Overheidsbrede Cyberoefening & Webinars

Red teaming in de praktijk

Oefenen met een realistische digitale aanval

#1.3

centrum informatiebeveiliging en privacybescherming

BIO Baseline Informatiebeveiliging Overheid

NORTHWAVE Intelligent Security Operations

Rijksoverheid

UNIE VAN WATERSCHAPPEN

Interprovinciaal Overleg van, voor en door provincies

VNG Vereniging van Nederlandse Gemeenten

Dit whitepaper is in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties tot stand gekomen als onderdeel van de Overheidsbrede Cyberwebinars en Cyberoefening.

Inhoudsopgave

Managementsamenvatting

Elke organisatie loopt risico's. De grote afhankelijkheid van technologie heeft digitale risico's nadrukkelijk aan het risicopalet toegevoegd. Digitale risico's dienen net als klassieke risico's, zoals brand, in kaart gebracht en beheerst te worden. Je wilt weten of de genomen maatregelen de veiligheid van de organisatie op het gewenste niveau brengen. Daar zijn verschillende meetinstrumenten voor. Een red team oefening is zo'n meetinstrument.

Een red team oefening levert een beeld op van de feitelijke veiligheid van de organisatie. Het is geen papieren oefening maar probeert de realiteit zoveel mogelijk na te spelen aan de hand van realistische aanvalsscenario's. Een red team oefening toetst daarmee op een unieke wijze het samenspel van jouw beveiligingsmaatregelen, zowel op het gebied van mensen, processen als techniek.

Daarnaast creëert een red team oefening *awareness*: het opent de ogen voor de huidige feitelijke staat van veiligheid van de organisatie en geeft aan waar nog werk verzet moet worden.

Het DOEL van een red team oefening is:

- Meten in welke mate de organisatie 'in control' is op het gebied van informatiebeveiliging (hoe digitaal weerbaar zijn we);
- Vaststellen van gebreken of zwakheden (wat kan beter);
- Trainen van het personeel, met name het security team (leren en verbeteren).

De OPBRENGST van een red team oefening is:

- Een beeld van de feitelijke veiligheid van jouw organisatie op het gebied van informatiebeveiliging;
- Een oefening van de gehele organisatie: mensen, processen én technologie;
- Het creëren van *awareness* in alle lagen van de organisatie: de medewerkers zijn zich bewust van hun handelen en de risico's.

Om dit te bereiken dient een red team oefening op de juiste wijze te worden opgezet. Dit wordt in dit document uitvoerig behandeld aan de hand van de volgende vijf stappen:

Inleiding

Een red team oefening is een cyberweerbaarheidsoefening in de vorm van een realistische aanvalssimulatie. Het zogenaamde red team voert een zo realistisch mogelijke digitale aanval uit op je organisatie. Het team test en traint hiermee jouw organisatie.

Dit whitepaper beschrijft wat er komt kijken bij een red team oefening, welke vormen, elementen en spelers er zijn bij zo'n oefening, en waar je rekening mee moet houden als je zelf een red team oefening wilt organiseren.

Hoofdstuk 1 bevat een uitleg van alle elementen van een red team oefening. De erop volgende hoofstukken beschrijven de praktische kant van een red team oefening: waar je aan moet denken, wat je moet doen, hoe je een leverancier kunt beoordelen, welke afspraken je van tevoren moet maken en wat er komt kijken bij de opvolging na afloop van een oefening.

Tenslotte bevat dit whitepaper een checklist waarin de belangrijkste aandachtspunten worden opgesomd.

1 Wat is een red team oefening?

1.1 Definitie

Als er brand uitbreekt is directe actie nodig. Het personeel moet worden geëvacueerd, de brandweer gebeld, noodprocedures in gang gezet. Als je onvoldoende voorbereid bent kan dat tot grote schade leiden en zelfs mensenlevens kosten. Maar hoe weet je of je voldoende voorbereid bent?

