Buyers guide

Security testen

CYBERVEILIG NEDERLAND

Inhoudsopgave

Introductie

Cybersecuritymaatregelen zijn noodzakelijk om schade door een storing, uitval of misbruik van een informatiesysteem of computerinfrastructuur te voorkomen, ontdekken, beperken of te herstellen. Veel van deze maatregelen kunnen organisaties zelf nemen. Voor sommige zullen ze productleveranciers of dienstverleners willen inschakelen om hen hierbij te helpen.

Er is in Nederland en daarbuiten inmiddels een divers landschap van dit soort leveranciers beschikbaar die allen een breed pallet van producten en diensten aanbieden. De uitdaging is om daarin een weg te vinden. En dat is best lastig. De gebruikte terminologie binnen het cybersecuritydomein is specialistisch van aard en diensten die op het oog vergelijkbaar lijken, blijken in de praktijk toch heel verschillend te zijn.

Dit document beoogt voor het domein van de security testen een hulpmiddel te vormen. Met dit document bieden we vanuit de cybersecuritysector meer inzicht in wat de verschillende securitytesten inhouden en hoe ze zich tot elkaar verhouden.

Met deze informatie hopen we dat u een specifiekere uitvraag kunt doen in de markt als u behoefte heeft aan een securitytest. Dit document geeft heldere definities van de verschillende diensten en laat zien wat de huidige mogelijkheden zijn op dit gebied. Op deze manier kunt u scherper kiezen wat bij u past, maar u kunt met deze informatie bijvoorbeeld ook offertes beter met elkaar vergelijken. Dit document zien wij als een aanvulling op het eerder gepubliceerde Cybersecurity Woordenboek (zie cyberveilignederland.nl/woordenboek) waarvan de definities als uitgangspunt in dit document zijn gebruikt.

We hebben deze buyers guide securitytesten primair geschreven voor uitvoerend verantwoordelijken voor security binnen een organisatie, voor security verantwoordelijken zoals CISO's en voor inkopers van securityproducten en -diensten. Voor andere doelgroepen is dit document vanzelfsprekend eveneens bruikbaar. De keuze voor onderwerpen hebben we echter vanuit de primaire doelgroep gemaakt.

Voordat u begint aan een securitytest

Het is goed om u te realiseren dat een securitytest op zichzelf een infrastructuur, applicatie of andere asset niet veiliger maakt. Het is bovenal een middel om u te voorzien van inzicht in uw kwetsbaarheden en daarmee de reële risico's voor uw organisatie. Op basis van deze inzichten kunt u maatregelen nemen om de geïdentificeerde kwetsbaarheden weg te nemen en – voor zover nodig – geïnformeerde keuzes maken over het toekomstige securitybeleid van uw organisatie.

Om ervoor te zorgen dat de uitkomsten van een test de juiste inzichten geven, is het handig om uw behoeften vooraf helder te formuleren, alvorens te zoeken naar een geschikte dienstverlener. Dit voorkomt dat er een securitytest uitgevoerd wordt die niet (geheel) aan uw verwachting voldoet, of antwoord geeft op het verkeerde securityvraagstuk. Het helder formuleren van deze behoeftes kan lastig zijn, als er binnen de organisatie nog weinig kennis of ervaring is met security(testen). Met de volgende adviezen hopen we u hiermee op weg te helpen.

Securitytesten vormen soms onderdeel van een audit. Bij een audit wordt een organisatie getoetst aan een bepaald vooraf opgesteld normenkader. De audit toetst of voldaan wordt aan de norm(en). Een securitytest is gericht op het vinden van kwetsbaarheden en kan bij een audit worden ingezet om te toetsen of aan bepaalde security-eisen is voldaan.

