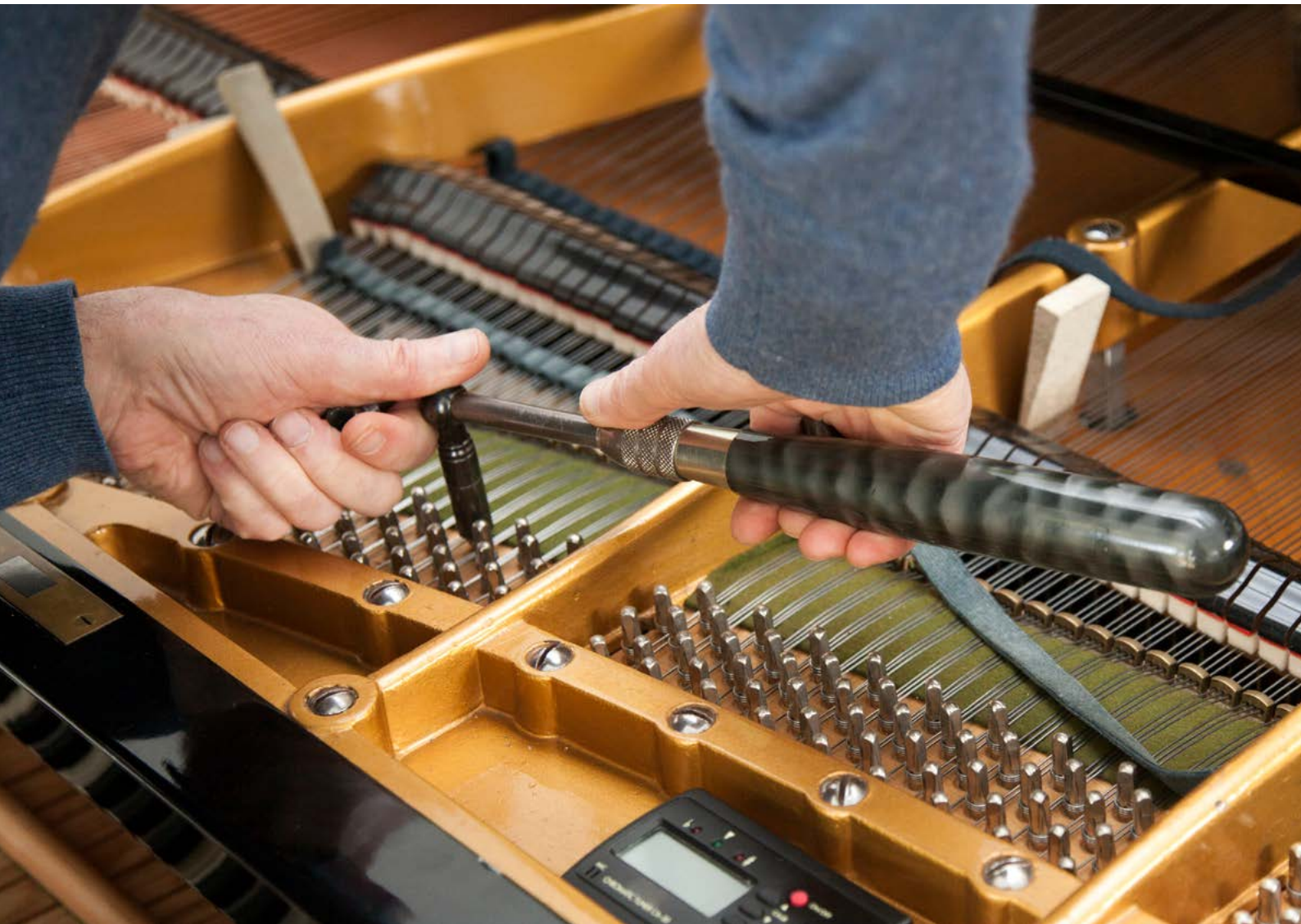
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Whitepaper securitytesten



Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

De volgende partijen hebben in belangrijke mate bijgedragen aan de kwaliteit van deze whitepaper:

- Auditdienst Rijk
- BDO
- Belastingdienst
- Capgemini
- Deloitte
- Fox-IT
- Informatiebeveiligingsdienst voor gemeenten
- Logius
- Ministerie van Buitenlandse Zaken
- Ministerie van Economische Zaken en Klimaat
- Ministerie van Justitie en Veiligheid
- Nationale Politie
- OWASP
- Port of Amsterdam
- PwC
- Radically Open Security
- Rijkswaterstaat
- Secura
- Securify
- Software Improvement Group
- Sogeti
- UWV

Inhoudsopgave

Inleiding

Securitytesten bieden inzicht in kwetsbaarheden en de bijbehorende risico's van een informatiesysteem. Dit stelt de organisatie in staat om te leren en de juiste beveiligingsmaatregelen effectiever toe te passen, waardoor de weerbaarheid van de organisatie wordt verhoogd. Bovendien is securitytesten een vereiste om te voldoen aan diverse security- en privacyregelgevingen. De betrouwbaarheid van informatiesystemen is cruciaal voor het goed functioneren van organisaties. Effectieve beveiligingsmaatregelen dragen bij aan de betrouwbaarheid van zowel de dienstverlening als de bedrijfsvoering. Securitytesten geven een realistisch beeld van de kwaliteit van de geïmplementeerde beveiligingsmaatregelen.

Dit is een handleiding voor opdrachtgevers van een securitytest

Een goede opdrachtformulering en gedegen regie op de uitvoering van een securitytest zorgen voor een resultaat dat aansluit op de behoefte van de opdrachtgever.

Idealiter leveren securitytests geen grote verrassingen op, maar geven ze een bevestiging van de kwaliteit van het ontwikkelproces. Achteraf kijken of iets toevallig veilig is geworden zorgt dikwijls voor vervelende verrassingen en vertragingen. Een algemene regel luidt dat hoe eerder tijdens de ontwikkeling een beveiligingskwestie wordt ontdekt, hoe eenvoudiger en goedkoper deze verholpen kan worden.[1]

Laat de securitytest dus geen compensatie zijn voor het ontbreken van voldoende aandacht voor security tijdens de ontwikkeling, maar een middel om een mate van zekerheid te krijgen, te leren en verder te verbeteren.

Jij bent de opdrachtgever

Deze whitepaper is als wegwijzer bedoeld voor securitytests die kunnen worden toegepast op informatiesystemen die in gebruik zijn of in gebruik genomen gaan worden. Een securitytest kan in diverse situaties aan de orde zijn.

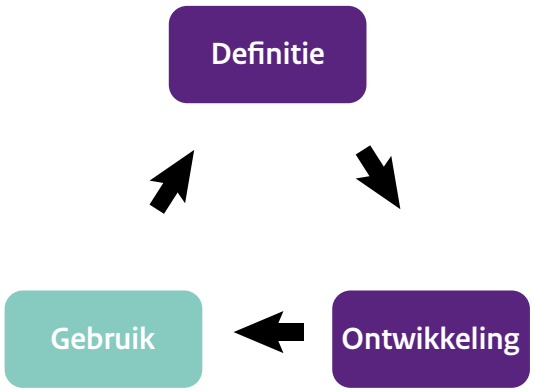
- Een security officer wil inzicht in de kwetsbaarheden van zijn ict-landschap.
- Een projectleider wil het beveiligingsniveau van een informatiesysteem op de proef stellen en weten in hoeverre aan de beveiligingseisen wordt voldaan.
- Een deliverymanager wil aantonen dat het geleverde product of dienst tegen bepaalde dreigingen bestand is.
- Een applicatie-eigenaar wil aantonen dat een applicatie geen bekende kwetsbaarheden bevat.
- Een productmanager wil de broncode van een product laten testen op kwetsbaarheden.

