veranderingen ondergaat;
4. Houd rekening met een doorlooptijd van een maand tussen de offertebeoordeling en de start van de test;
5. Wees duidelijk over een interne planning, doorlooptijd en wanneer de opdracht uiterlijk afgerond moet zijn (harde deadline of niet)?

3.4 Kosten

Een pentest uitbesteden kost geld. Geef aan hoe u de kosten in de offerte gespecificeerd wilt hebben, dus welke kostenstructuur u wilt in de offerte:

- op basis van nacalculatie
- als vaste prijs. De kostenindicatie ligt in dit geval gemiddeld 10-20% hoger, maar een dergelijke afspraak laat minder ruimte voor onzekerheden.
- vaste prijs met nacalculatie, waarbij in overleg meerkosten gemaakt worden

3.5 Rapportage

De resultaten van de pentest worden vastgelegd in een vorm van een rapportage. Geef duidelijk aan welke informatie de rapportage moet bevatten:

- De gebruikte applicaties (inclusief versienummer)
- De parameters die zijn gebruikt bij de tests
- Het tijdstip waarop de test is uitgevoerd
- Het IP-adres waarvandaan de test is uitgevoerd
- Een toelichting per gevonden verbeterpunt
- Een inschatting van de prioriteit per verbeterpunt

Geef ook aan of u de testresultaten direct na de test met zowel de testers en beheerders wilt bespreken (de zogenaamde *hot wash meeting*). Zo'n gesprek biedt de mogelijkheid om door middel van discussie eventuele latere meningsverschillen over testresultaten te voorkomen.

TIP: Vraag altijd om een conceptrapportage, zodat u de gelegenheid hebt om deze aan te vullen en/of te corrigeren.

3.6 De tester(s)

Omdat bij een penetratietest individuele kennis en ervaring van de tester een grote rol spelen is het zinvol om naar de CV's van de testers te vragen.

Vraag leveranciers om in hun aanbieding aan te geven hoe zij omgaan met integriteit en screening van hun medewerkers. Vraag eventueel naar verklaringen omtrent het gedrag, registratie als particulier onderzoeker en/of screeningen door Justitie of veiligheidsdiensten.

Neem ook als eis op dat de test uiteindelijk ook daadwerkelijk wordt uitgevoerd door mensen van wie u het CV gezien en goedgekeurd heeft.

3.7 De methodiek en testplan

De kwaliteit van de penetratietest wordt mede bepaald door de methodiek. Vraag daarom in de offerteaanvraag naar stappenplan waarin de activiteiten in volgorde worden beschreven en op welke methodiek de aanpak is gebaseerd.

Het is verstandig om voor de start van de penetratietest een uitgebreid testplan te vragen, waarbij per test staat vermeld wat de risico's zijn. Stel als voorwaarde dat u vooraf een akkoord moet geven op het testplan, dan houdt u zelf de controle over de risico's die u tijdens de penetratietest mogelijk loopt.

3.8 De organisatie

Vraag leveranciers in het offertetraject naar de voorwaarden van hun beroepsaansprakelijkheidsverzekering. Een dekking van enkele honderdduizenden euro's per geval is minimaal te verwachten. Op deze manier verzekert u zich ervan dat eventuele schade ook daadwerkelijk kan worden vergoed.

Tevens zegt de aanwezigheid van een dergelijke verzekeringspolis iets over de soliditeit en betrouwbaarheid van de leverancier.

3.9 Overige randvoorwaarden

Stel in de offerteaanvraag, indien relevant, ook de volgende eisen:

- De tester moet alle bevindingen na afloop van de test overhandigen of vernietigen, om het uitlekken van gevoelige informatie te voorkomen.
- Als de tester privacygevoelige informatie in kan zien, spreek dan af hoe de tester daarmee omgaat?
- De IP-adressen die gebruikt worden voor het uitvoeren van de test moeten vooraf worden overlegd, zodat de opdrachtgever weet of een aanval onderdeel is van de penetratietest of toevallig een gelijktijdige kwaadaardige aanval is.

3.10 Communicatie

Goede communicatie tussen opdrachtgever en opdrachtnemer is essentieel om misverstanden en incidenten te voorkomen en te zorgen dat de pentest ongestoord verloopt.

Stel daarom in de offerteaanvraag eisen aan de communicatie. Dat kan bijvoorbeeld door een communicatieparagraaf op te nemen met daarin een overzicht van doelgroepen, communicatieboodschap, overlegmomenten, bereikbaarheid tijdens de pentest, het regelen van één aanspreekpunt voor de testers etc.