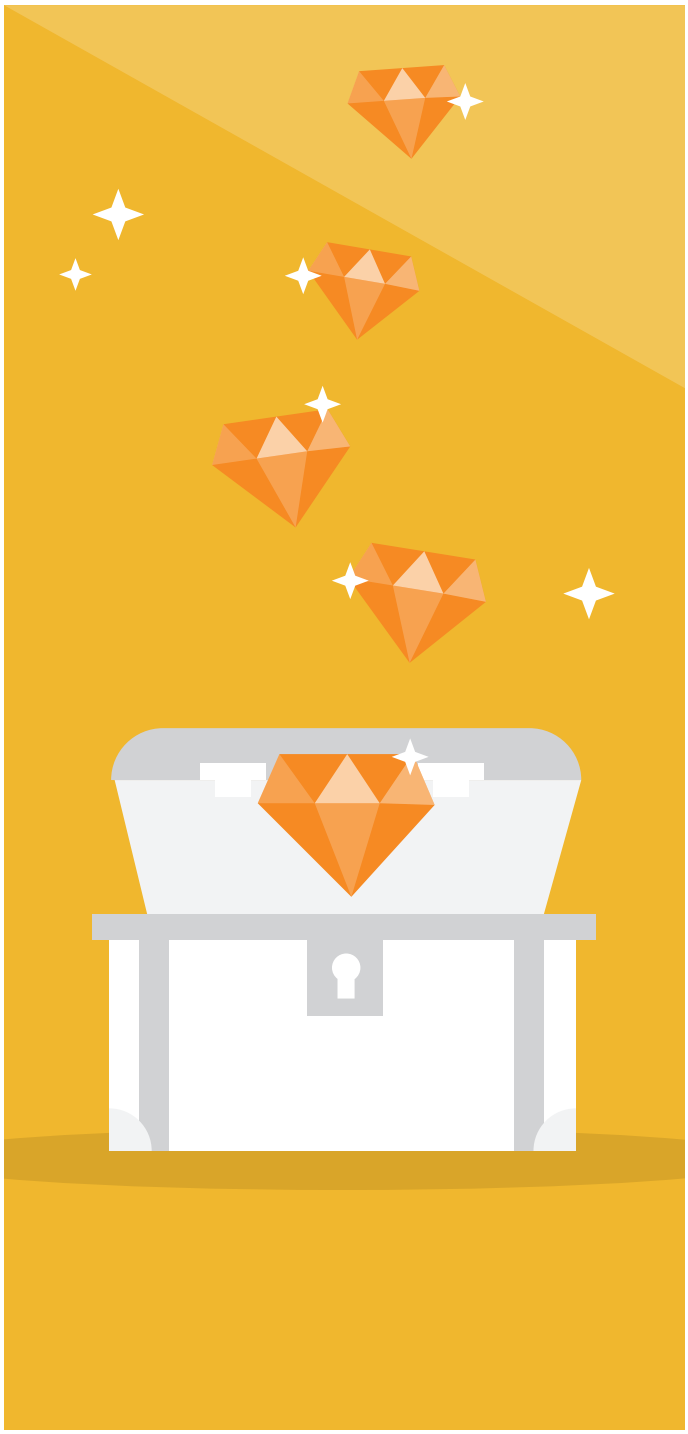
Inzicht in kroonjuwelen, de kritische assets van uw

Allereerst is het van belang dat u een duidelijk overzicht heeft van uw meest kritische digitale assets, ook wel kroonjuwelen genoemd. Welke systemen, processen en gegevens zijn kritisch voor uw primaire proces? Deze verdienen de meeste aandacht in uw beveiliggingsplan en daarmee ook in uw keuzes ten aanzien van uit te voeren securitytesten.

Niet altijd heeft u een vrije keuze als het gaat om testen. Soms moet u voldoen aan (dwingende) verplichtingen. Denk bijvoorbeeld aan belanghebbenden die verlangen dat uw organisatie inzicht kan bieden in aanwezige kwetsbaarheden en wat er is gedaan om deze te verhelpen. Ook kunnen er eigen (interne) verplichtingen zijn of kunnen er bijvoorbeeld toezichthouders betrokken zijn die verwachten dat uw organisatie securitytesten uitvoert.

Bij de verschillende manieren van testen die in dit document worden toegelicht, is een belangrijk startpunt dat er een goed overzicht bestaat van de aanwezige digitale assets. Voor veel middelgrote, maar ook voor grote ondernemingen is dit niet altijd als vanzelfsprekend aanwezig. Naast de eigen lokale infrastructuur, maken veel organisaties tegenwoordig gebruik van clouddiensten (software-as-a-service – SAAS, infrastructure-as-a-service – IAAS, platform-as-a-service – PAAS) en kan er sprake zijn van een hybride IT omgeving waarin complexe koppelingen tussen systemen zijn aangebracht. Op deze koppelvlakken bevinden zich vaak kwetsbaarheden waarvan kwaadwillenden gebruik maken.

Een complete (of zo compleet mogelijke) inventaris is daarom een belangrijke randvoorwaarde voor een effectieve securitytest. Als u een deel van uw infrastructuur niet in zicht heeft, ontstaan er blinde vlekken en zogenaamde schaduw IT. Juist deze blinde vlekken bieden kansen voor aanvallers. Een vergeten testserver kan bijvoorbeeld buiten gelden-de regels actief zijn in een infrastructuur en kwetsbaarheden bevatten die misbruikt kunnen worden. Als deze delen van een infrastructuur niet in beeld zijn, kunnen ze bij een securitytest gemist worden en kan een vals gevoel van veiligheid ontstaan.



Dreigingen, gevaren en risico's

De volgende stap is het beschrijven van de dreigingen en gevaren die deze systemen, processen of gegevens zouden kunnen treffen. Dreigingen zijn gebeurtenissen die optreden omdat iemand een negatieve intentie heeft, zoals het onbruikbaar maken van systemen middels een aanval met gijzelsoftware, of een digitale inbraak waarbij kwetsbare gegevens worden buitgemaakt. Gevaren treden willekeurig op, bijvoorbeeld als gevolg van een programmeerfout of het kapotgaan van hardware door oververhitting. Hoewel de focus bij securitytesten vaak ligt op intentionele dreigingen, is het ook goed om te kijken naar de accidentele gevaren. De testen die in dit document worden beschreven richten zich primair op dreigingen.

