Penetratietest

Whitepaper

RedTeam
CYBER SECURITY

Alles wat je moet weten over penetratietesten

Penetratietesten, of pentesten, vormen voor veel bedrijven een complex onderwerp. Het niet kennen van de ins en outs van zo'n test kan een groot struikelblok zijn voor het nemen van de juiste beslissing. Uiteindelijk kan dit forse impact hebben op de beveiliging van jouw bedrijf.

Deze RedTeam Cyber Security whitepaper helpt bedrijven alle aspecten van penetratietestdiensten te begrijpen. Deze whitepaper is niet per se bedoeld voor IT-specialisten, maar is bedoeld voor mensen die verantwoordelijk zijn voor het beheren, plannen en managen van een penetratietestproject.

Blijf hackers een stap voor.

Lees daarom deze whitepaper rustig en aandachtig door. Want het kan een cybercrimineel niet schelen hoe groot of klein jouw organisatie is: een gemakkelijk doelwit is een gemakkelijk doelwit!

Wat is een pentest?

Penetratietesten kunnen worden gezien als ethisch hacken, soms ook wel white-hat-hacking genoemd. Het doel is om de beveiliging van jouw IT-infrastructuur methodisch te testen. Een penetratietest wordt uitgevoerd door een deskundig bedrijf tegen een vooraf gedefinieerde scope (wat is het doel van de pentest, wat is de omvang van het project) op een bepaald tijdstip.

De pentest omvat een actieve en passieve analyse van IT-infrastructuren en toepassingen. Af en toe worden menselijke invloeden ook op de proef gesteld door middel van social engineering. Pentesten zijn tegenwoordig een fundamenteel onderdeel van de risicobeheer strategie.

Het doel van penetratietesten is ten eerste om duidelijkheid te creëren over de tekortkomingen als het gaat om beschikbaarheid, integriteit en vertrouwelijkheid van data. Daarna volgt het hersteladvies.

Waarom zou je een penetratietest kopen?

De belangrijkste reden is: blijf hackers een stap voor! Een digitale inbraak kan enorme schade aanbrengen in jouw bedrijf of instelling. Denk aan financiële schade, maar ook aan reputatieschade. Penetratietesten verminderen het risico op een digitale inbraak drastisch.

Je denkt wellicht dat je over een zeer veilige infrastructuur beschikt, met alle processen, procedures en personeelstraining om dit te ondersteunen. Hopelijk heb je gelijk. Maar hoe weet je dat zeker? Een penetratietest is een ideale manier om je beveiligingsmaatregelen te testen, waardoor je relevant bewijs krijgt dat die inderdaad voldoen. Dit zal de gemoedsrust van jouw klanten en leveranciers en ook die van jezelf ten goede komen.

Complexer

Naarmate de technologie evolueert en jouw bedrijf groeit, worden technische infrastructuren steeds complexer. Het is niet ongebruikelijk dat daardoor de onveiligheid in jouw systeem toeneemt. Elke penetratietest behandelt jouw bedrijfsrisico's en de impact op de vertrouwelijkheid, integriteit en beschikbaarheid van jouw data. Elke test zet het licht op onveilige plekken en hoe die in relatie tot elkaar staan. Vergeet niet dat je zo veilig bent als de zwakste schakel.

De pentest geeft je dus een beeld van jouw huidige beveiligingsniveau. En geeft uiteraard aan waar je herstelwerkzaamheden moet gaan verrichten, voordat een aanvaller toe kan slaan.

Op deze wijze krijgen het management en de technische teams een goede indicatie hoe ze de risico's het beste op een gestructureerde manier kunnen prioriteren, plannen, budgetteren en verhelpen.

Wet- en regelgeving

Wet- en regelgeving, industrienormen en best practices dwingen bedrijven en instellingen steeds meer richting penetratietesten. Je zult in steeds meer gevallen moeten aantonen dat je er wettelijk voldoende aan hebt gedaan om ervoor te zorgen dat jouw infrastructuur in een goede algehele staat van beveiliging verkeert.