[1] Zie: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software

Een passende securitytest op het informatiesysteem

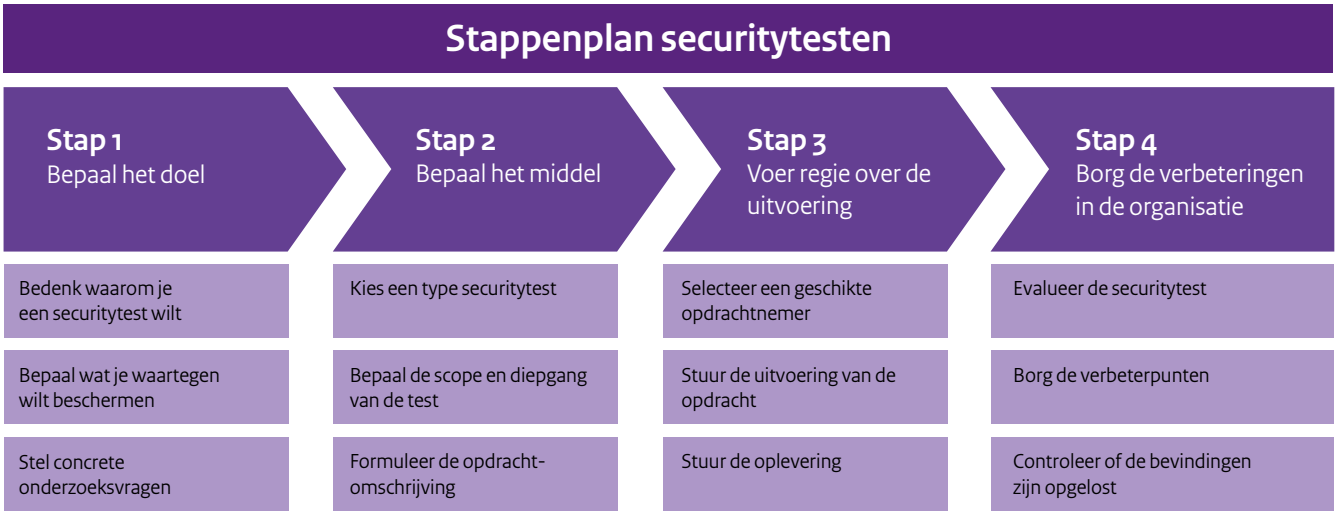
Deze whitepaper richt zich op het proces van het organiseren van een passende securitytest en hoe u daar sturing aan kunt geven. Dit is afhankelijk van uw specifieke situatie en de verschillende manieren waarop het actuele beveiligingsniveau van een informatiesysteem kan worden getoetst.

Figuur 1. Geeft een overzicht van de opdeling van het ontwikkelproces van een informatiesysteem. Hoewel het totale proces uitgebreider is, zijn voor het begrip en toepassing van de whitepaper grofweg drie fases gedefinieerd: definitie, ontwikkeling en ingebruikname. In elk van die fasen zijn verschillende vormen van securitytests van toepassing. De focus van deze whitepaper ligt op securitytests op een informatiesysteem dat in gebruik is, of klaar is om in gebruik te nemen.



Figuur 1. De levenscyclus van een informatiesysteem

Ga als volgt te werk



- **Stap 1: Bepaal het doel**
  Bepaal wat je waartegen wilt beschermen en welke inzichten je wilt krijgen.

- **Stap 2: Bepaal het middel**
  Bepaal welk type securitytest en welke opties het best passen bij de situatie en het doel. Hiermee maak je de opdrachtformulering voor de opdrachtnemer.

- **Stap 3: Voer regie over de uitvoering**
  Bepaal welke criteria voor jouw organisatie en securitytest het meest van belang zijn om tot selectie van een leverancier te komen en stuur de uitvoering van de opdracht.

- **Stap 4: Borg de verbeteringen in uw organisatie**
  Zorg voor een interne evaluatie door betrokkenheid van de verantwoordelijken en borg de voorgestelde verbeteringen.

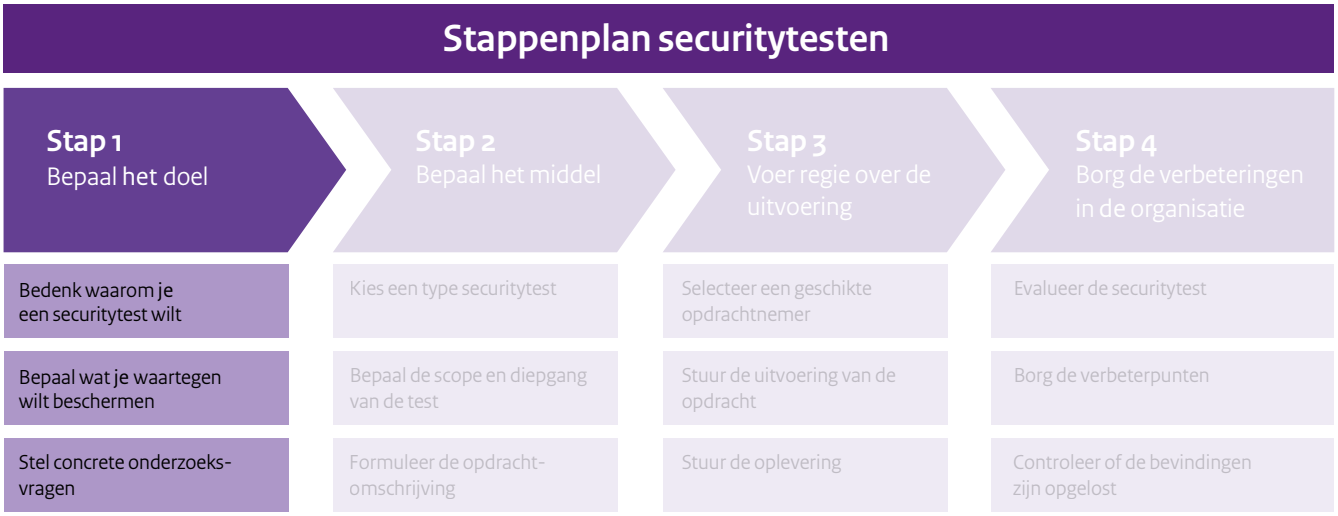
Om de meeste toegevoegde waarde te verkrijgen uit een security-test moeten er een aantal zaken worden voorbereid. Dan ben je gereed voor de daadwerkelijke uitvraag, afstemming met een opdrachtnemer, uitvoering en borging van de verbeteringen in de eigen organisatie.

Stap

1

Stap 1 Bepaal het doel

Stap 1 gaat over het vaststellen van wat u wilt bereiken met een securitytest. Daarvoor wordt hier ingegaan op het waarom, wat u waartegen wilt beschermen en wat voor inzichten als resultaat u daarvoor nodig heeft. In de vervolgstappen wordt ingegaan op het bereiken daarvan. Drie vragen helpen u om het doel van de test vast te stellen. Bedenk waarom u een securitytest wilt



1.1 Bedenk waarom je een securitytest wilt

De aanleiding voor het organiseren van een securitytest is vaak gerelateerd aan het securitybeleid, bijvoorbeeld bij grote veranderingen in de ict-infrastructuur of het opslaan en verwerken van een bepaald type gevoelige informatie. Soms wil de organisatie zekerheid over de continuïteit van dienstverlening, een positieve differentiator ten opzichte van concurrenten, of bevestiging dat een aangeschaft product bestendig is tegen misbruik. Organisaties adopteren ook diverse securitystandaarden waarin vaak een vorm van een periodieke securitytest wordt vereist.