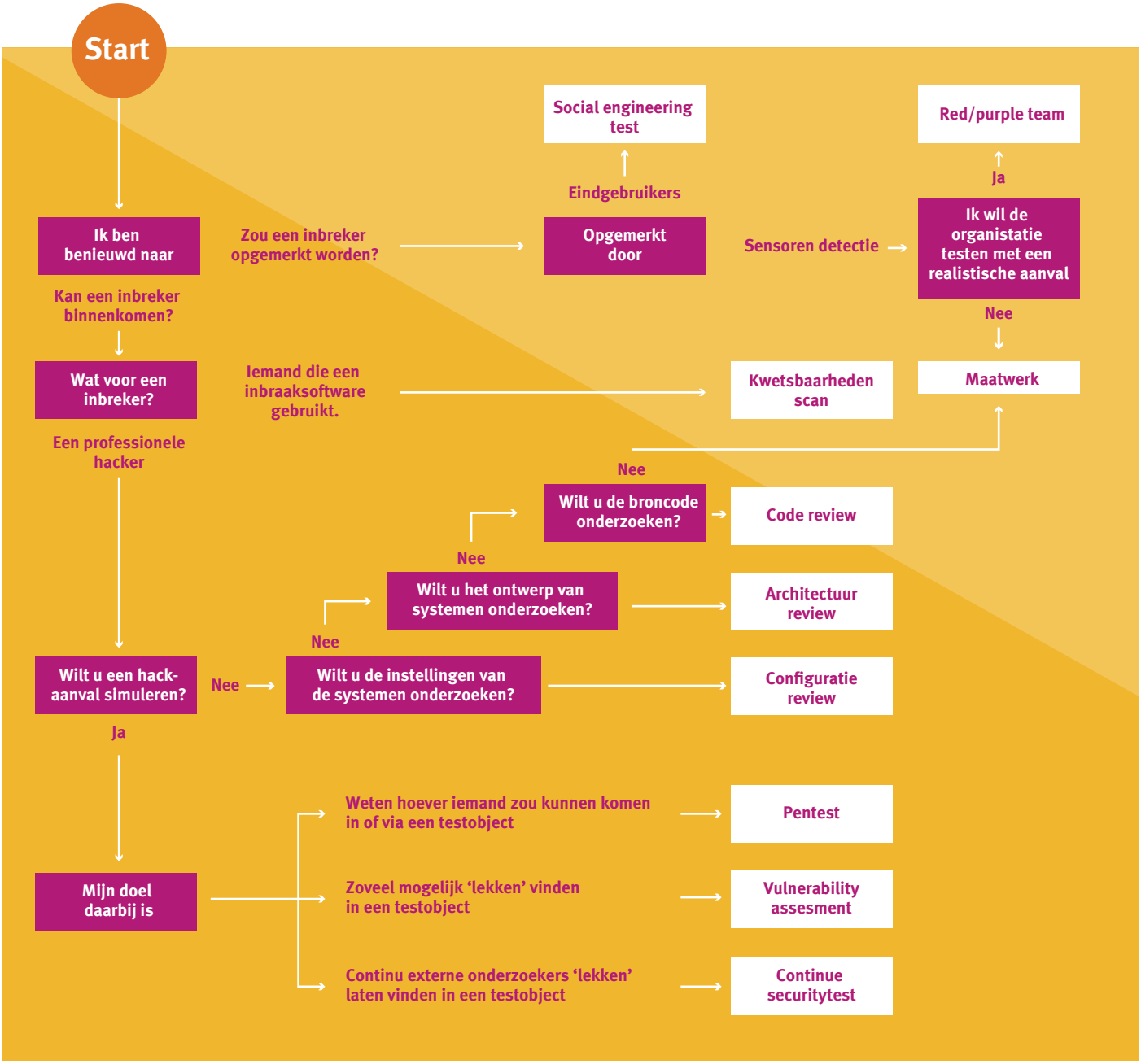
De dreigingen en gevaren moeten in de context van de organisatie beschouwd worden op hoe reëel deze zijn en tot welke schade ze potentieel kunnen leiden. Dit worden risico's genoemd. Op basis van deze risico afweging kunt u een gewenst beveiligingsniveau vaststellen en dit bepaalt vervolgens welke scenario's moeten worden getest. Het is belangrijk dat mogelijke toe te brengen schade aan de geïdentificeerde kroonjuwelen in de scenario's goed omschreven is. Een securitydienstverlener kan u helpen bij het formuleren van dreigingen, risico's en testscenario's.