Een goed begin is het halve werk

Je hebt inmiddels gelezen wat penetratietesten zijn en waarom ze zo belangrijk zijn. Voordat we ingaan op de meer gedetailleerde analyse van de anatomie van penetratietesten, zijn er overwegingen en beperkingen waar je goed over na moet denken.

1.

Denk na over de scope. Die is van groot belang. Een test met een verkeerde scope zal van beperkt nut zijn, of zelfs helemaal niet. Tijd en moeite zijn dan verspild. Onthoud altijd dat je alleen items moet testen die binnen de scope vallen. Je kunt natuurlijk een bedrijf voor penetratietesten inschakelen en zeggen ‘hack alles’, maar dit zal waarschijnlijk veel tijd en geld verspillen. Op de juiste manier de focus leggen op een scope die breed en diep genoeg is, is een veel betere optie.

2.

Houd je doelstellingen in gedachten en stel onderzoeksvragen op. De penetratietest uitkomst moet antwoord geven op de onderzoeksvragen.

3.

Reserveer voldoende budget. De kwaliteit van de test wordt beïnvloed door jouw budgettaire beperkingen. Zorg ervoor dat je voldoende budget hebt waarmee je alles kunt testen wat voor de scope noodzakelijk is.

4.

Bepaald het juiste type test. Er zijn veel verschillende soorten security testen en het is van vitaal belang om de juiste ervan toe te passen. Later in deze whitepaper gaan we in op de verschillende testvariëteiten.

5.

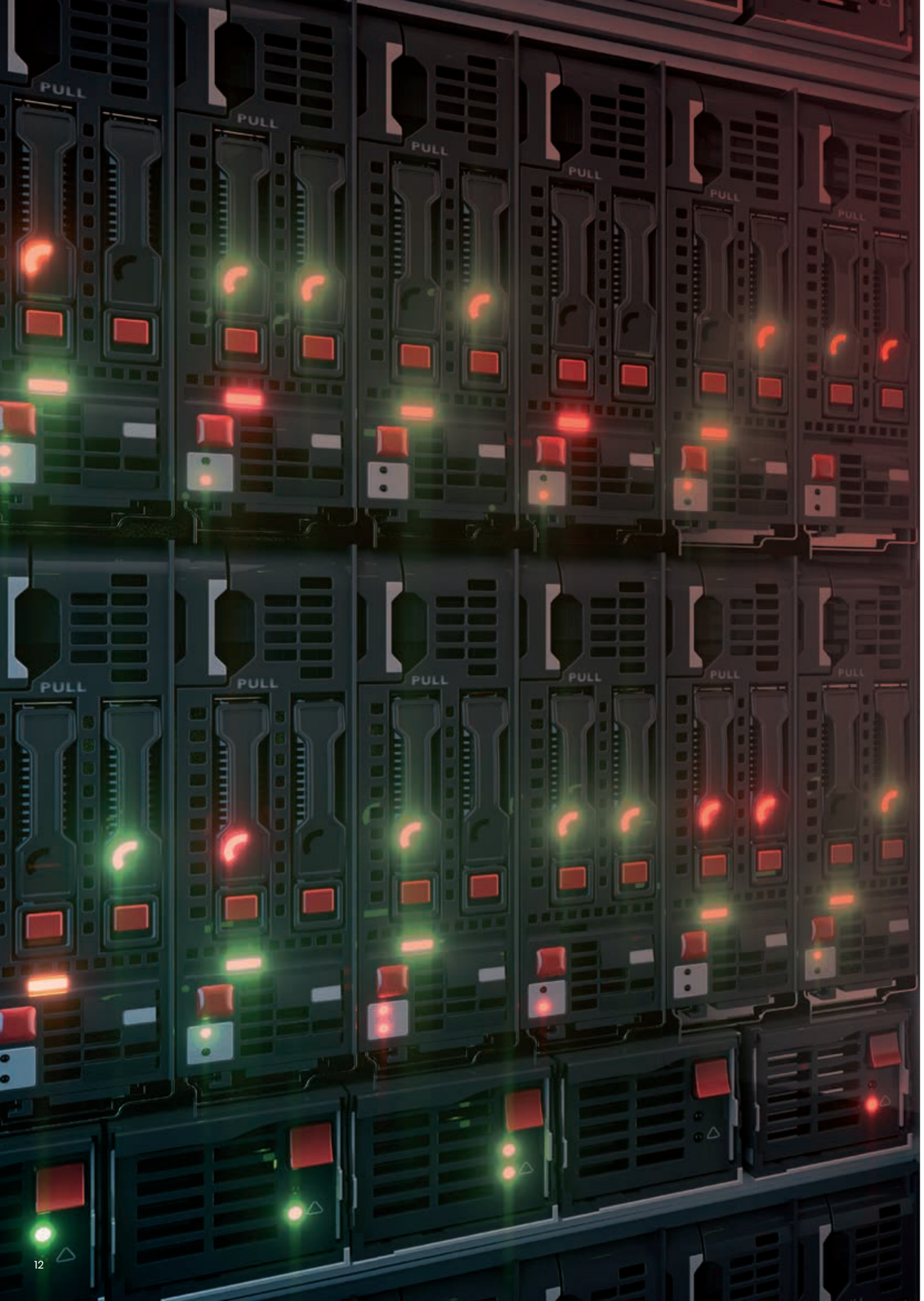
Kwaliteit van de testers. Het niet krijgen van de juiste mensen om de klus te klaren, kan leiden tot een kwalitatief onvoldoende resultaat. Hoe zorg je dat je over de juiste kennis en vaardigheden beschikt.