Een brandoefening levert antwoord op die vraag. Een goede brandoefening is meer dan alleen even evacueren. De hele procedure wordt zo echt mogelijk nagespeeld: het alarm, de evacuatie, de acties (zoals het bellen van de brandweer of het afschakelen van systemen). Tekortkomingen komen tijdens de oefening aan het licht. Deze tekortkomingen kunnen vervolgens verholpen worden.

Een red team oefening is het digitale equivalent van een brandoefening. De brand is hierbij de aanvaller die uit is op jouw kroonjuwelen of die jou schade wil toebrengen. De oefening bestaat uit een realistische aanval van een goedgezinde aanvaller: het red team. Zij helpen net als in de brandoefening je tekortkomingen aan het licht brengen zodat die verholpen kunnen worden.

> **Een red team oefening is een vorm van aanvalssimulatie. Het team dat in deze simulatie de aanvallende partij speelt probeert de organisatie zo realistisch mogelijk aan te vallen. Dit gebeurt aan de hand van aanvalsscenario's die worden opgesteld op basis van actuele dreigingsinformatie.**

De oefening is genoemd naar de aanvallende partij: het **red team**. De verdedigende partij, jouw security team, heet binnen de context van de oefening het **blue team**. De oefening wordt gecoördineerd door het **white team**.

De verdediging van een organisatie is een samenspel van mensen, processen en technologie.[1] Red team oefeningen gaan daarom verder dan alleen technologie. Alle aspecten van je security worden getest.

Aspecten die in een red team oefening getest worden zijn bijvoorbeeld:

- Hoe analyseert het security team de uitkomsten van de monitoring;
- Hoe kan een combinatie van techniek en mensen worden gebruikt om binnen te komen of verder te komen? (phishing, slecht gekozen wachtwoorden);
- Wat gebeurt er in de organisatie met een melding na detectie en analyse?

[1] Alternatieve benamingen voor deze driedeling zijn: mens, techniek en organisatie of mensen, systemen en processen. De Engelse term is people, process and technology.

1.2 Oorsprong

De term red team vindt zijn oorsprong in de koude oorlog. In oorlogssimulaties van het Amerikaanse leger was het red team de groep die de agressor speelde en het blue team de groep die de verdediging op zich nam. De agressor probeerde daarbij buiten de bestaande paden te treden om de verdediging te verrassen.

De kleur rood zou zijn gekozen omdat dat de kleur van de vlag van de Sovjet-Unie was. Ook de Sovjet-Unie hield overigens dergelijke oefeningen, waarbij de kleur van de agressor blauw was en de verdediger rood.

Een van de voordelen van een red team is dat ze als aanvaller wezenlijk anders denken dan de verdediger. De verdediger is vaak blind voor zijn eigen fouten. Het aanwijzen van 'tegendenkers' is veel ouder dan de term red team. Een bekend voorbeeld is de in 1587 door paus Sixtus V benoemde *advocatus diaboli*, de advocaat van de duivel. Als het Vaticaan voornemens was om iemand zalig te verklaren was het de taak van de advocatus diaboli om met redenen aan te komen waarom dat niet door kon gaan.

1.3 Doel

Bij een red team oefening is het niet de weerbaarheid tegen brand die getest wordt, maar de cyberweerbaarheid. De doelen van een red team oefening zijn net als bij een brandoefening:

- Meten in welke mate de organisatie 'in control' is op het gebied van informatiebeveiliging (waar staan we);
- Vaststellen van gebreken of zwakheden (wat kan beter);
- Trainen van het personeel, met name het security team (leren en verbeteren).

Het laatste doel uit dit rijtje is het belangrijkste. Een red team oefening is bedoeld om de organisatie te helpen. Het is dus géén krachtmeting en het is zeker niet de bedoeling om de organisatie 'kapot te hacken' of anderszins schade toe te brengen. Een red team oefening is educatief. Het rode team is jouw sparringpartner.