Securityvraag

Uit alle informatie over kroonjuwelen, dreigingen, gevaren en risico's tezamen kunnen de securityvragen worden afgeleid. Bijvoorbeeld: 'We willen weten of een aanvaller via het Internet toegang kan krijgen tot ons financiële systeem', of 'We willen weten of ons nieuwe commerciële klantsysteem de vertrouwelijkheid van persoonsgegevens kan waarborgen, of 'We willen weten of de softwarecode cruciale fouten bevat die kunnen leiden tot uitval van de software'. Deze vragen bepalen de uiteindelijke aanpak en de scope van de securitytest. Een securitydienstverlener kan u helpen bij het formuleren van uw exacte securityvragen en het vertalen van deze securityvraag naar een geschikte testaanpak en scope voor de uit te voeren securitytest.

Welke securitytest zet ik in voor welk doel?

Er is een breed scala aan securitytesten beschikbaar. En iedere test heeft een ander doel. Onderstaand schema heeft tot doel om inzicht te geven welke typen securitytesten voor welke doelstellingen kunnen worden ingezet om te detecteren hoe kwetsbaar een organisatie is voor bepaalde dreigingen.



Een glossary met securitytesten

Het overzicht uit de vorige paragraaf laat zien dat de securitytesten grofweg in 7 hoofdgroepen zijn in te delen:

1. Security review van een ontwerp of implementatie
2. Kwetsbaarheden scan
3. Vulnerability assessment
4. Penetratietest
5. Social engineering test
6. Red teaming
7. Continue securitytesten

In onderstaande paragrafen wordt een toelichting gegeven op deze testen.

Ontwerp/ implementatie security review

In dit type testen wordt geanalyseerd of het ontwerp en de implementatie van een bepaalde infrastructuur of software vanuit een security perspectief op een goede manier is gerealiseerd. Bijvoorbeeld in de opstartfase van een nieuw ontwikkelproject, als het security ontwerp hand in hand moet lopen met het functionele ontwerp. Een ander voorbeeld is een security review als onderdeel van een due diligence traject bij een overname.

Bij een ontwerp/implementatie security review kunnen verschillende aspecten worden beschouwd:

1. Architectuur review
2. Code review
3. Configuratie review

Architectuur review

BEGRIP

Architectuur

BETEKENIS

Het ontwerp en de opbouw van een computersysteem en netwerk. Het ontwerp regelt hoe businessprocessen, applicaties, data en technologie samenhangen.

Tijdens deze review wordt het ontwerp en opbouw van het te onderzoeken systeem beschouwd vanuit een security perspectief. Dit houdt in dat er op basis van documentatie en vraaggesprekken een passieve ('papieren') toets wordt uitgevoerd op het ontwerp c.q. de architectuur. Zo kan er op basis van bijvoorbeeld best practices – denk aan richtlijnen voor het beveiligen van een intern netwerk of applicatie – worden nagegaan waar het ontwerp mogelijk nog kwetsbaar is. Ook stelt een dergelijke review in staat om observaties en aanbevelingen te doen voor wat betreft operationele securitytechniek, procesmatige/organisatorische verbeterringen en menselijke betrokkenheid. Denk bijvoorbeeld aan beheersprocessen voor security die niet op orde zijn (het tijdig doen van updates, verandermanagementprocessen met beperkte aandacht voor security etc).

Het voordeel van een dergelijke review is dat er vanuit een breed perspectief kan worden meegedacht en geadviseerd. Dit heeft met name toegevoegde waarde in het ontwerp / initiatieproces of als er behoefte bestaat aan een second opinion. Een nadeel is dat er geen daadwerkelijke technische toetsing wordt uitgevoerd op de mogelijke kwetsbaarheden. Dus in dat opzicht is er eigenlijk geen sprake van een daadwerkelijke 'test'. De betrokken adviseurs zijn namelijk ook sterk afhankelijk van de informatie die zij ontvangen uit gesprekken en kunnen wellicht daardoor details missen die van belang zijn voor de analyse.

Code review

BEGRIP	BETEKENIS
Code review	Analyse van de broncode van een programma. Het doel is zwakke plekken te vinden. Men zoekt voor een groot deel handmatig, niet aan de hand van een uitputtende lijst van kwetsbaarheden.

Zorgen voor zo veilig mogelijk geschreven code, als basis voor het veilig functioneren van een systeem of applicatie, biedt een goede securitywaarborg. Temeer omdat veel ontwikkelpartijen doorgaans niet primair worden gecontracteerd om de veiligheid van een asset, zoals bijvoorbeeld een applicatie, op het hoogste niveau te brengen. Security is misschien wel onderwerp van de opdracht, maar weegt in de praktijk niet altijd even zwaar als toegankelijkheid, snelheid en andere business doelstellingen. Ook werken partijen in de praktijk nog maar weinig conform de cyclus voor de ontwikkeling van veilige software ('Secure Software Development Lifecycle').

Tijdens de review wordt de broncode van het programma geanalyseerd vanuit een securityperspectief. Er wordt beoordeeld of er in de code keuzes zijn gemaakt die resulteren in zwakke plekken die misbruikt kunnen worden. Dit gebeurt op basis van best practices en ervaring.