Wet- en regelgeving kunnen ook aanleidingen zijn van een securitytest. Voorbeelden zijn NIS2 de Cyberbeveiligingswet[2] met betrekking tot de zorgplicht voor vitale infrastructuur en het melden van beveiligingslekken, organisaties die DigiD gebruiken als authenticatiemiddel, de AVG[3] met betrekking tot het verkrijgen van een bepaalde mate van zekerheid of toepasselijke securitymaatregelen zijn getroffen of de BIO[4] voor overheidsorganisaties.

[2] https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

[3] Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg

[4] Zie: https://www.communicatierijk.nl/vakkennis/r/rijkswebsites/verplichte-richtlijnen/baseline-informatiebeveiliging-rijksdienst

1.2 Bepaal wat je waartegen wilt beschermen

Zorg dat je vooraf de juiste vragen stelt zodat de behoeftestelling concreet en duidelijk naar een uitvoerder gecommuniceerd kan worden.

- Welke gegevens wil je beschermen?
- Welk niveau van bescherming heb je nodig?
- Tegen welke scenario's wil je in welke mate bestand zijn?
- Ligt de nadruk op beschikbaarheid, integriteit, vertrouwelijkheid of een combinatie daarvan?
- Betreft het alleen de infrastructuur en applicatie, of is er behoefte om ook organisatie-aspecten mee te testen?

Twee activiteiten die onderbouwing bieden voor wat je waartegen wilt beschermen en waarom, zijn de risicoanalyse en dreigingsanalyse. De expertise van degenen die deze activiteiten uitvoeren bepalen in sterke mate de kwaliteit van de resultaten van de risicoanalyse en dreigingsanalyse. Betrek daarnaast ook de juiste belanghebbenden. Het betrekken van experts aan de opdracht-geverskant helpt om de vaak aanwezige kennisasymmetrie te minimaliseren, zodat er een goede discussie kan worden gevoerd met een uitvoerder, wat uiteindelijk bijdraagt om de juiste antwoorden te krijgen op de juiste vragen.

Een vaak voorkomende bron van verwarring bij het aanvragen van een securitytest is een te algemene omschrijving van de test. In het geval van een penetratietest kan een aanvaller bijvoorbeeld op verschillende manieren binnendringen. Wees daarom specifiek in de behoeftestelling. Bijvoorbeeld: ik wil testen of een kwaadwillende medewerker, bij andere gegevens kan komen dan van

zichzelf. Doordat een test vaak beperkt is in tijd, is het belangrijk dat de uit te voeren tests passen bij de specifieke zorgen die er zijn ten aanzien van de te beschermen belangen.

1.3 Stel concrete onderzoeksvragen

Maak vooraf helder welke inzichten er als resultaat nodig zijn om de juiste middelen te bepalen voor de securitytest. Soms blijven onderzoeksvragen te abstract geformuleerd, zoals “is het systeem te hacken?”; elk systeem is te hacken met genoeg tijd en middelen. Het gevaar wanneer de vraag of de scope te vaag of te breed is, is dat de test waarschijnlijk te veel informatie oplevert, waardoor wat nodig is ondergesneeuwd raakt door het grote aantal bevindingen.

Wees daarom specifiek in de gewenste uitkomsten en scope die daarbij horen. Bepaal vanuit de aanleiding op businessniveau de benodigde resultaten en vertaal die naar specifieke onderzoeksvragen. Zo kan gericht getest worden.

Voorbeelden van benodigde resultaten	Voorbeelden van specifieke onderzoeksvragen
Inzicht in de effectiviteit van ict-controlemaatregelen	Hoe kunnen ongeautoriseerde personen toegang tot specifieke bedrijfsgegevens verkrijgen?
Inzicht in de mate van security-awareness	In hoeverre is het personeel zich bewust van de risico’s van een phishingaanval? In welke mate is de organisatie kwetsbaar voor dit type aanval?
Laaghangend fruit ontdekken	Welke informatie en kwetsbaarheden zijn vanuit ongeautoriseerd perspectief van een specifiek systeem te onthullen?
Ontwikkelaars laten leren	Wat kunnen de ontwikkelaars leren over hoe bepaalde securityverbeteringen gedaan kunnen worden op basis van de bevindingen?
Inzicht in het beveiligingsniveau van een systeem	In welke mate ben ik weerbaar tegen bepaalde dreigingen? Ben ik kwetsbaar voor een bepaalde dreiging, bijvoorbeeld tegen besmetting van ransomware?

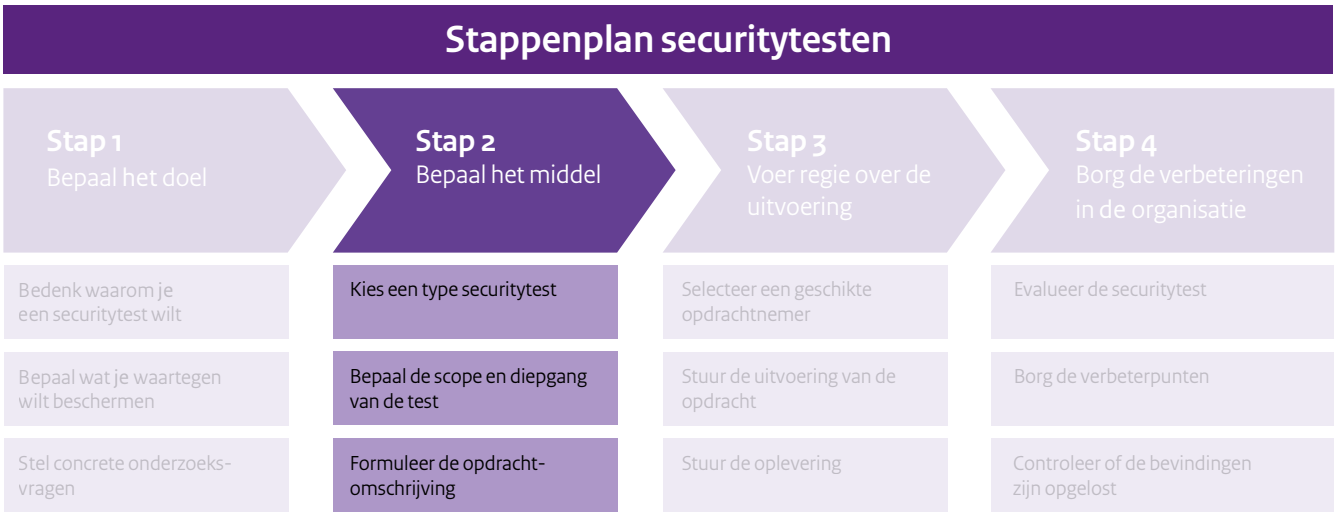
Tabel 1. Enkele veelgezochte inzichten als resultaten

Stap

2

Stap 2 Bepaal het middel

Nu de doelstelling is ingekaderd, is het zaak om een passende securitytest te kiezen. Hiervoor maakt je een securitytestprofiel waarmee er een opdrachtomschrijving voor de opdrachtnemer kan worden opgesteld.



2.1 Kies een type securitytest

Verschillende dienstverleners kunnen afwijkende terminologie gebruiken voor de verschillende typen securitytests. Deze whitepaper hanteert de verklaringen uit het Cybersecurity Woordenboek.[5]

Vanwege de afbakening van deze whitepaper worden fysieke toegang, social engineering, coordinated vulnerability disclosure, bug bounty en red teaming niet behandeld.[6]

2.1.1 Een vulnerability-assessment is breed

Scan met een vulnerability-assesment om zo breed mogelijk te testen. Scan op ontbrekende patches en bekende kwetsbaarheden, zwakke securityconfiguraties zoals standaardwachtwoorden of onvoldoende encryptie, onveilig ingestelde netwerkservices, veelvoorkomende webapplicatie-issues of informatielekken.