De meerwaarde van een red team oefening schuilt in het realistisch simuleren van een aanval. Een technische test kan vaststellen *of* je security werkt; een red team oefening vertelt *hoe* je security werkt. Je krijgt een blik op de feitelijke veiligheid van jouw organisatie. De uiteindelijke opbrengst van een red team oefening is dat jouw organisatie als de echte aanval komt daar gestroomlijnder en beter mee omgaat. En daarbij gaat het niet alleen om techniek: een red team oefening test nadrukkelijk ook mensen en processen. Het is een integrale oefening waarbij de hele organisatie betrokken is.

1.4 Een frisse blik

Mensen en organisaties worden blind voor hun eigen fouten. Daar zijn verschillende redenen voor. Eén daarvan staat in de psychologie bekend als bevestigingsvooroordeel (confirmation bias): de neiging om alleen te letten op informatie die de bestaande ideeën en overtuigingen bevestigen. Een andere reden is groepsdenken: de neiging om eensgezindheid binnen de groep boven een kritische instelling te stellen.

Een red team kijkt met een frisse blik naar de security van de organisatie. Omdat een red team van buiten de organisatie komt, heeft zij geen last van *confirmation bias* of groepsdenken.

Daarnaast brengt het red team de hacker-manier van denken mee, waarbij niets voor vaststaand wordt aangenomen. De red teamers kunnen denken als een aanvaller, maar staan aan jouw kant.

Een Amsterdamse firma had een indrukwekkende security, niet alleen digitaal, maar ook fysiek. Niemand kwam binnen zonder opgemerkt te worden. De firma liet een red team oefening uitvoeren waarbij ook de fysieke verdediging getest mocht worden. Hieruit kwam naar voren dat ze de voorkant van het pand weliswaar tot een onneembare vesting hadden gemaakt maar de achterkant niet. Omdat niet alle medewerkers elkaar kenden kon een lid van het red team gekleed in pak zich voordoen als een collega die even een kortere route nam en eenvoudig het balkon opklimmen waar op dat moment de vrijdagmiddagborrel werd gehouden.

Risicomanagement is tamelijk abstract en moeilijk objectief te meten. Door het inzetten van een realistische aanval begint het te leven onder de betrokkenen en wordt het concreet.

De organisatie waar de red team oefening zou worden uitgevoerd besteedde speciaal aandacht aan alle medewerkers die contact hadden met externen. Hier hadden ze extra bescherming ingezet. Alleen waren ze daarbij het HR-personeel vergeten. Een sollicitatiebrief met een bewerkte PDF als bijlage gaf het red team vrijwel direct de initiële toegang tot het bedrijfsnetwerk.

1.5 De red team oefening tegenover andere testen

Een red team oefening is maar een van de manieren om de staat van jouw beveiliging te onderzoeken met het doel verbeteringen aan te brengen. In deze paragraaf zetten we een aantal veel gebruikte en nuttige tests naast elkaar en bekijken we hoe de red team oefening zich tot de andere tests verhoudt.

1.5.1 Compliance audit

Een **compliance audit** geeft inzicht in de mate waarin afspraken, regels en procedures worden nageleefd. Een audit wordt vaak afgezet tegen een bestaande norm of wet, zoals ISO 27001, de BIO of de AVG. De auditor controleert of de beveiligingsmaatregelen en -procedures zijn geïmplementeerd zoals beschreven of voorgeschreven. De nadruk ligt hier op de processen binnen de organisatie.

1.5.2 Awareness test

Een **awareness test**, zoals bijvoorbeeld een phishing test, geeft inzicht in de mate waarin de mensen binnen jouw organisatie op de hoogte zijn van verschillende voor hen relevante aspecten van informatiebeveiliging. Herkennen ze verdachte situaties, weten ze hoe ze dan moeten handelen, en doen ze dat ook? De nadruk bij een awareness test ligt op de mensen binnen de organisatie.