6.

Wees voorbereid. Penetratietesten kunnen impact hebben op de omgeving. Denk daarbij aan hoog resourceverbruik van systemen, vertraging in dataoverdracht en er kunnen waarschuwingen in logging - en monitoring applicaties verschijnen. Zorg voor support tijdens het uitvoeren van de testen zodat storingen kunnen worden verholpen, mochten deze zich voordoen.

7.

Maak een volledige back up. De tests kunnen van invloed zijn op je productiesystemen, dus is het een goed idee om een volledige back-up uit te voeren voordat het testen begint.



Penetratietesten regelmatig uitvoeren.

Geen enkele penetratietest kan ooit een garantie bieden dat je 100% veilig bent. Elke dag kunnen nieuwe kwetsbaarheden, technieken en technologieën worden onthuld of ontdekt. Wat een penetratietest echter wél oplevert, is het bewijs dat je jouw systemen zo veilig mogelijk hebt ingericht. Hierdoor wordt de kans op een succesvolle aanval drastisch verkleind.

Een penetratietest is slechts een momentopname. Daarom schrijven de meeste beveiligingsnormen voor dat penetratietesten regelmatig moeten worden uitgevoerd, doorgaans om de zes maanden of een jaar en bij grote wijzigingen.

Soorten penetratie-testen

Penetratietesten zijn er in drie belangrijke vormen: black box, white box en grey box. Het is belangrijk om de verschillende typen tests te begrijpen.