4 LEVERANCIERSELECTIE

In de offerteaanvraag heeft u de eisen aan de penetratietest vastgelegd. Verschillende leveranciers hebben daarop een offerte gebaseerd en nu moet u daaruit de beste kiezen. Dit hoofdstuk biedt u hiervoor enkele handreikingen.

4.1 Wegingsfactoren

Offertes bevatten standaard verschillende onderdelen (zie het hoofdstuk hiervoor):

- Kwaliteit (waaronder rapportage, testers, methodiek, organisatie)
- Planning
- Kosten
- Voorwaarden

De mate waarin elk onderdeel meeweegt in een eindoordeel is afhankelijk van u als de opdrachtgever. U bepaalt de weging voordat u met de selectie begint. De weging zal vooral worden beïnvloed door factoren vanuit uw eigen organisatie; bij een pentest als onderdeel van een project waarbij de planning strak is, zal het onderdeel planning zwaarder meewegen. Als uw budget krap is, kunt u het onderdeel kosten zwaarder laten meewegen.

4.2 Kwaliteit

De algemene kwaliteit van de offerte wordt bepaald door de mate waarin de activiteiten van de offerte het gestelde doel bereiken. Specifieke onderwerpen waarover een oordeel kan worden geveld zijn:

De rapportage

Wordt voldaan aan de rapportage-eisen die in de offerteaanvraag staan gesteld? Als voorbeeldrapportages zijn verstuurd kunnen ze gebruikt worden om een inschatting te maken van de kwaliteit van de rapportage.

De tester(s)

Aan de hand van de CV's kan een beoordeling gemaakt worden van de kwaliteit van de testers. Een relevante beveiligingscertificering (bijv. CISSP, CPTS, CPTE, CPTM[2]), ervaring of reputatie kan een indicatie geven van de expertise op beveilingsgebied.

[2] Certified Information Systems Security Professional, Certified Penetration Testing Specialist|Expert|Master

Ook de integriteit van de tester(s) is van belang. U laat mensen ‘inbreken’ en mogelijk bij zeer waardevolle informatie komen. Het is een tijdje mode geweest om (voormalige) criminele hackers in te huren vanwege hun (veronderstelde) vaardigheden; het is zeer de vraag of u daarmee zaken wilt/mag doen.

Blijkt uit de CV’s dat de individuele testers en het bedrijf als geheel al eerder vergelijkbare projecten succesvol hebben uitgevoerd?

De methodiek

Goede methodieken zijn bijvoorbeeld gebaseerd op de Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP) of de NIST Guideline on Network Security Testing. Wat ook van belang kan zijn is het gebruik van op maat gemaakte testscripts, wanneer het te testen systeem uniek is.

De organisatie

Het is belangrijk dat de leverancier onafhankelijk is. Als deze bijvoorbeeld een geheimhoudingsverklaring heeft afgesloten met de maker van het te testen product, of er een financiële relatie mee heeft, zou dat de resultaten van de penetratietest kunnen beïnvloeden.

Ook kunt u leveranciers op bedrijfseconomische aspecten beoordelen. Te denken valt aan zaken als continuïteit (hoe lang bestaat het bedrijf al, hoe groot is het) of beroepsaansprakelijkheid (is de leverancier verzekerd voor het geval er iets misgaat – multinationals eisen vaak van leveranciers in deze sector dat ze voor minimaal 1 miljoen euro verzekerd zijn).

4.3 Planning

De planning, specifiek de doorlooptijd, kan van groot belang zijn wanneer er sprake is van harde deadlines, bijvoorbeeld voor de oplevering van een product. Let bij beoordeling van de planning op garanties die de aanbieder geeft over de uitvoering en oplevering en de manier waarop de aanbieder de planning onder controle gaat houden.

4.4 Kosten

Een aspect dat relatief gemakkelijk onderling te vergelijken is, is de prijs van de offerte. Let daarbij wel op de kostenstructuur. Er kan een vaste prijs worden aangeboden maar ook een indicatie van een totaalprijs waarbij op basis van nacalculatie achteraf het werkelijk gemaakte aantal uren in rekening wordt gebracht. Dat laatste hoeft niet onredelijk te zijn, want het verloop van een pentest is nu eenmaal afhankelijk van wat de tester tegenkomt. De vraag is wie het risico draagt dat er meer werk is dan verwacht. Bij een vaste prijs ligt dat bij de leverancier, bij nacalculatie bij u als opdrachtgever. Een middenweg kan zijn om af te spreken dat bij een nacalculatiebenadering niet zonder onderlinge overeenstemming meerkosten zullen worden gemaakt.