1.5.3 Vulnerability assessment

Een **vulnerability assessment** is een door tools ondersteunde handmatige controle waarbij men zwakke plekken in een systeem opspoort[2]. Een vulnerability assessment is zeer breed in opzet. De gekozen systemen worden gescand op bekende zwakheden, maar na verificatie worden de gevonden kwetsbaarheden echter niet uitgebuit om dieper in het systeem te komen. Een vulnerability assessment is zuiver technisch van aard.

1.5.4 Pentest

Tijdens een **pentest** (penetration test) wordt geprobeerd om zo diep mogelijk het systeem binnen te dringen door middel van kwetsbaarheden en zwakheden in de configuratie. Hiermee wordt aangetoond dat het mogelijk is daadwerkelijk een systeem binnen te dringen. Een pentest begint vaak met een onderzoeksvraag, bijvoorbeeld: "*Is het mogelijk Windows domain admin te worden binnen mijn Windows Active Directory-omgeving?*" Pentesten zijn minder breed in hun opzet dan vulnerability assessments en brengen niet per definitie alle kwetsbaarheden in kaart. Ook een pentest is zuiver technisch van aard.

1.6 Organisatiebrede insteek

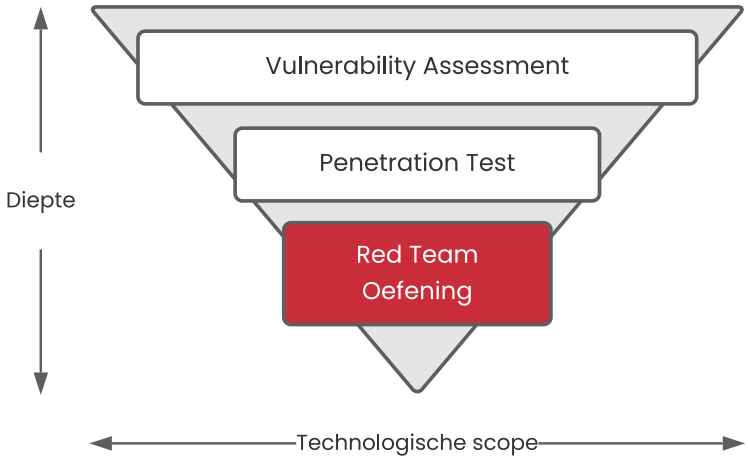
Een **red team oefening** heeft een organisatiebrede insteek en kijkt behalve naar techniek ook naar gedrag en reactie van personeel (mensen) en beveiligingsprocedures (processen). De opdracht voor het red team kan hierbij bijvoorbeeld zijn om toegang tot de kroonjuwelen van een organisatie te krijgen. Het team voert daarvoor een gerichte aanval uit op basis van een of meerdere aanvalsscenario's.

Een red team oefening zoekt nog meer de diepte dan een pentest. Er wordt ook getest of de geïmplementeerde beveiligingsprocedures en eventuele aanwezige monitoring en detectie in de praktijk afdoende werken om een gerichte aanval te detecteren, erop te reageren en ervan te herstellen (detect, respond, recover cyclus). Net als in de praktijk is het vinden van één zwakheid voldoende voor het red team om zich toegang te verschaffen tot het ICT-landschap van jouw organisatie. Eenmaal binnen gaat het red team gericht op zoek naar jouw kroonjuwelen.

---

[2] Zie ook het cybersecurity woordenboek: https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/

De hulpmiddelen om de technologische staat van je security te onderzoeken verschillen dus zowel in de breedte als in de diepte van elkaar, waarbij de red team oefening het diepst graaft.



Figuur 2: positie van de Red Team oefening t.o.v. vulnerability assessment en penetratie test.