Een review van de broncode vanuit securityperspectief kan voorafgaand aan het 'live' brengen van een systeem helpen om bekende kwetsbaarheden te ontdekken en verhelpen. Tevens kan een code review op een reeds operationeel systeem – onder meer op basis van bekend geworden nieuwe kwetsbaarheden – van toegevoegde waarde zijn. Bijvoorbeeld door gebruik te maken van nieuwe inzichten in fouten en omissies, en rekening te houden met hoe kwaadwillenden actueel misbruik kunnen maken van uw applicatie op basis van de nieuwste inzichten daarover.

Configuratie review

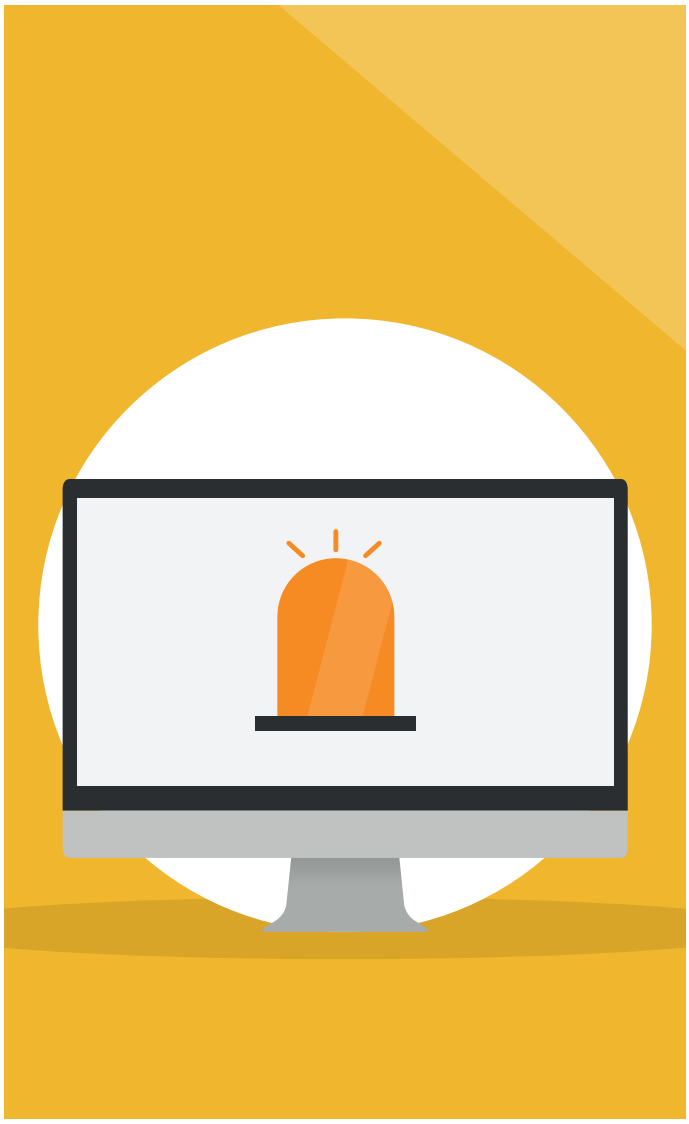
BEGRIP	BETEKENIS
Configuratie	De manier waarop hardware en software is ingesteld voor het gewenste doel.

Tijdens een configuratie review wordt de configuratie van de te onderzoeken hardware/software gecontroleerd vanuit een security perspectief. Een security tester zal op basis van best practices en ervaring op zoek gaan naar kwetsbaarheden in de configuratie die een securityrisico kunnen vormen. Ook is het mogelijk om securityeisen die vooraf zijn bepaald door de onderzoekers te laten valideren tijdens een configuratiereview.

Een bekend object voor een configuratiereview vormt een firewall, maar ook andere specifieke netwerkcomponenten of -apparaten lenen zich voor een configuratie review. Het verder versterken van de beveiliging van componenten zoals printers en switches wordt ook wel ‘security hardening’ genoemd en vormt een belangrijke manier om de kans op misbruik van uw systemen op voorhand te beperken. Bij hardening worden de functies die niet worden gebruikt in de systemen uitgezet. Daardoor kunnen zij niet misbruikt worden door derden.

Kwetsbaarhedenscan

BEGRIP	BETEKENIS
Kwetsbaarhedenscan	Een geautomatiseerde controle die zwakke plekken in een systeem opspoort. Alleen als het vals alarm is, haalt men die er handmatig uit.



Een kwetsbaarhedenscan is een geautomatiseerde test waarbij security scanning software wordt gebruikt om een overzicht te verkrijgen van mogelijke kwetsbaarheden van een asset, zoals bijvoorbeeld een webapplicatie. Eventuele valse meldingen (false positives) worden meestal uit de testresultaten gefilterd. Er vindt geen uitgebreide handmatige test plaats op de systemen en applicaties die deel uit maken van de reikwijdte van de test. Omdat sommige kwetsbaarheden alleen te vinden zijn door handmatig te testen, levert een kwetsbaarhedenscan doorgaans een minder diepgaand resultaat dan de een handmatige vulnerability assessment of penetratietest. Wel is dit type test zeer geschikt om snel een eerste indruk te krijgen van aanwezige kwetsbaarheden in een digitale omgeving.