4.5 Voorwaarden

De juridische voorwaarden spelen ook een rol in de keuze voor de leverancier. Denk aan de algemene voorwaarden die van toepassing zijn; zijn dat de voorwaarden van de leverancier of van de opdrachtgever? Maar ook zaken als aansprakelijkheid, verzekeringen, geheimhouding- en vrijwaringverklaringen spelen hierbij een rol. Meer informatie hierover staat in bijlage B.

5 DE UITVOERING

Als eenmaal een leverancier is geselecteerd dan is het als opdrachtgever van belang om op de volgende zaken te letten:

- Zorg dat communicatielijnen duidelijk zijn;
- Tref intern de juiste organisatorische maatregelen ter voorkoming van onnodige escalatie;
- Laat u goed op de hoogte houden.

In dit hoofdstuk worden deze zaken nader toegelicht.

5.1 Communicatie

Bij leverancier en opdrachtgever moet helder zijn hoe de communicatielijnen lopen. Een vast contact, of mogelijk twee vaste contacten (projectmanagementcontact en technisch contact) moeten beschikbaar zijn bij de opdrachtgever. Een leverancier zal u ook om dergelijke contactpersonen vragen, waarbij vooral van belang is wie aan uw kant het zogenaamde *Trustee Contact* is.

De pentesters zullen tussentijdse meldingen van ernstige zaken direct willen melden bij hun opdrachtgever; u kunt dat ook van hen eisen. Dat kan over gevoelige zaken gaan; het Trustee Contact is daarbij per definitie voor de pentesters vertrouwd.

Het komt ook voor dat een bevinding persoonlijk met het Trusted Contact te maken heeft. De pentesters ontdekken bijvoorbeeld een systeem waarop u als Trusted Contact rechten heeft die u helemaal niet zou moeten hebben en die u theoretisch in staat stellen om fraude te plegen. Maak hierover van tevoren goede afspraken; spreek af dat ook deze zaken gewoon met u worden besproken, of spreek met uw leidinggevende af dat hij in zo'n speciaal geval als 'terugvalcontact' functioneert.

5.2 Voorkoming van escalatie

Tijdens de pentest moeten technisch beheerders van de te testen systemen direct contact kunnen leggen met de pentesters en vice versa. Bij storingen in een operationeel systeem zal een beheerder namelijk direct de test willen stopzetten om deze als mogelijke oorzaak van de storing uit te sluiten. Als u de technisch beheerders niet op de hoogte brengt van de pentest, zorg dan dat bij een storing iemand in de 'meldingsketen' direct daarboven op de hoogte is van de test en de testers onmiddellijk kan informeren.

Dezelfde maatregel is van belang om detectie van de pentest niet onnodig te laten escaleren als beveiligingsincident; iemand in de keten van escalatie moet kunnen

vaststellen en verifiëren dat het om een geplande pentest gaat. Andersom moet ook helder zijn hoe de pentest te herkennen is (liefst afkomstig van één en hetzelfde IP-adres), zodat een echte inbraak niet ten onrechte voor de pentest wordt aangezien.

5.3 Informatie over de voortgang

Laat u gedurende het project regelmatig op de hoogte houden over de voortgang. Vraag desnoods al bij de offerteaanvraag hoe de leverancier u gedurende het project op de hoogte houdt. Niet alleen houdt u zo meer grip op het project, ook helpt het de kwaliteit van de resultaten te verbeteren als u al gedurende de tests in staat bent om feedback te geven aan de testers.

Uiteraard is dit vooral van belang bij grotere testtrajecten met een brede scope; bij een pentest van één systeem of website zijn dagelijkse updates minder belangrijk.

6 RESULTATEN

Het resultaat van een pentest is een rapport met bevindingen. Dit hoofdstuk gaat in op dit resultaat.

6.1 Wat betekent het resultaat voor u?

Het eindrapport van een pentest bevat een heldere omschrijving van wat, wanneer en hoe getest is. Daarnaast bevat het een algemene conclusie, aanbevelingen en een overzicht van individuele technische bevindingen met bijbehorende aanbevelingen.