1.6.1 Identificeren, beschermen, detecteren, reageren, herstellen

Behalve de diepte zoekt een red team oefening ook de breedte, alleen op andere vlakken dan andere tests. Niet alleen test de oefening naast techniek ook mensen en processen, ook worden meer stappen in de *cybersecurity lifecycle* getest.

[3] definieert de volgende vijf 'functies', of stappen in de *cybersecurity lifecycle*:

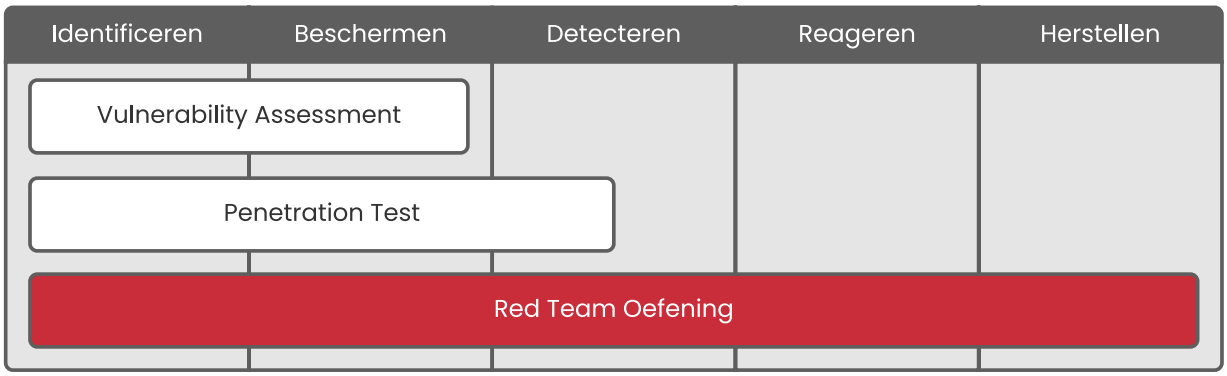
Tabel 1: NIST framework nader toegelicht

Functie	**Engels**	**Toelichting**
Identificeren	Identify	Inventarisatie van bedrijfsmiddelen en cyberrisico's (systemen, data, dreigingen, resources, risicomanagementstrategie, etc.)
Beschermen	Protect	Maatregelen om de kritieke gegevens, middelen en services te beschermen tegen aanvallen (antivirus, awareness, updates, etc.)
Detecteren	Detect	Ondernomen activiteiten om een cyberaanval te kunnen ontdekken (monitoring, anomalieëndetectie, etc.)

[3] https://www.nist.gov/cyberframework/framework

Reageren	Respond	Mogelijkheden om de schade tijdens een aanval te beperken en de aanval af te slaan (communicatie met relevante partijen, response plan, etc.)
Herstellen	Recover	Activiteiten om te herstellen van een (geslaagde of afgeslagen) aanval en terug te keren naar de normale operatie (systeemherstel, verbeteringen n.a.v. lessons learned, review, etc.)

Met het NIST framework in het achterhoofd kunnen we de drie technische security testen als volgt met elkaar vergelijken:



Figuur 3: Red Teaming bestrijkt alle facetten van het NIST framework.

De red team oefening is hier de enige die ook volledig test hoe detecteren, reageren en herstellen binnen de organisatie ingericht zijn. Een red team oefening levert een totaaloverzicht op. Werken mensen, processen en technologie goed samen bij een realistische aanval? Waar zitten de gaten? Wat werkte wel en wat niet?