Black box

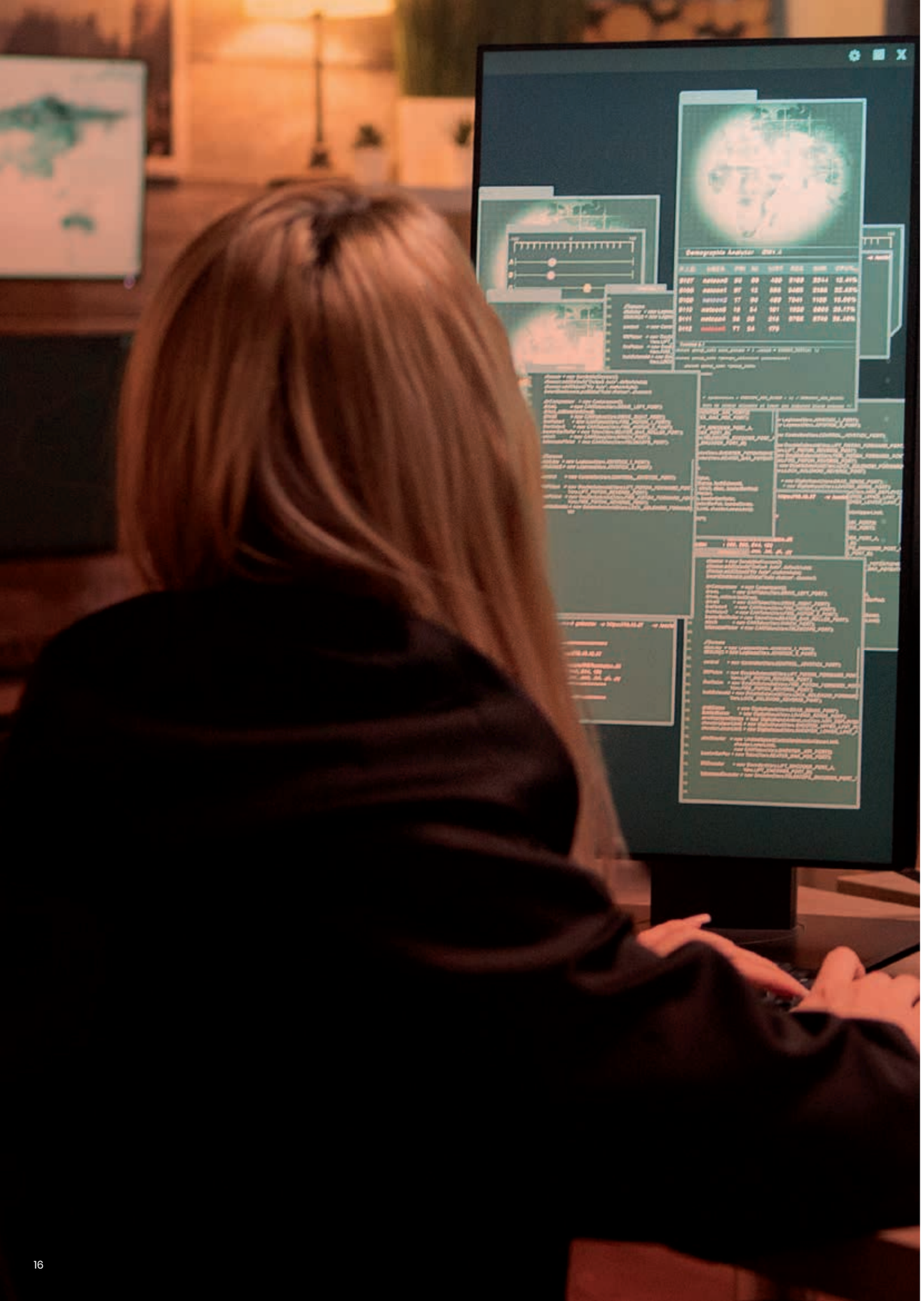
Bij een black box-test hebben de penetratietesters weinig voorkennis van het doel object. Dit is een realistisch scenario dat in praktijk veel voorkomt. De penetratietester wordt dan in dezelfde situatie geplaatst als een kwaadwillende hacker. De nadelen van black box-tests zijn dat het afgesproken tijdsbestek mogelijk niet voldoende is om alles te testen en dat sommige delen van het doel object mogelijk niet worden getest, omdat ze niet zijn ontdekt.

Grey box

Een grey box-test onthult gedeeltelijke informatie over de doelsystemen aan de penetratietesters. Deze hybride benadering is de meest gebruikelijke vorm van penetratietests. Dit omdat de tester een methodische aanval kan simuleren zonder elk detail van de doelsystemen te hoeven kennen.