Veelgebruikte tests richten zich bijvoorbeeld op de externe infrastructuur en worden gebruikt om na te gaan in hoeverre de organisatie – bezien vanuit haar ‘buitenkant’ vanaf het internet – mogelijk kwetsbaarheden vertoont die kunnen worden misbruikt om ongeautoriseerd toegang te krijgen tot een organisatie. Er zijn echter ook geautomatiseerde hulpmiddelen die juist de nadruk leggen op een interne IT-infrastructuur of op specifieke applicaties daarbinnen.

Vulnerability assessment

BEGRIP

Vulnerability

BETEKENIS

Handmatige controle waarbij men zwakke plekken in een systeem opspoort. Men bepaalt vooraf hoe men dat doet. Bij een vulnerability assessment probeert men alle zwakke plekken te vinden in een klein gebied. Dat is anders dan bij een penetratietest waarbij men zo diep mogelijk in een systeem wil komen.

Bij een vulnerability assessment is het doel een zo volledig mogelijk overzicht te verkrijgen van alle kwetsbaarheden binnen een heel specifiek gedefinieerde scope, zoals een specifieke webapplicatie of IT-systeem. Het betreft hier een handmatige test waarbij de kwetsbaarheden door de security onderzoekers worden gezocht. Om de volledigheid van een dergelijke test te garanderen maken de onderzoekers zoveel mogelijk gebruik van checklists zoals de Certified Secure Web Application Security Checklist voor webapplicaties. In tegenstelling tot een kwetsbaarhedenscan testen en valideren de onderzoekers de gevonden kwetsbaarheden dus handmatig. De uitkomst van een dergelijke test is een zo volledig mogelijk overzicht van alle in de applicatie of infrastructuur aanwezige kwetsbaarheden.

Penetratietest

BEGRIP	BETEKENIS
Penetratietest	Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden. Dat gebeurt wel bij een kwetsbaarhedenscan.

Bij een penetratietest (afgekort pentest en soms ook indringerstest of A&P test genoemd) is het doel om inzicht te krijgen in hoe ver een kwaadwillende zou kunnen komen als hij inbreekt in de te onderzoeken asset, zoals bijvoorbeeld een IT-infrastructuur, een WIFI netwerk of een app(licatie). Het doel is om zover mogelijk de omgeving binnen te dringen en hierbij de meest ernstige kwetsbaarheden in kaart te brengen binnen de beschikbare tijd. De uitkomst van een dergelijke test is een rapportage waarin verschillende aanvalspaden, kwetsbaarheden en handelingsperspectieven voor het verbeteren van de beveiliging van het onderzoeksobject zijn beschreven. Soms wordt de test vormgegeven rondom een aantal concrete scenario's, bijvoorbeeld: 'Kan een kwaadwillende de mail van de directieleden lezen?' of 'Kan een kwaadwillende een bepaald systeem op afstand uitzetten?'

Er zijn diverse varianten van penetratietesten:

Blackbox
Test zonder voorkennis van het te testen object.

Greybox
Een test waarbij de onderzoeker beperkt toegang heeft tot een te onderzoeken object, bijvoorbeeld via een gebruikersaccount met beperkte rechten. Dit is een reëel scenario in het geval dat bij een aanval effectief gebruik is gemaakt van social engineering technieken (zie volgende paragraaf) of waarbij een malafide gebruiker een dreiging vormt voor het te testen object.

Whitebox
Dit betreft een test waarbij vooraf kennis is gedeeld over ontwerp en architectuur.

Crystalbox
Bij deze test is naast kennis over ontwerp en architectuur ook de broncode beschikbaar gesteld en informatie over de configuratie. Soms wordt dit type test ook een whitebox test genoemd.

Timebox
Dit is een test die stopt nadat een bepaalde hoeveelheid tijd of budget is besteed. Echter, vrijwel alle bovenstaande testen worden over het algemeen beperkt in tijd en budget.

Deze varianten worden soms ook gebruikt bij vulnerability assessments. Een uitgebreide uitleg over penetratietesten is voorhanden in het whitepaper security testen dat is gepubliceerd door het NCSC en met input van diverse marktpartijen tot stand is gekomen.

Social engineering test

BEGRIP	BETEKENIS
Social engineering	Als een aanvaller iemand misleidt door bijvoorbeeld in te spelen op nieuwsgierigheid of behulpzaamheid. Op deze manier probeert de aanvaller bijvoorbeeld aan informatie te komen om in een digitaal systeem in te breken.

Bij deze test wordt onderzocht in hoeverre een organisatie kwetsbaar is voor social engineering. Een aanval vanuit dit perspectief wordt veelal nagebootst door een zogenaamde mystery guest of phishingsimulatie. Hierbij worden medewerkers verleid (lees: gemanipuleerd) om in tegenspraak met securityrichtlijnen te handelen.