Realiseert u zich dat het eindrapport altijd een de visie van de tester blijft; een pentest houdt geen rekening met het relatieve belang van uw informatie binnen uw bedrijfsproces; het is aan u als opdrachtgever om uiteindelijk een eigen interpretatie te geven aan de bevindingen en aanbevelingen. U kunt dan bij het vaststellen van de risico's rekening houden met uw eigen bedrijfsprocessen.

6.2 Wat doet u ermee?

Een groot risico is dat de resultaten van een penetratietest niet worden opgepakt binnen uw organisatie. Zoek, om dit te voorkomen, aansluiting bij een volgsysteem voor auditbevindingen, waarover de interne rekenkamer (de financiële, organisatorische of EDP-auditors) mogelijk beschikt. Dat garandeert dat bevindingen in beeld blijven totdat ze ofwel zijn opgelost, ofwel door het management geaccepteerd.

Als uw organisatie niet over een dergelijk volgsysteem beschikt is het een alternatief om de opvolging van de eigenlijke pentest als een aanvullende fase in het gehele project te definiëren of om hiervoor een nieuw project te starten. Hiermee belegd u duidelijk de verantwoordelijkheid voor het verwerken van de resultaten en kunt u voorkomen dat de resultaten niet worden opgepakt omdat de reguliere dagelijkse werkzaamheden een hogere prioriteit krijgen.

TIP: u kunt uw leverancier als extra controle vragen om een korte hertest van de bevindingen na 3, 6 en/of 9 maanden. Een hertest van gedane bevindingen kost niet veel tijd en geld en laat u precies zien of de bevindingen zijn opgevolgd. U kunt een dergelijke hertest al in de initiële offerteaanvraag opnemen.

7 CONCLUSIE

Een penetratietest inkopen is complex; het omvat onder andere de scope, vrij te geven informatie, en testmethodiek, daarnaast spelen juridische afspraken, kwaliteitsbeoordeling en communicatie een rol. Per onderdeel moet een keuze gemaakt worden die het beste aansluit bij de doelstelling van de penetratietest.

In dit white paper is het hele traject van een penetratietest behandeld, van de offerteaanvraag tot aan het verwerken van de resultaten. Hiermee is de lezer in staat om een passende penetratietest uit te laten voeren, met minimale risico's voor de organisatie en een maximaal rendement.

BIJLAGE A: LITERATUURLIJST

Nr	*Omschrijving*
[1]	http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf Guideline on Network Security Testing - NIST
[2]	http://www.sans.org/reading_room/whitepapers/auditing/conducting_a_penetration_test_on_an_organization_67 Conducting a Penetration Test on an Organization - SANS
[3]	http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf OWASP Testing Guide - OWASP
[4]	http://isecom.securenetltd.com/osstmm.en.2.1.pdf Open-Source Security Testing Methodology Manual - OSSTMM

BIJLAGE B: JURIDISCHE ZAKEN

Strafrecht en vrijwaringverklaringen

Naast de voornoemde technische en tactische aspecten aan een penetratietest zijn er enkele juridische dimensies die aandacht vereisen. Sinds november 2006 omschrijft het wetboek van Strafvordering het delict computervredebreuk als volgt:

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan.

Essentieel in deze omschrijving zijn de voorwaarden voor opzettelijkheid en wederrechtelijkheid. Met wederrechtelijkheid wordt bedoeld dat de handeling in strijd moet zijn met het recht. Dit betekent onder andere dat er geen toestemming is gegeven door de rechtmatige eigenaar van de geautomatiseerde werken.

Met opzet wordt bedoeld dat er sprake moet zijn van het oogmerk om wederrechtelijk binnen te dringen.

In het geval van een penetratietest zal er in beginsel altijd sprake zijn van opzet op het binnendringen, dit is immers het achterliggende doel van de test. Aan deze voorwaarde zal dus zonder meer voldaan worden. Het gevaar op het verrichten van een strafbare daad door de uitvoerder van de test ligt op de loer.