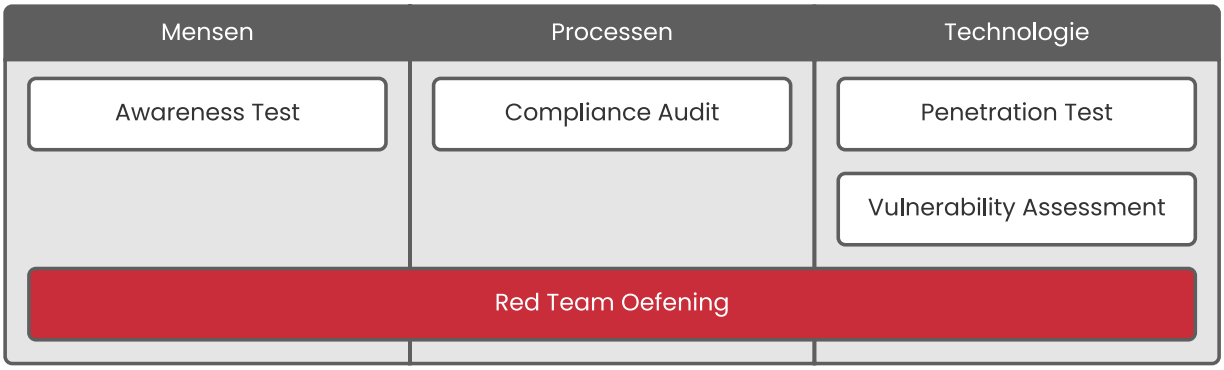
Het red team stond voor een raadsel. Ze hadden via phishing wachtwoorden achterhaald en probeerden daarmee in te loggen op een remote werkplek van de opdrachtgever. Dat werkte de ene keer wel en de andere keer niet, maar het was niet te voorspellen wanneer wel of niet.

Achteraf bleek dat de opdrachtgever gebruik maakte van multifactor authenticatie, waarbij de gebruikers een app hadden waar ze op akkoord moesten drukken bij het inloggen. Blijkbaar deden een aantal gebruikers dat automatisch, ook als ze niet zelf aan het inloggen waren. Zo bleek dat een technische oplossing (multifactor authenticatie) niet voldoende is, maar dat awareness over hoe je omgaat met zo'n app ook belangrijk is.

1.6.2 Mensen, processen, technologie

Als we tenslotte voor de eerder besproken testen naast elkaar zetten welke aspecten van informatiebeveiliging ze omvatten: mensen, processen en technologie, dan blijkt ook hier de red team oefening de meest omvattende te zijn.

Daarmee verliezen de andere tests overigens niet hun waarde: in hun specifieke deeldomein onderzoekt elk van deze tests elementen die bij een red team oefening niet altijd naar voren zullen komen. Een red team oefening zal de andere tests dan ook nooit vervangen en deze tests zullen op de geëigende tijdstippen óók moeten worden uitgevoerd.



Figuur 4: red team oefening raakt de aspecten: mensen, processen en technologie.

1.7 De kill chain

Een red team oefening simuleert een realistisch aanvalsscenario volgens de stappen die een aanvaller ook zou nemen. Zo'n aanval kent verschillende stappen, die weer opgesplitst kunnen worden in tactieken die al of niet in die stap gebruikt worden. Een veelgebruikt model is de Cyber Kill Chain van Lockheed Martin[4], maar er zijn veel meer bruikbare modellen, zoals bijvoorbeeld de Unified Kill Chain[5], opgesteld door Paul Pols, met als doel om de meest gebruikte modellen te verenigen. We vereenvoudigen de kill chain hier nog verder: in alle modellen zijn de stappen die de aanvaller doet ruwweg op te delen in drie fases.

Tabel 2: Kill chain fase overzicht

Fase	Cyber security term	Omschrijving
IN	Initial foothold	Alle acties tot en met het binnenkomen op het netwerk: verkenning, ontwikkeling, hacken, social engineering.

[4] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[5] https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

THROUGH	Network propagation	Binnen het netwerk bewegen: meer rechten verkrijgen, meer systemen overnemen
OUT	Action on objectives	Uitvoeren van het doel van de aanval: versleutelen met ransomware; stelen bedrijfsgeheimen, etc.