White box

Bij een white box-test krijgen de testers volledige openheid, inclusief een uitsplitsing van doelsystemen, netwerkdiagrammen en firewallregels. Door alle aspecten van de omgeving te testen, kunnen beveiligingsproblemen sneller en in grotere aantallen worden ontdekt. Het voor de hand liggende nadeel van deze test is dat het geen realistisch scenario is, aangezien een kwaadwillende hacker in de echte wereld niet zo veel kennis zou hebben en niet zo bevooroordeeld zou zijn als de tester. Maar als het om beveiliging gaat, bestaat er dan ooit echt zoiets als te veel?



Het positioneren van penetratie-testen

Extern

Externe penetratietests simuleren de mogelijkheden van een aanvaller om toegang te krijgen tot het interne netwerk. Dit wordt vaak gedaan met gevoelige gegevens verkregen uit openbare bronnen.

Intern

Interne penetratietests simuleren een aanval die vanaf het interne netwerk plaatsvindt. Dit geeft aan wat een aanvaller (of een insider) kan zien en wat ze intern kunnen doen, zoals van het ene netwerk naar het andere gaan, interne communicatie onderscheppen, etc.

Penetratietests moeten extern, intern of vanuit beide hoeken worden gepositioneerd en uitgevoerd. Het doelwit tijdens de penetratietest is hetzelfde: het verschil is waar de aanval vandaan komt.

Testsoorten

Er zijn verschillende soorten penetratietests, elk ontworpen om verschillende aspecten van jouw beveiligingsproces te testen. De volgende soorten tests komen het meest voor en zijn over het algemeen geschikt voor alle organisaties. De beschrijving van tests varieert, waarbij elk bedrijf verschillende terminologieën kan gebruiken.

1. ‘Infrastructuur’ of ‘Netwerk’ penetratietests

Bij dit type test wordt een infrastructuur of netwerk beoordeeld op de huidige operationele beveiligingsniveaus. Denk hierbij aan netwerk segmentatie, actieve netwerkservices, huidig patchbeleid, onjuiste configuraties, ontwerpfouten en effectiviteit van beveiligingscontroles. Het doel is om eventuele bijbehorende kwetsbaarheden te identificeren en gecontroleerd te exploiteren.

2. Applicatie penetratietests

Hier worden de functionaliteiten, processtromen en beveiligingscontroles van applicaties getest vanuit een ongeauthentiseerd en/of geauthentiseerd perspectief. Deze tests hebben specifiek betrekking op accesscontrol, sessie en configuratiemanagement, foutafhandeling, gegevensbescherming en gebruikersinvoer. Applicatie penetratietests komen van pas als je een onafhankelijke toets op je applicatie wilt hebben om te beoordelen hoe verschillende onderdelen zijn ingericht. Mogelijk zijn er interacties die directe of indirecte beveiligingsproblemen kunnen veroorzaken. Met alle gevolgen van dien.

3. Testen van configuraties

Dit type test is bedoeld om de huidige inrichting van verschillende systeemcomponenten te beoordelen. Het is een niet-indringende testaanpak, ontworpen om de configuratie te auditen vanuit het oogpunt van systeemhardening en best-practices. Het helpt ervoor te zorgen dat de huidige en toekomstige infrastructuur wordt geïmplementeerd in overeenstemming met de best practices van de branche, waardoor de kans op manipulatie en uitbuiting van de systemen wordt verkleind.

4. Social engineering

Social engineering betreft het menselijke element van beveiliging, waarbij penetratietesters zullen proberen toegang te krijgen tot gevoelige informatie door menselijke psychologie toe te passen en door te manipuleren. Hiervoor zijn specifieke technieken noodzakelijk. Vaak worden hierbij de pijlen gericht op de medewerkers van jou organisatie. Technieken zoals phishing en het testen van de fysieke beveiliging van een bedrijf (inlooptest) worden hierbij toegepast.

5. Wireless penetratietests

Dit type omvat het identificeren van zwakke punten in draadloze netwerkarchitecturen door netwerkverkeer, accesspoints, malafide apparaten, versleutelingsstandaarden en netwerk segemntatie en patchniveaus te analyseren en te inspecteren.