Vulnerability-assessments worden gebruikt voor testen op bekende kwetsbaarheden in de breedte. De securitytester laat zien dat er een kwetsbaarheid gedetecteerd is maar hij maakt geen daadwerkelijk misbruik van deze omissie in de beveiliging en probeert niet de systemen verder binnen te dringen. Dit is handig voor de snelheid van de test of wanneer er zeer kritieke objecten onderzocht worden, waarbij men niet verder wil testen dan de oppervlaktetesten vanwege mogelijke onberekenbare vervolgschade door bijvoorbeeld verouderde technologie.

2.1.2 Een penetratietest gaat diep

Een penetratietest gaat in plaats van de breedte de diepte in. Bij een penetratietest (ook wel pentest), zal een daarvoor getrainde pentester zoeken naar kwetsbaarheden en deze proberen uit te buiten, gebruikmakend van uiteenlopende tools en handmatige procedures, afhankelijk van de afgesproken onderzoeksvragen en scope. De opdrachtgever kan dan inzicht krijgen hoe moeilijk het is om daadwerkelijk kwaad te doen met de gevonden kwetsbaarheid.

In sommige gevallen heeft een pentest pas meerwaarde wanneer het vulnerability-assessment en het proces om die bevindingen te verhelpen opgezet en werkend is.[7] Als een organisatie nog geen vulnerability-assessment heeft uitgevoerd en de bevindingen verholpen heeft, dan zal een pentest minder effectief zijn, omdat veel van de kwetsbaarheden ook gevonden hadden kunnen worden met een lichter middel, te weten een vulnerability-assessment. Daardoor gaat tijd verloren die ook gebruikt had kunnen worden om te zoeken naar kwetsbaarheden die moeilijker vindbaar.

[5] Zie: https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/

[6] Het NCSC heeft een leidraad voor coordinated vulnerability disclosure, zie: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad. Zie voor andere testtypen ook: https://en.wikipedia.org/wiki/Social_engineering_(security) en https://www.darkreading.com/threat-intelligence/think-like-an-attacker-how-a-red-team-operates/d/d-id/1332861

[7] Zie: CIS Control 20: Procedures and Resources: https://www.cisecurity.org/controls/cis-controls-list/

Om als opdrachtgever meer inzicht te krijgen in de manier waarop dit soort tests plaatsvindt, kunt u kijken naar de diverse pentest-methodologieën die op een rij gezet zijn door bijvoorbeeld OWASP.[8] Overige details en advies hoe het meest uit penetratie-tests gehaald kan worden ook door het NCSC-UK uiteengezet.[9]

2.1.3 Een broncodereview is grondig

Een broncodereview is een inspectie van de broncode van een applicatie door een expert. Het doel van een broncodereview is het vinden van kwetsbaarheden in die broncode: het is een systematisch onderzoek naar programmeerfouten die tijdens de ontwikkeling over het hoofd zijn gezien. Deze securitytest van toepassing in de ontwikkelfase, maar ook in de gebruik- en beheerfase omdat de praktijk leert dat broncode nooit foutloos in gebruik wordt genomen. Achteraf worden er nog altijd fouten gevonden, zie bijvoorbeeld de onderdelen uit de OWASP Top 10 van riskante kwetsbaarheden in web-[10] en mobiele applicaties[11].

Een goede broncodereview vereist specifieke kennis van en vaardigheden in de gebruikte programmeertalen, frameworks, externe componenten en afhankelijkheden. Geautomatiseerde statische analyses, compositie-analyses en handmatige reviews zijn vaak onderdeel van een broncodereview.

2.2 Bepaal de scope en diepgang van de test

Naast de soorten securitytests die passen bij een bepaald volwassenheidsniveau, zijn er ook opties voor de breedte en diepgang van de test, die helpen om de opdrachtformulering in te kaderen.

2.2.1 Bepaal de scope van de test

Voor een goede securitytest is het belangrijk dat de scope van het te testen informatiesysteem duidelijk wordt vastgesteld. Dit is zowel van belang voor de volledigheid van de te verwachten testresultaten, als voor het voorkomen van overbodige testactiviteiten.

De inbreng van de systeemeigenaar, architect, technisch specialist en securityspecialist is nodig om de afhankelijkheden tussen de componenten aan te geven. Geef hierbij ook aan wat niet in scope zit van de test zodat de uitvoerders van de test geen verkeerde aannames kunnen doen.

- **Externe infrastructuur**
  Dit is de infrastructuur (ip-reeksen, VPN, firewalls) die vanaf het internet beschikbaar is. Alle kwaadwillenden kunnen deze bereiken.
- **Interne infrastructuur**
  Dit is de infrastructuur die achter de beschermende laag van bijvoorbeeld een VPN of firewall zit. Dit is ook belangrijk om te testen om “defense-in-depth” toe te passen. Wanneer een kwaadwillende door de VPN of firewall heen is, hoe ver kan deze dan op het netwerk komen en wat kan de eigenaar hiertegen doen? Ook een ontevreden werknemer die kwaad wil heeft dit uitgangspunt.
- **Applicatie**
  Een applicatie is een verzameling programmacode die een taak uitvoert, zoals een webapplicatie, script, mobiele applicatie of speciaal programma.
- **Organisatie**
  De organisatie is het verband van mensen en processen die samenwerken aan het organisatiebelang. Kwaadwillenden kunnen inspelen op mensen om hun handelingen te beïnvloeden of om processen te omzeilen. Dit wordt social engineering genoemd.

2.2.2 Bepaal de mate van binnendringen

Een andere variabele is hoe ver een securitytester mag gaan: de mate van binnendringen. Maak hierover vooraf duidelijke afspraken. Dit is gedeeltelijk inherent aan de keuze voor een vulnerability-assessment of een penetratietest. Bij een vulnerability-assessment laat een tester zien dat hij een kwetsbaarheid gedetecteerd heeft met een eenvoudige aanpak, waarbij in het algemeen niet verder wordt geprobeerd de in systemen binnen te dringen. Bij een pentest zal een tester naast het vinden van kwetsbaarheden, ook proberen deze uit te buiten, zoals een aanvaller zou doen. De opdrachtgever kan dan achterhalen hoe moeilijk het is om daadwerkelijk kwaad te doen met de gevonden kwetsbaarheid. Ongeacht het type securitytest kun je echter nadere afspraken maken met de opdrachtnemer.

2.2.3 Bepaal hoeveel informatie je vooraf aan de securitytesters geeft

De opdrachtgever kan ervoor kiezen om de testers te voorzien van informatie voorafgaand aan de test, afhankelijk van vanuit welk perspectief de test dient plaats te vinden. Daarvoor worden de volgende termen gebruikt:

- **Black box**
  Zonder informatie vooraf, de tester weet niets; enkel bijvoorbeeld een ip-adres, domeinnaam of bedrijfsnaam.
  Dit is vaak realistischer op het vlak van informatie die een echte aanvaller zou hebben, al heeft een aanvaller in de praktijk veel meer tijd. OSINT (Open Source Intelligence, openbaar beschikbare informatie via bijvoorbeeld internet) is hier een belangrijke bron van informatie voor de tester.