1.8 Dreigingsbeeld

Een red team oefening probeert de realiteit zo goed mogelijk te simuleren en zal daarom gebaseerd zijn op actuele dreigingen. Die dreigingsinformatie (ook wel *threat intel* genoemd) wordt verkregen door de analyse van actuele aanvallen. Het samenvoegen van dreigingsinformatie leidt tot een dreigingsbeeld. Een dreigingsbeeld kan generiek zijn, maar ook specifiek voor een bepaalde regio, sector of zelfs organisatie worden opgesteld.

De Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) publiceert jaarlijks een cybersecuritybeeld[6]. Dit bevat een dreigingsbeeld dat zich focust op de overheid en de Nederlandse vitale infrastructuur en kan, aangevuld met dreigingsinformatie uit andere bronnen, prima dienen als basis voor een red team oefening.

Een recente publicatie[7] van de AIVD/MIVD geeft meer informatie over door statelijke actoren uitgevoerde cyberaanvallen aan de hand van de Cyber Kill Chain. Per stap in de Cyber Kill Chain wordt uitgelegd welke activiteiten een statelijke actor uitvoert en welke preventieve en detectieve beveiligingsmaatregelen kunnen worden genomen.

Dreigingsinformatie kan overal vandaan komen. Er zijn wereldwijd vele organisaties die zich bezighouden met het verzamelen en analyseren van informatie. Veel hiervan wordt gedeeld. Soms moet je wel even weten waar je moet kijken. Zo houdt bijvoorbeeld Thai-CERT heel goed bij welke APT zich richt op welke sectoren en welke landen[8].

Een leverancier van red team oefeningen zal altijd een generiek dreigingsbeeld paraat hebben. Mogelijk is er voor jouw sector een specifieker dreigingsbeeld beschikbaar. Als dat niet het geval is, of het dreigingsbeeld nog specifieker moet zijn, dan zal het op maat moeten worden gemaakt. Wellicht kan je leverancier dat voor je doen, mogelijk moet je hiervoor een derde partij inschakelen.

---

[6] https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

[7] https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen

[8] https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

1.9 Kaders

Een formeel kader geeft houvast bij het modelleren van gerichte aanvallen. Het beschrijft op een gestandaardiseerde manier welke acties het aanvallende team kan nemen. De scenario's, die we in de volgende paragraaf zullen bespreken, kunnen eraan opgehangen worden.

Nog belangrijker is dat je dit ook terugziet in de rapportage. Oefeningen op basis van een formeel kader zijn goed in staat aan te geven waar precies de problemen in de informatiebeveiliging zitten en hoe je die kunt mitigeren.

MITRE ATT&CK

Een veelgebruikt kader voor het samenstellen van red team aanvalsscenario's is het MITRE ATT&CK framework.[9] Dit framework bevat (per 27 april 2021 – het framework wordt geregeld bijgewerkt) 14 tactieken (fases) met 185 aanvalstechnieken en 367 subtechnieken. Voor elk van deze technieken bevat het framework een beschrijving, maar geeft ook aan hoe de techniek gemitigeerd kan worden.

Het MITRE ATT&CK framework is gebaseerd op aanvallen die 'in het wild' zijn waargenomen en is daarmee een uitstekende basis voor scenario's.

Daarnaast biedt een formeel kader de mogelijkheid om bij een volgende red team oefening een andere aanbieder, die hetzelfde kader gebruikt, te kiezen. De uitkomsten kunnen dan met elkaar vergeleken worden, zodat je weet hoe jouw informatiebeveiliging zich door de jaren ontwikkeld heeft.

[9] https://attack.mitre.org/matrices/enterprise/

TIBER

Het Threat Intel Based Ethical Red teaming (TIBER) framework[10] is bedoeld voor organisaties in de financiële sector. Naast banken maken ook verzekeraars er steeds meer gebruik van. Een officiële TIBER oefening vindt in Nederland altijd onder toezicht van DNB (De Nederlandsche Bank) plaats. TIBER staat bekend als een betrouwbare maar stevige test die sterk drukt op de capaciteit van het blue team. Je kunt je voor een oefening laten inspireren door de TIBER-NL guide[11], gepubliceerd door DNB.