De fasen van een penetratietest

Een goede penetratietest volgt een voorgeschreven methodologie bij de uitvoering. Deze omvat doorgaans zeven stappen, die hier worden beschreven.

1

Scope definitie & interacties voorafgaand aan de test

Hier worden alle eisen verzameld en doelen gesteld. Het is waar de soorten tests, afspraken, tijdlijnen en beperkingen worden vastgesteld en overeengekomen. Dit is essentieel voor een soepele en goed gecontroleerde test.

2

Verzameling van informatie en beoordeling van bedreigingen

Intelligence gathering is een benadering van informatieverkenning die erop gericht is zoveel mogelijk informatie te verzamelen. Deze informatie wordt gebruikt als extra aanvalsvector bij het doordringen van de doelsystemen tijdens het kwetsbaarhedenonderzoek en de exploitatiefasen. Ook het beoordelen van waar de dreiging het meest realistisch is en op basis daarvan testen definiëren doen we in deze fase.

3

Analyse van kwetsbaarheden

Deze fase is bedoeld om gebreken in netwerken, systemen en/of applicaties te ontdekken met behulp van actieve en passieve technieken, waaronder misconfiguraties van hosts en services, huidig patchbeleid of onveilig applicatieontwerp.

4

Exploitatie

Met behulp van de kwetsbaarhedenanalyse uit de vorige stap worden alle externe en intern gerichte systemen die binnen de scope vallen aangevallen. Dit omvat een combinatie van publiek beschikbare en op maat gemaakte exploits en technieken om configuraties en beveiligingscontroles te testen. Daarmee wordt geprobeerd om toegang te krijgen tot gevoelige informatie en in het algemeen om toegang tot de doelsystemen in kwestie te verkrijgen.

5

Analyse van kwetsbaarheden

Het doel van deze fase is om de waarde van de gecompromitteerde doelsystemen te bepalen door te proberen privileges te verhogen en over te stappen naar andere omliggende systemen en netwerken die binnen de scope zijn gedefinieerd.

Belangrijk is dat er geen exploits of andere scripts achterblijven op de gecompromitteerde systemen. Dit zorgt ervoor dat de systemen niet blootgesteld worden aan onnodige risico's als gevolg van de tester.

6

Rapporteren

Alle informatie die in de voorgaande stappen wordt genoemd, wordt gedocumenteerd. Er wordt een uitgebreid maar ook goed te lezen en begrijpen rapport opgeleverd, inclusief:

- alle risico's gebaseerd op de huidige server/applicaties en configuratie;
- een management samenvatting een management samenvatting die ook begrijpbaar is voor mensen zonder technische achtergrond;
- kwetsbaarheden en actieve services op de servers en applicaties;
- wat er gedaan is om elk beveiligingsprobleem te exploiteren;
- stappen om het risico's op te lossen;
- maatregelen op korte en lange termijn ter verbetering.

7

Debriefing / bevindingen overleg

Deze stap is geen strikte vereiste, maar raden wij wel altijd aan. Na het afronden en opleveren van een penetratietestrapport, kunnen bij de debriefing de bevindingen en risico's in het rapport toegelicht worden en de gelegenheid worden geven om eventuele vragen te stellen.

Denk je dat je over een veilige infrastructuur beschikt?

Maar weet je dat wel zeker?

Hoe plan en beheer je een penetratietest?

1. Bepaal de businessrequirements (vereisten) en stel doelen waaraan voldaan moet worden;
2. Bepaal de aanpak en soorten penetratietests die je nodig hebt. Dit omvat eventuele beperkingen, evenals eventuele specifieke testscenario's die je mogelijk nodig hebt;
3. Als je niet zeker weet wat er in de scope moet worden opgenomen, RedTeam Cyber Security biedt hulp bij het hele scopeproces.
4. Beoordeel de risico's van het testen van deze systemen. Als je geen enkele impact kunt veroorloven op een bedrijfskritisch live-systeem, zijn er andere manieren om te testen, zoals het testen op een accepatie systeem als deze vergelijkbaar is ingericht;
5. Bepaal een tijdschema voor de uit te voeren tests, bijvoorbeeld tijdens kantooruren of buiten kantooruren;
6. Hertest de bevindingen indien deze zijn opgelost, om vast te stellen of dit succesvol is gemitigeerd.