[8] Zie: https://www.owasp.org/index.php/Penetration_testing_methodologies
[9] Zie: https://www.ncsc.gov.uk/guidance/penetration-testing
[10] Zie: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[11] Zie: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks

- **Grey box**
  De tester heeft gedeeltelijke informatie vooraf, bijvoorbeeld inloggegevens van een gebruiker met een bepaalde rol binnen het systeem, zodat getest kan worden wat een aanvaller kan bereiken indien hij bepaalde rechten heeft in een systeem. Een ander voorbeeld is een tester toegang tot een gebouw geven om te testen hoe ver hij kan komen als de eerste beschermingslaag, de fysieke maatregelen in dit geval, is gepasseerd.
- **White box**
  De tester krijgt alle informatie vooraf, bijvoorbeeld ontwerpdocumentatie, inloggegevens, voorbeeldberichten en broncode, ook als er geen broncodereview wordt uitgevoerd. De termen crystal box en white box betekenen hetzelfde. Bij een whiteboxtest kan efficiënter getest worden binnen de beschikbare tijd. Een whiteboxtest is een type test waarbij informatie wordt verstrekt die normaal gesproken niet openbaar is, waaronder de broncode. Dit garandeert echter niet dat er een grondige codereview wordt uitgevoerd. Het kan zijn dat de code vooral wordt gebruikt om een pentest te sturen. Als het doel is dat ook een codereview wordt uitgevoerd, dan is het zaak dat er bij de test ook een gespecialiseerde codereviewer is betrokken en er daadwerkelijk gestructureerd wordt geoordeeld over het voor security relevante programmeer-werk. In de praktijk worden penetratietests en codereviews meestal door verschillende specialisten uitgevoerd.

2.2.4 Bepaal de diepgang van de securitytest

De mate van diepgang varieert per type securitytest. Een vulnerability-assessment is relatief oppervlakkig en eenvoudig en vergt minder moeite en een lager kennisniveau dan een penetratietest en een broncodereview, maar geeft veel mogelijk onjuiste bevindingen als er niet handmatig geverifieerd wordt. Een penetratietest gaat meer de diepte in en vereist meer moeite, creativiteit, doorzettingsvermogen en een hoger kennisniveau om minder gangbare kwetsbaarheden te vinden en zich via opstappunten toegang te verschaffen. Een broncodereview gaat het diepst doordat het de fundamenten van een applicatie inspecteert. Onafhankelijk van het type securitytest kun je afspraken maken met de opdrachtnemer over de gewenste diepgang.

2.3 Formuleer de opdrachtomschrijving

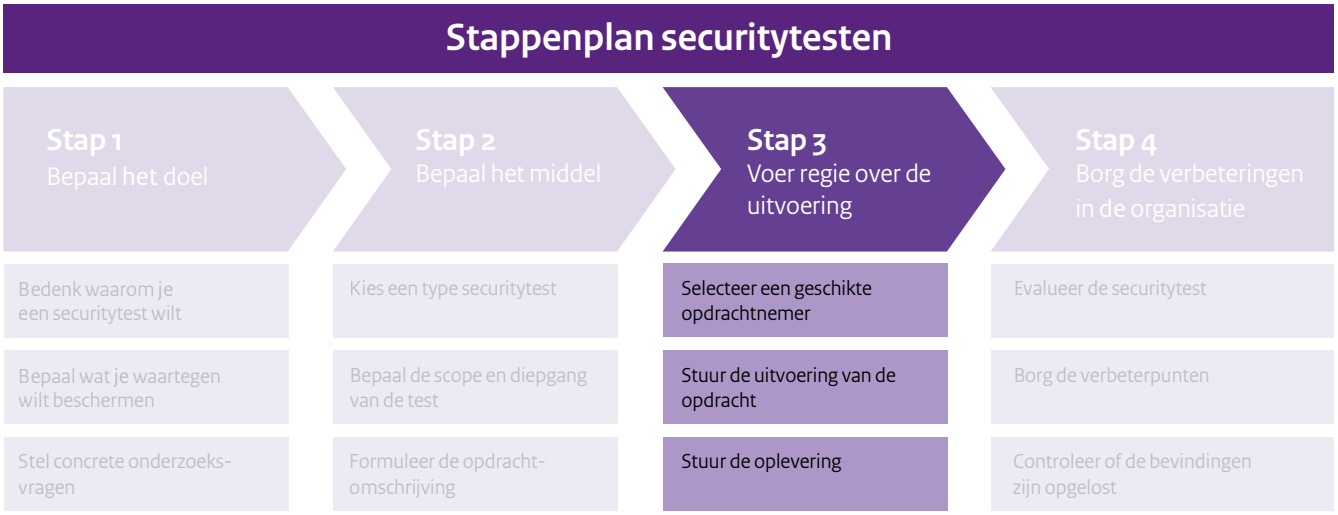
Gebruik de resultaten uit Stap 1 en 2 om tot een securitytestprofiel te komen. Dit is de input voor de opdrachtformulering. Werk daarin de eerder geformuleerde onderzoeksvragen uit, zodat een passende securitytest het juiste antwoord geeft. Gebruik het securitytestprofiel in Bijlage A om een opdracht op te stellen die in de markt kan worden uitgezet.

Stap

3

Stap 3 Voer regie over de uitvoering

Deze stap gaat verder in op het selecteren van een geschikte uitvoerder van de securitytest. Door te zorgen voor duidelijke afspraken, kan er worden gestuurd op een oplevering volgens verwachting. De getoonde drie vragen helpen daarbij.



3.1 Selecteer een geschikte opdrachtnemer

Je bent tot een eerste versie gekomen van de opdrachtformulering voor de securitytest. Ga met deze basis op zoek naar een match met een uitvoerende partij. Stel criteria op over wat voor jouw het belangrijkst is, om ervoor te zorgen dat de opdrachtnemer voldoet aan de verwachtingen. De interne of externe leverancier zal dan aan de meeste criteria moeten voldoen, maar uiteindelijk gaat het om de klik. Er moeten namelijk afspraken met elkaar worden gemaakt, communiceren en elkaar vertrouwen om de gewenste resultaten te krijgen. Dat werkt het beste wanneer de opdrachtgever en opdrachtnemer open en transparant met elkaar communiceren.

3.1.1 Stel een shortlist op

Op welke criteria kun je partijen die securitytests uitvoeren het beste vergelijken? Aangezien het om beveiliging gaat, en dus om gevoelige zaken, is het belangrijk zorgvuldig te overwegen welke opdrachtnemer in aanmerking komt. Houd rekening met de indicatoren betrouwbaarheid, kwaliteit en toegankelijkheid, waarbinnen jezelf de prioritering aanbrengt, zodat je beter voorbereid het selectieproces doorgaat. Dit helpt je om een shortlist op te stellen.

Betrouwbaarheid
- Vertrouwensrelatie
- Bescherming van testgegevens

Kwaliteit
- Solide reputatie, historie en ethiek
- Vakbekwame securitytesters, vaardigheden, referenties; ervaring met te testen technologieën of maatregelen
- Hoge kwaliteit van dienstverlening, toegevoegde waarde
- Kennis van de branche of organisatie
- Research & development-capaciteiten
- Voorbeeldrapportages

Toegankelijkheid
- Beschikbaarheid van testers en flexibiliteit
- Open & transparante communicatievorm

3.1.2 Onderhoud contact met potentiële opdrachtnemers

Als eenmaal een shortlist is gemaakt, moet er contact worden gehouden met potentiële opdrachtnemers tijdens het selectieproces. De initiële opdrachtformulering aan het eind van stap 2 is een goede basis voor wat je verwacht van de securitytest. Door in contact te blijven met de opdrachtnemer vergroot je de kans dat je krijgt wat je nodig heeft. Onderwerpen die vaak verdere toelichting behoeven zijn de scope, prioritering, budgettering en of betrokken partijen op de hoogte zijn van de testwerkzaamheden.

3.1.3 Voer een intakegesprek

Het hoofddoel van de intake is het verzamelen van de benodigde informatie, zodat de opdrachtnemer zijn voorstel (offerte of plan van aanpak) kan maken. Er dient een goede intake plaats te vinden waarin de opdrachtgever en opdrachtnemer op basis van risico's en dreigingen bepalen welke testactiviteiten nuttig zijn.