Om dit te voorkomen is het essentieel de wederrechtelijkheid aan de daad te ontnemen. Dit kun u doen door de uitvoerende partij, voor het begin van de pentest, te vrijwaren door middel van het ondertekenen van een vrijwaringverklaring. In een dergelijke verklaring wordt in ieder geval het volgende aangegeven:

VOORBEELD STRAFRECHTELIJKE VRIJWARINGSVERKLARING:

- het analyseren en/of binnendringen van en/of in het geautomatiseerd werk van de opdrachtgever, waarbij de beveiliging van het systeem wordt geanalyseerd en/of doorbroken en/of de toegang wordt verworven met behulp van valse signalen of een valse sleutel dan wel een valse hoedanigheid wordt aangenomen, een en ander zoals bedoeld in Artikel 138a Wetboek van Strafrecht, dan wel iedere poging daartoe;

- het verzenden van computervirussen en/of Trojan Horses naar e-mailadressen en systemen binnen de organisatie van de opdrachtgever, beperkt tot door de opdrachtgever aangegeven onderdelen van het geautomatiseerd werk; (indien van toepassing)

geschiedt **in opdracht** van en op **uitdrukkelijk verzoek** van de opdrachtgever.

Aansprakelijkheid

Behalve het risico op het verrichten van een strafbare handeling moet u ook rekening houden met de aansprakelijkheid voor eventuele schade die een penetratietest kan veroorzaken. Deze schade kan niet alleen optreden bij u als opdrachtgever, maar het is ook mogelijk dat een derde partij nadeel ondervindt. Als u geen afspraken maakt over wie er verantwoordelijk is voor deze schade is de kans op misverstanden en juridisch getouwtrek groot. Om die reden is het aan te raden in de vrijwaringverklaring tevens een verklaring op te nemen die hier duidelijkheid in schept.

Uitgangspunt is hierbij dat de leverancier zijn werk op een normale wijze kan verrichten, zonder dat zij aansprakelijk gehouden kan worden voor schade die optreedt als gevolg hiervan. Het is bijvoorbeeld voor te stellen dat een geslaagd binnendringen in een operationele omgeving bepaalde diensten binnen deze omgeving ontoegankelijk maakt. Als een dergelijke situatie het gevolg is van de normale werkzaamheden van de leverancier – deze is immers ingehuurd om te proberen binnen te dringen – zal deze geen aansprakelijkheid voor de ontstane schade willen en kunnen dragen.

Wanneer de schade echter het geval is van handelen buiten de scope van de opdracht zal de leverancier wel aansprakelijkheid moeten erkennen. Dit zou bijvoorbeeld het geval zijn wanneer er was afgesproken enkel op een testomgeving te werken en de leverancier desondanks toch op de productieomgeving schade heeft veroorzaakt.

Een dergelijke verklaring zou als volgt kunnen luiden:

VOORBEELD VRIJWARINGSVERKLARING:
Leverancier is niet aansprakelijk voor enige schade, gevolgschade daaronder begrepen, en is in geen geval gehouden tot vergoeding van bedrijfsschade, winstderving, schade voortvloeiende uit aanspraken van derden jegens de opdrachtgever of welke andere schade dan ook, veroorzaakt door het analyseren en/of binnendringen dan wel iedere poging tot het analyseren en/of binnendringen van het geautomatiseerde werk van de opdrachtgever.

Deze handelingen voltrekken zich onder de uitdrukkelijke voorwaarde dat leverancier uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door de opdrachtgever aangegeven onderdelen van het geautomatiseerd werk.

Het is denkbaar dat de penetratietest van de leverancier naast schade bij de opdrachtgever ook nadeel voor derde partijen oplevert. In het eerdere voorbeeld van een operationele omgeving waarop diverse diensten ontoegankelijk worden naar aanleiding van een penetratietest, zouden de gebruikers van deze diensten hier aanzienlijke schade door kunnen leiden. Denk bijvoorbeeld aan banken en hun internetbankierdiensten.

Om te voorkomen dat de leverancier hiervoor op moet draaien zal hij in zijn vrijwaring zonder twijfel een bepaling over aansprakelijkheid jegens derden willen opnemen:

> Opdrachtgever vrijwaart leverancier van iedere (verdere) aansprakelijkheid die jegens derden op leverancier zou kunnen rusten met betrekking tot door leverancier verrichte diensten.

Ook in dit geval geldt weer dat wanneer de leverancier buiten de scope van de opdracht heeft gehandeld, hij wel aansprakelijk gesteld kan worden.

Verzekering

In het geval dat er schade wordt veroorzaakt waar de leverancier toch aansprakelijk voor is, is het van belang dat de leverancier wel in staat is om de schade te vergoeden. Ook bij een klein onderzoek kan het om relatief grote bedragen gaan.