Wat moet ik verder doen?

Om een test soepel en goed te laten verlopen, zijn er enkele dingen die je moet doen. Ontvang een ondertekende geheimhoudingsverklaring om vertrouwelijkheid te garanderen. Zorg ervoor dat alle relevante mensen binnen de organisatie op de hoogte zijn van de penetratietests. Maak proactief een back-up van alle kritieke gegevens van systemen die deel gaan uitmaken van de penetratietests, aangezien deze tijdens de tests kunnen worden beïnvloed. Zorg voor alle benodigde middelen zoals VPN-toegang, IP-whitelisting enz., voorafgaand aan de aanvang van penetratietests helder in beeld zijn, om te voorkomen dat er vertragingen optreden tijdens de uitvoering van de tests. Laat de penetratietesters onmiddellijk weten wanneer je een storing, of andere problemen ervaart tijdens de test. In contact blijven is belangrijk om snel te kunnen reageren.

Mythen en onjuistheden

Er zijn veel mythen en onjuistheden als het gaat om penetratietesten. Hier is onze poging om voor eens en altijd een einde te maken aan de verwarring.

Penetratietesten zijn niet aantrekkelijk voor kleine bedrijven

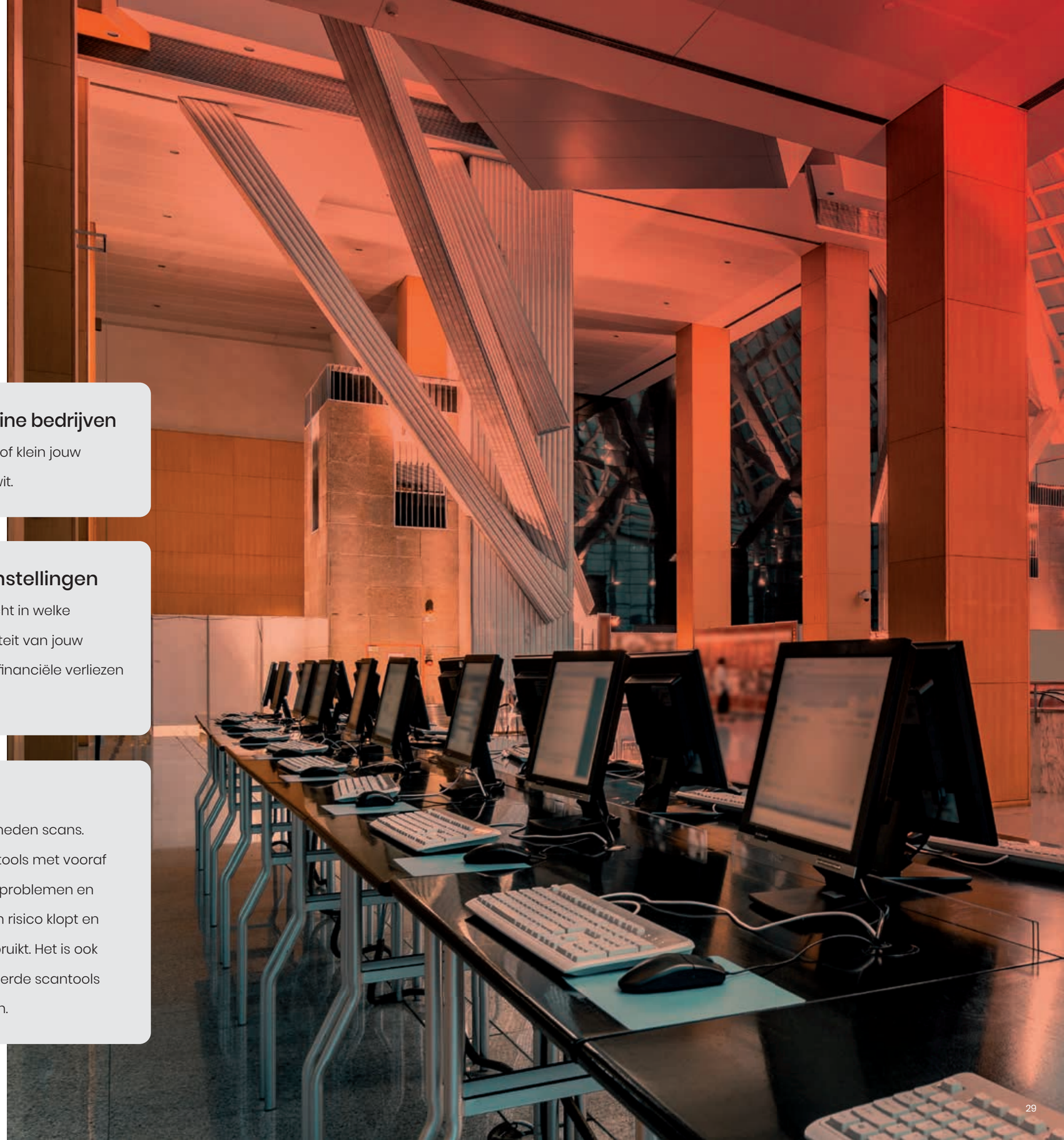
Dat klopt niet. Het maakt een cybercrimineel niet uit hoe groot of klein jouw organisatie is: een gemakkelijk doelwit is een gemakkelijk doelwit.