Voordat er een intake kan plaatsvinden met een potentiële opdrachtnemer, moeten er echter een aantal randvoorwaarden zijn ingevuld vanwege de gevoeligheid van de informatie rondom een securitytest.

- een geheimhoudingsverklaring waar de betrokken partijen akkoord mee dienen te gaan als maatregel tegen het uitlekken van gevoelige informatie;
- afspreken en vastleggen hoe wordt omgegaan met bevindingen die in aanmerking komen voor coordinated vulnerability disclosure (cvd);
- protocollen afspreken voor veilige communicatie, opslag en verwijdering van gegevens, en verspreiding van de rapportage, zodat de informatie en discussies rondom de test niet in de openbaarheid komen.

Als de voorwaarden zijn afgesproken waaronder de informatie gerelateerd aan de securitytest wordt uitgewisseld, kan een afspraak ingepland worden om de intake te laten plaatsvinden. Deze intake kun je het beste face-to-face houden, vanwege de gevoeligheid van de te delen informatie. Daarnaast draagt een face-to-face-intake bij aan het opbouwen van een vertrouwensrelatie met de testpartij, en het voorkomt aannames.

Om niet voor verrassingen te komen staan kun je in het intakegesprek of in vervolggesprekken ook kennismaken met de daadwerkelijke testers. Je wilt voorkomen dat bijvoorbeeld een bepaalde tester naar voren wordt geschoven in de aanbieding, terwijl de test uiteindelijk wordt uitgevoerd door een ander die niet aan het gezochte profiel voldoet.

Zorg dat er voldoende kennis in huis is of wordt gehaald om het organiseren van een securitytest te kunnen doorlopen. Met de juiste kennis kun je een risicoanalyse opstellen, een opdracht formuleren, regie voeren en de rapportage beoordelen. Wanneer deze kennis niet in huis is, tref dan compenserende maatregelen die onafhankelijk staan van de opdrachtnemer om verstrengeling van belangen te voorkomen. Betrek bijvoorbeeld advies bij een derde partij.

Verduidelijk de volgende aandachtspunten tijdens de intake en leg ze vast:
- doorspreken van het opgestelde securitytestprofiel en initiële opdrachtformulering door de opdrachtgever;
- discussie over de opdracht en uitleg hoe leverancier te werk gaat;
- uitleg van wat nadrukkelijk wel en niet in scope is;
- de prioritering van aandachtsgebieden binnen de test;
- bevestiging van de betrokken partijen en goedkeuringen die nodig zijn indien er componenten zijn die buiten de verantwoordelijkheid van de opdrachtgever vallen;
- toelichting op de risicoanalyse en uitwerking van de dreigingsanalyse met verdere input van de opdrachtnemer;
- verduidelijking van de aanleiding, doelstelling, beoogde resultaten en specifieke onderzoeksvragen;
- het plan van aanpak van de opdrachtnemer;
- planning, budget en opleveringsvorm;
- eventueel vervolg, planning van de hertest.

De intake geeft een opdrachtnemer ook de kans om uitgebreider in te gaan op verwachtingen van de opdrachtgever en de omvang van het te testen informatiesysteem. Dit draagt bij aan de definitieve offertestelling voor de test. Na verder vragen blijkt er vaak extra informatie naar boven te komen die anders op een later moment voor verwarring kan zorgen, zoals eigenaarschap, scope en afhankelijkheden. Als de intake naar tevredenheid is verlopen en er een akkoord wordt bereikt, dan is het zaak dat de afspraken duidelijk in het contract komen.

3.2 Stuur de uitvoering van de opdracht

Een gedegen voorbereiding voorkomt dat tests moeten worden uitgesteld of bepaalde resultaten niet worden behaald. Testers op de juiste manier faciliteren zorgt voor de randvoorwaarden voor een goede testuitvoering.

3.2.1 Bereid de uitvoering voor

Bepaalde aandachtspunten in de voorbereiding door de opdrachtgever kunnen een grote impact hebben op de test.

- methode van validatie en classificatie van bevindingen;
- testen van autorisaties (met en zonder testaccounts, black box, grey box of white box);
- inloggegevens;
- monitoring van aanvalspogingen;
- toestemming voor:
  - bruteforce-aanvallen (of bijvoorbeeld enkel offline);
  - testen die denial of service (verstoring van de dienstverlening) teweeg kunnen brengen;
  - testen op productie- of acceptatie-omgeving.
- whitelisting van de testers, dat wil zeggen het toestaan van bepaalde verkeersstromen afkomstig van de testers;[12]
- hoe om te gaan met scope wijzigingen tijdens de test: door wijzigingen in scope tijdens de test vanwege nieuwe inzichten, kan het voorkomen dat de test achteraf niet meer volledig de vooraf afgesproken scope dekt;
- duidelijkheid over de behoefte aan een hertest (binnen afzienbare tijd na afstemmen bevindingen);
- vrijwaringsovereenkomst met de betrokken partijen;
- Rules of Engagement (spelregels van de test);
- intakeformulier;
- afspraken hoe om te gaan met bevindingen met betrekking tot:
  - closedsource-broncode;
  - opensource-broncode.
- afspraken hoe om te gaan met verkregen documenten en bijvoorbeeld de broncode;
- documentatie die dient te worden opgeleverd (bijvoorbeeld inclusief onbewerkte output van tools of niet);
- pre-test of sanity check om te kijken of daadwerkelijk alles gereed is (bijvoorbeeld of de testomgeving extern bereikbaar is).

3.2.2 Faciliteer de uitvoering

Bepaalde aandachtspunten in de facilitering door de opdrachtgever kunnen een grote impact hebben op de test.

- Zorg voor een securitytestbegeleidersrol. Dit helpt bijvoorbeeld bij het opvangen van de testers op locatie.
- Zorg voor communicatie-afspraken:
  - vooraf aan de securitytest;
  - tijdens de securitytest;
  - na de securitytest.
- Informeer de betrokken systeem- en netwerkbeheerders.
- Zorg dat de juiste omgevingen beschikbaar zijn tijdens de test en dat er niet gelijktijdig andere activiteiten plaatsvinden, zoals grote wijzigingen, back-up- en restore-acties of andere tests die de resultaten kunnen beïnvloeden.
- Zorg dat de juiste werkplekken voor de opdrachtnemer zijn ingericht met netwerkverbinding.

3.2.3 Houd de lijnen met de opdrachtnemer kort

Door tijdens de test korte lijnen te hanteren in de communicatie met de opdrachtnemer, kunnen zaken snel opgehelderd worden. Dit helpt bijvoorbeeld om workarounds voor onvoorziene omstandigheden snel af te spreken en zo onnodig oponthoud te voorkomen.

- frequente updates van bevindingen en voortgang, bijvoorbeeld een korte dagelijkse stand-up;
- direct contact bij urgente bevindingen;
- afstemming van de prioriteiten indien meer tijd dan afgesproken aan een bepaald onderdeel is besteed;
- scopewijzigingen tijdens het testen tijdig afstemmen;
- beheerders of ontwikkelaars mee laten kijken met de uitvoering van de securitytest zodat zij ervan kunnen leren.

3.3 Stuur de oplevering

Betrek tijdig de juiste stakeholders, niet alleen aan het begin van de securitytest maar ook wanneer de oplevering nadert. Om helder te hebben onder welke interne of externe verantwoordelijkheden bepaalde bevindingen vallen, kan een passende vorm worden afgesproken zodat vraag en antwoord kan plaatsvinden en onduidelijkheden worden opgehelderd (bijvoorbeeld een face-to-face-bijeenkomst om de bevindingen door te spreken) voor de definitieve oplevering plaatsvindt.