Dit kan er bijvoorbeeld toe leiden dat er toegang wordt verkregen tot een pand, logingegevens, een systeem en/of specifieke data. Ook is denkbaar dat fysieke toegang leidt tot het verkrijgen van digitale toegang. Er kunnen bijvoorbeeld zogenaamde 'rogue devices' worden achtergelaten die zorgen voor digitale toegang op afstand. Ook kan er op andere manieren, zoals via onbeveiligde poorten, beperkt beveiligde WiFi of via devices toegang worden verkregen tot een digitaal systeem.

Dit type testen wordt meestal ingezet met als doel verdere bewustwording te realiseren en de (fysieke) beveiliging (van locaties) aan te scherpen. Ook kunnen deze testen onderdeel uitmaken van een realistische aanvalssimulatie, ook wel 'red teaming' genaamd (zie volgende paragraaf).

Red teaming

BEGRIP

red teaming / adversary simulation

BETEKENIS

Oefening waarbij een organisatie aanvallen naspeelt om te ontdekken hoe goed ze is beschermd tegen aanvallen. Het red team speelt aanvallen en aanvalsmethodes na van een gekozen tegenstander. Het blue team probeert aanvallen van het red team op te sporen en vervolgens tegen te gaan. Als ze een echte aanval tegenkomen, pakken ze die ook aan. Soms is er ook een white team. Dit team zorgt dat de oefening haar doel bereikt. Bijvoorbeeld door te bepalen welke informatie de beide teams krijgen. De samenwerking tussen het red team en het blue team heet ook wel purple teaming. Bij een red team oefening ligt de nadruk op samenwerking tussen teams, en op het nadoen van tegenstanders en aanvallen. Bij een penetratietest probeert men zo diep mogelijk in een systeem binnen te dringen.

Om de maximale waarde te kunnen halen uit red teaming is het van belang dat de organisatie al verschillende maatregelen heeft genomen op gebied van cybersecurity. Een red team security test is een middel om te controleren of deze maatregelen in praktijksituaties daadwerkelijk effectief zijn. Net zoals kwaadwillenden in de praktijk doen, maakt het ‘red team’ met haar aanvallende securityspecialisten gebruik van een combinatie van technische aanvallen, social engineering en zwakheden in bedrijfsprocessen. Het resultaat is een goed beeld van de weerbaarheid van de organisatie tegen een realistische aanval en een goede indruk van hoe de organisatie hierop reageert. Met name dit laatste is een wezenlijk onderdeel van een red team test: aangezien een organisatie ook vooral wil weten hoe snel en adequaat het verdedigende - blue team - reageert op aanvallende acties.

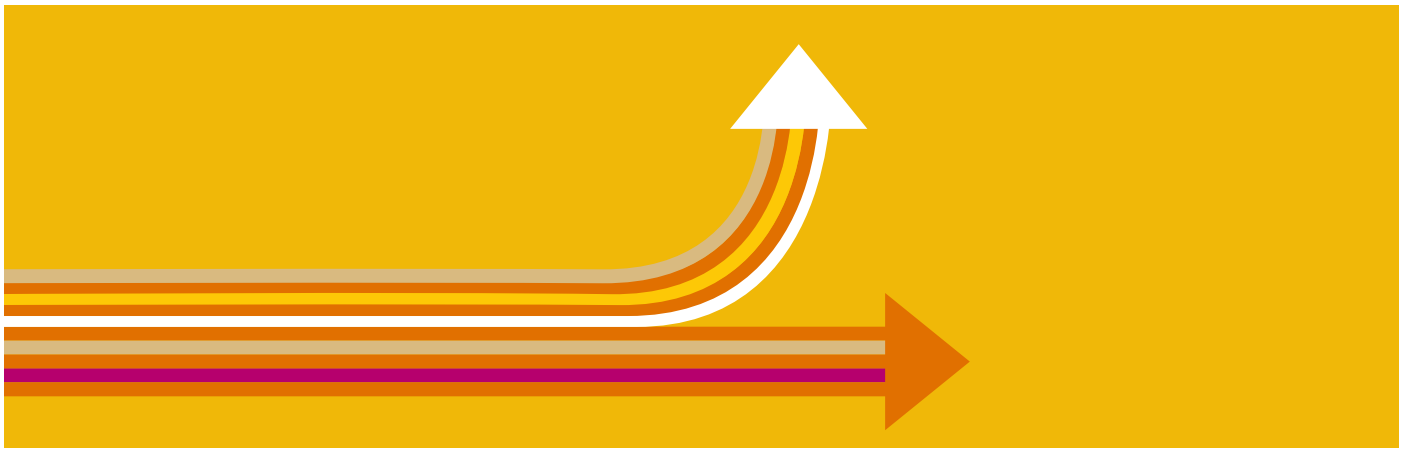
Een uitgebreide evaluatie van de door het red team en blue team uitgevoerde acties wordt ook wel een purple teaming sessie genoemd. Purple teaming kan ook real time plaatsvinden.