Het is alleen voor de overheid of financiële instellingen

Beveiliging is een integraal onderdeel van jouw bedrijf, ongeacht in welke branche je actief bent. Het is van vitaal belang om de continuïteit van jouw bedrijfsactiviteiten te waarborgen en om reputatieschade en financiële verliezen te voorkomen die met een hack gepaard gaan.

Ze zijn hetzelfde als kwetsbaarheden scans

Organisaties verwarren penetratietesten vaak met kwetsbaarheden scans. Kwetsbaarheden scans zijn gebaseerd op geautomatiseerde tools met vooraf gedefinieerde checks die controleren op bekende beveiligingsproblemen en patching, zonder te valideren (het controleren of het gevonden risico klopt en ook echt toepasbaar is) of de kwetsbaarheid kan worden misbruikt. Het is ook belangrijk om in gedachten te houden dat deze geautomatiseerde scantools geen kwetsbaarheden oppikken die niet in hun database staan.



Tot slot

Penetratietests bieden de mogelijkheid om jouw huidige beveiligingspositie te valideren en je bedrijf te beschermen. Door de juiste scope en het juiste type test te selecteren, kun je jouw beveiligingslekken eenvoudig identificeren en verhelpen. Het vinden van een penetratietestbedrijf dat je vertrouwt, met de juiste mensen om een goed resultaat te garanderen, is een fundamenteel aspect van het hele proces.

Het penetratietestbedrijf zal jou door elke fase van het proces moeten helpen, totdat de gebreken zijn verholpen en risico's tot een minimum zijn beperkt. De tests zijn niet alleen afhankelijk van de tools, maar ook van de creativiteit, vindingrijkheid en kennis van de tester om de vooraf gedefinieerde doelstellingen te bereiken.

Penetratietests vormen geen op zichzelf staande procedure, maar moeten een integraal onderdeel zijn van jouw algehele risicobeheer strategie. En onthoud altijd dat echte beveiliging een holistische, algemene benadering is die veel verder gaat dan technische maatregelen. Goede beveiliging moet een cultuur zijn binnen jouw bedrijf, gebaseerd op een cyclus van continue verbetering.

RedTeam
CYBER SECURITY

026 20 22 028
info@redteam-security.nl
Meander 901 6825 MH Arnhem

www.redteam-security.nl