[12] In het geval van vulnerability-assessments en penetratietests is het voor de testers vaak onbekend waar blokkerende verdedigingslagen zoals een firewall of IDS zitten. Als in Stap 2 is bepaald dat deze verdedigingslagen niet binnen de scope van de test vallen is het onnodig tijdrovend om dit tijdens de test te omzeilen of ongedaan te maken.

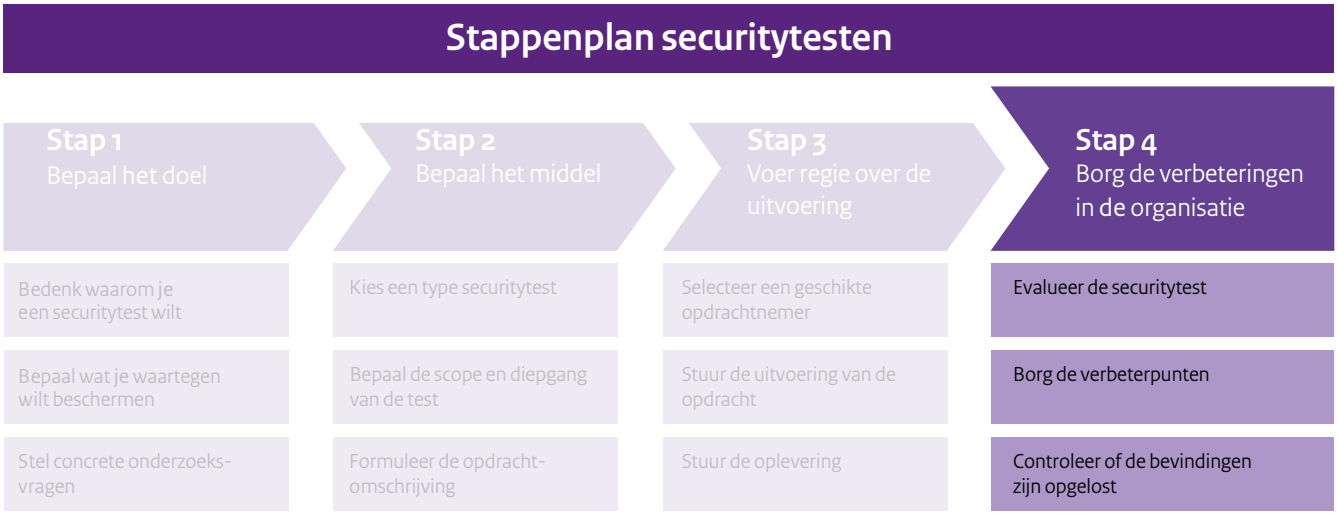
Stap

4


TU/e
Technische Universiteit
Eindhoven
University of Technology
WIND TUNNEL

Stap 4 Borg de verbeteringen in de organisatie

Nu de oplevering heeft plaatsgevonden van de securitytest, is het belangrijk om eventuele voorgestelde verbeteringen te borgen in de organisatie zodat ook in andere delen van de organisatie niet dezelfde fouten worden gemaakt en eventueel dezelfde verbete-ringen kunnen worden toegepast. De getoonde drie vragen helpen daarbij.



4.1 Evalueer de securitytest

Plan kort na de oplevering van de resultaten een evaluatie in met de betrokkenen, zodat gebruikgemaakt wordt van het momentum van de securitytest. Als het te lang duurt, is het risico groot dat er nooit meer iets mee gebeurt door overige prioriteiten in het dagelijks werk van de betrokkenen. De interne evaluatie zou de volgende elementen moeten behandelen, zodat de organisatie ervan kan leren.

Evalueer de resultaten

Nu de overdracht heeft plaatsgevonden, zou duidelijk moeten zijn voor de betrokkenen wat de impact is van de technische bevindingen op de business, de geschatte moeite voor het oplossen van de bevindingen en wat mogelijk de achterliggende oorzaken ervan zijn. Bespreek ter evaluatie de volgende punten:

- Zijn deze resultaten conform afspraken over kwaliteit (diepgang, argumentatie, bewijzen)?
- Zijn de resultaten zelf een verrassing voor de organisatie? Welke conclusie kan getrokken worden uit de bevindingen en achterliggende oorzaken?
- Boek een sessie met interne betrokkenen en de opdrachtnemer over de securitytest, zodat alle bevindingen helemaal duidelijk zijn voor de betrokkenen en eventuele vragen gesteld kunnen worden. Bovendien motiveert dit de interne organisatie om vooraf de rapportage goed door te lezen.

4.2 Borg de verbeterpunten

De organisatie heeft er baat bij om duidelijke verbeterpunten te bepalen op de verschillende verantwoordelijkheidsgebieden. Verbeterpunten kunnen gelden voor infrastructuur, applicaties of organisatie, maar ook voor componenten die zijn uitbesteed. Verduidelijk daarom op welke componenten van het informatie-systeem de bevindingen van toepassing zijn en welke partijen daarvoor verantwoordelijk zijn. Zie toe dat de bevindingen op componenten onder verantwoording van andere partijen daar ook gecommuniceerd en neergelegd worden en dat de afhandeling daarvan wordt bijgehouden. Dit is pas effectief als dit wordt geborgd in een proces voor het verwerken van bevindingen en verbeteringen uit de securitytests.

De eigen organisatie moet voorbereid zijn om acties en verant-woordelijkheid te nemen op basis van de bevindingen. Heeft de organisatie wel het personeel met de juiste vaardigheden om de bevindingen te verhelpen?

Registreer de bevindingen uit securitytestrapportages, bijvoorbeeld in servicemanagementpakketten die de organisatie al gebruikt. Dit kan ook gebruikt worden om erop toe te zien dat actiepunten worden uitgevoerd, zodat niet eenzelfde test de volgende keer dezelfde bevindingen oplevert.