Soms is het uitgebreid verzamelen van dreigingsinformatie (threat intelligence) en het opstellen van aanvalscenario’s op basis van deze gegevens een apart onderdeel van een red team test. Hierbij spreekt men ook wel van een Threat Intell Based Ethical Red team of TIBER test.

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

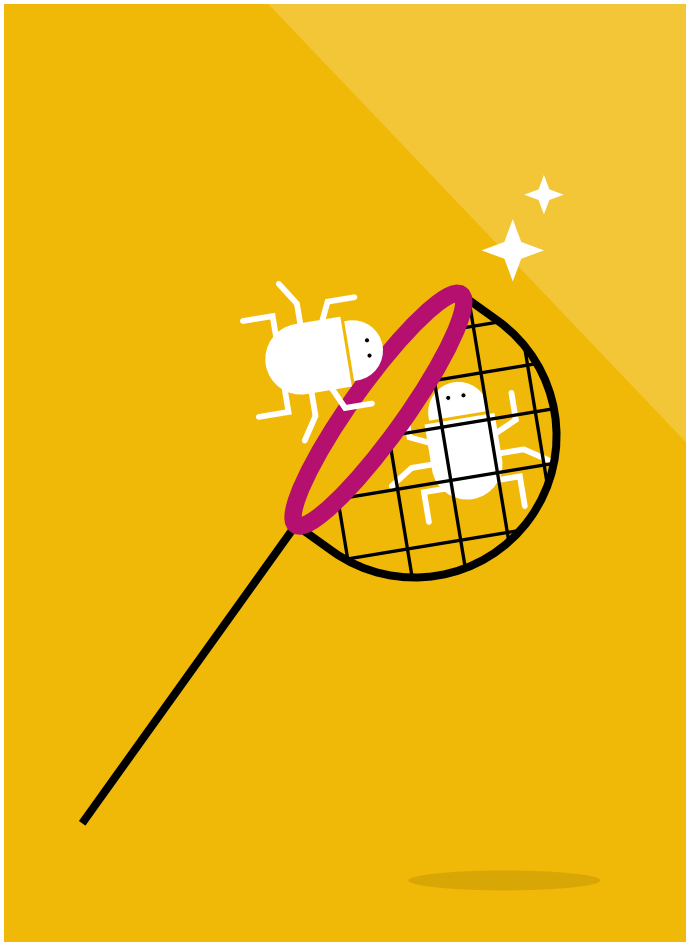
Continue security testen

Een andere aanpak van securitytesten is het uitnodigen van security onderzoekers om zelf op zoek te gaan naar kwetsbaarheden in een infrastructuur. Twee mogelijke manieren om dit te doen is via een bug bounty programma of via coordinated vulnerability disclosure.



Bug bounty programma

BEGRIP	BETEKENIS
Bug bounty	Beloning die iemand krijgt als hij een beveiligingslek in een digitaal systeem heeft gevonden en gemeld. Men krijgt de beloning van de eigenaar van het digitale systeem.



Bij een bug bounty programma worden security onderzoekers actief uitgenodigd om kwetsbaarheden in bepaalde systemen op te sporen. De eigenaar van het systeem stelt vooraf een bepaalde beloning ter beschikking. De hoogte van de beloning hangt over het algemeen samen met factoren als de ernst van de kwetsbaarheid die een onderzoeker aantreft en de mate waarin dit netjes gerapporteerd wordt aan de organisatie.

Coordinated vulnerability disclosure (CVD)

BEGRIP

Coordinated vulnerability disclosure

BETEKENIS

Standaard proces waarmee security onderzoekers zwakke plekken in computersystemen en producten kunnen melden. Ze mogen dat alleen doen als ze zich houden aan de spelregels van de organisatie voor dit soort meldingen. Het Nationaal Cyber Security Centrum (NCSC) heeft een handleiding waarin staat waaraan de spelregels moeten voldoen. Deze methode is de opvolger van de Responsible Disclosure. Het belangrijkste verschil met vroeger is dat de onderzoeker nu niet meer alleen verantwoordelijk is voor de gevolgen van een beveiligingslek.

Er is een grote community met hackers die zich bezighoudt met het vinden en rapporteren van kwetsbaarheden. Deze community kan actief worden gestimuleerd om op zoek te gaan naar kwetsbaarheden in uw systemen door op uw website te vermelden dat u hiervoor openstaat. Wel is het dan ook van belang dat u deze informatie goed in ontvangst kunt nemen. Een handleiding over hoe u dit het beste kunt aanpakken kunt u downloaden op de website van Cyberveilig Nederland.

Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld.

De definities van de begrippen die zijn opgenomen in dit document komen uit de tweede druk van het Cybersecurity Woordenboek (ISBN 9789083026411).

Eerste uitgave: 1 juli 2021

Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op cyberveilignederland.nl

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10

CYBERVEILIG NEDERLAND