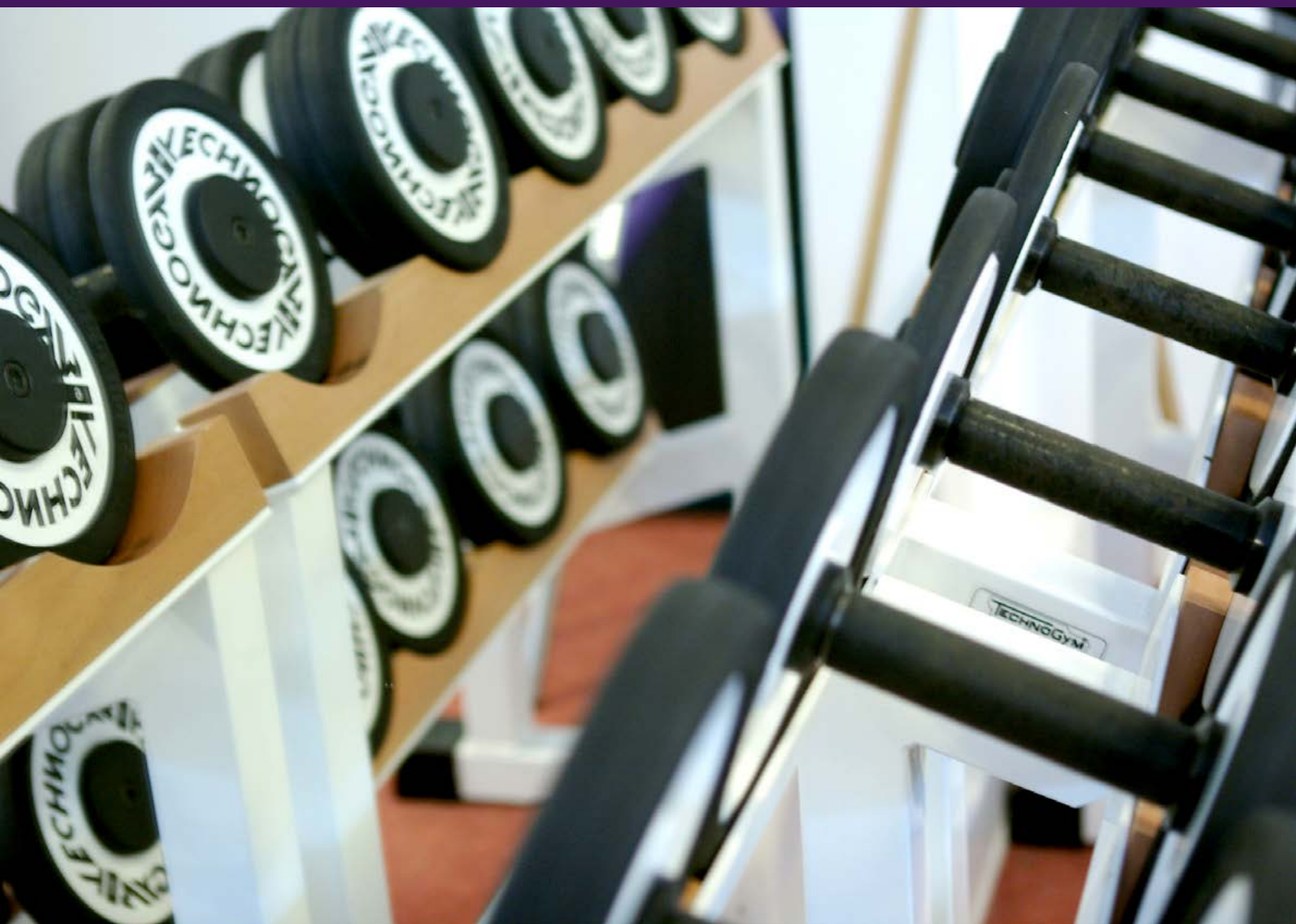
Sluit aan op het overkoepelende risicomanagement

Door aansluiting te zoeken bij een overkoepelend risicomanagementproces en risicoregister kunt u bevindingen optimaal borgen in de organisatie. Ook kunt u dan vastleggen hoe de organisatie omgaat met eventuele restrisico's bij het niet of onvolledig opvolgen van de aanbevelingen.

Controleer of de bevindingen zijn opgelost

Omdat geverifieerd moet worden of een voorgestelde verbetering daadwerkelijk is doorgevoerd kun je een hertest plannen.

Bijlagen



Bijlage A Securitytestprofiel

Securitytestprofiel		
Stappenplan		Input voor opdrachtformulering – detaillering
Stap 1: Bepaal het doel		
Bedenk waarom je een securitytest wilt		
Bepaal wat je waartegen wilt beschermen	Infrastructuur	
	Applicatie	
	Organisatie	
Stel concrete onderzoeksvragen		
Stap 2: Bepaal het middel		
Kies een type securitytest		Vulnerability-assessment, penetratietest, broncodereview
Bepaal de scope en diepgang van de test	Scope	Externe infrastructuur, interne infrastructuur, applicatie, organisatie
	Mate van binnendringen	
	Informatie vooraf	Black box, grey box, white box
	Diepgang	
Te testen onderdelen		
Component A		Aantal regels code, programmeertalen, frameworks, protocollen, ip-adressen, architectuurdiagram, verkeersstromen
Component B		
Component C		

Bijlage B Checklist standaardelementen securitytestovereenkomsten

		Vulnerability-assessment	Penetratietest	Broncodereview
A.	Offerte			
B.	Plan van aanpak			
C.	Intakeformulier			
D.	Geheimhoudingsverklaring			
E.	Vrijwaringsverklaring			
F.	Rapportage			

A Offerte

1. Plan van aanpak
2. Voorbeeldrapportage
3. Overzicht kosten en activiteiten
4. Tijdplanning
5. Mensen die de test gaan uitvoeren

B Plan van aanpak

1. Opdrachtformulering aan de hand van het securitytestprofiel
2. Testmethodiek en scenario's
3. Aanvalsstrategieën
4. Risicoclassificatiemethodiek
5. Opleveringsvorm
6. Fasering
7. Afspraken over vernietiging van informatie
8. Locatie

C Intakeformulier

1. Contactinformatie opdrachtgever
2. Contactinformatie testers
3. Contactinformatie hostingpartijen
4. Informeren van derde partijen die systemen of applicaties in scope hosten
5. Communicatieplan
6. Rapportagetaal
7. Opleveringsvorm
8. Voorgestelde planning
9. Voorgestelde testtijden
10. Voorgestelde scope
    a. De specifieke scope van de te verwachten test (welke componenten zitten in de keten);
        I Infrastructuurinformatie
        II Applicatie-informatie
        III Organisatie-informatie
    b. De tests die juist niet in scope zitten (welke handelingen mogen absoluut niet gebeuren);
    c. De componenten die niet in scope zijn;
    d. Op basis van een risicoafweging is vastgelegd welke aanvalsvectoren in scope zijn;

e. Op basis van een risicoafweging is vastgelegd welke onderzoekselementen in scope zijn;
f. Er is gedefinieerd welke aannames er zijn gemaakt;
g. Er is afgesproken welke middelen de opdrachtnemer tot zijn beschikking krijgt voor de onderzoeken, zoals inloggegevens en digitale of fysieke toegangspunten.

11. Schematische weergave van de scope

D Geheimhoudingsverklaring

1. Ontvangstbewijs van informatie
2. Inzage in getroffen maatregelen
3. Restitutie/vernietiging van verkregen informatie
4. Verplichtingen in het kader van vertrouwelijkheid van informatie
5. Onthouding van ongeoorloofde openbaarmaking
6. Afspraken over hoe te handelen bij een bevinding die in aanmerking komt voor coordinated vulnerability disclosure en wie wat daarin doet
7. Juridische gevolgen
8. Ondertekening

E Vrijwaringsverklaring

1. Afspraken over wat er moet gebeuren wanneer er issues optreden waardoor de planning uitloopt
2. Afspraken over aansprakelijkheid door de opdrachtnemer
3. Afspraken over vertrouwelijkheid en verwijdering van informatie en resultaten
4. Afspraken over wat er moet gebeuren als er persoonsgegevens worden aangetroffen
5. Afspraken over het niet achterlaten van informatie op de geteste systemen
6. Afspraken over het mogelijk achterblijven van bewijs in de logbestanden van de geteste systemen
7. Afspraken over configuratiebestanden en mogelijke tijdelijke wijzigingen daarop tijdens de test en het terugzetten van de originele configuratie-instellingen
8. Afspraken over autorisatie voor mogelijke penetratiepogingen op de afgesproken scope, waarbij er tools worden gebruikt die vooraf getest zijn en zelf vrij van kwaadaardige code
9. Afspraken over denial-of-servicetests die de continuïteit van de dienstverlening van de opdrachtgever kunnen verstoren
10. Afspraken over communicatie over de betreffende testactiviteiten op eventuele need-to-knowbasis in verband met eventuele detectie van en respons op de tests
11. Afspraken over minimale potentiële impact op de continuïteit van dienstverlening van de opdrachtgever
12. Ondertekening van vrijwaring

F Rapportage

1. Rapport met bevindingen
2. Managementsamenvatting
3. Bevindingen
   a. Omschrijving hoe de bevinding is gedaan
   b. Reproduceerbaarheid van de bevinding
   c. Impact van de bevinding
   d. Risicobeschrijving
   e. Advies
4. Toelichting van toegepaste testmethodiek
5. Conclusie

Deze brochure is een uitgave van:

Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC Den Haag
070-751 55 55
info@ncsc.nl
@ncsc_nl

Maart 2020