1.10 Scenario's

Een red team oefening is niet zomaar een willekeurige aanval. De aanval is zo opgesteld dat ze aansluit bij het dreigingsbeeld en de aspecten van de security die je wilt testen. Scenario's geven aan hoe de aanval eruit zal zien en welke acties het red team zal nemen. Een zekere mate van abstractie is daarbij noodzakelijk omdat het red team nog niet weet wat ze tegen gaat komen.

Een red team oefening werkt het best met een realistisch scenario. Wat is realistisch? Bij de meeste brandoefeningen zal kortsluiting realistischer zijn dan het afgaan van een bom.

Een red team oefening met een drone die op vierhoog het kantoor binnenvliegt is misschien wel sensationeel, maar voor de meeste organisaties te ver van de praktijk om de oefening zinvol te maken.

Een scenario voor een red team oefening beperkt zich niet tot technologie. Ook mensen en procedures worden immers getest.

Een professionele leverancier van een red team oefening zal altijd een generiek aanvalsscenario paraat hebben. Gezien de wereldwijde omvang van ransomware-aanvallen is het simuleren van een generieke ransomware-aanval (zonder versleuteling natuurlijk) bijvoorbeeld een voor de hand liggend scenario.

Idealiter speelt de klant zelf ook een rol in het bedenken van de scenario's. De kennis van de opdrachtgever en die van het red team vullen elkaar aan en maken zo betere en realistischere scenario's

[10] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[11] https://www.dnb.nl/media/1mdf3lmq/tiber-nl-guide.pdf

mogelijk. Door het delen van bedrijfsspecifieke strategische en tactische informatie kunnen de aanvalsscenario's meer op maat gemaakt worden.

Dat is niet valsspelen en het de aanvaller makkelijker maken. De red team oefening is immers bedoeld om met de voorhanden middelen de security zo goed mogelijk te testen. Het is niet zinvol om het red team tijd te laten spenderen aan het vinden van informatie die een aanvaller vroeg of laat toch wel zal achterhalen – die tijd is beter besteed aan de test zelf.

1.10.1 Voorbeelden van scenario's (versimpeld)

IN	Een aanvaller komt via één of meerdere technieken uit het MITRE ATT&CK framework zoals phishing met een malafide Office-document als bijlage, binnen op de computer van een werknemer.
THROUGH	De aanvaller weet admin-rechten te verkrijgen door meerdere technieken uit het MITRE ATT&CK framework toe te passen en verkrijgt daarmee toegang tot alle servers, waarop hij ransomware installeert.
OUT	Hij draait de ransomware, versleutelt daarmee alle data en vraagt losgeld.

Het red team kan dit scenario simuleren zonder versleuteling door het achterlaten van een gefingeerde losgeldboodschap.

IN	Een aanvaller komt het netwerk van een organisatie binnen door middel van het raden van een medewerker-wachtwoord. Vervolgens kan een VPN-verbinding opgezet worden door het ontbreken van multifactor-authenticatie, waarmee toegang tot het interne netwerk wordt verkregen.
THROUGH	Met behulp van meerdere technieken uit het MITRE ATT&CK framework zoals het stelen of vervalsen van Kerberos tickets (een authenticatiemethode) verhoogt de aanvaller zijn rechten en kan daarmee door het netwerk bewegen. Uiteindelijk wordt in de Windows Active Directory informatie gevonden over de systemen en het netwerksegment waar het SWIFT betalingssysteem zich bevindt. Uiteindelijk wordt ook toegang verkregen tot een tussenliggend system dat toegang heeft tot dit netwerksegment. De handleiding voor SWIFT betalingen staat ook op dit systeem.
OUT	Als eenmaal toegang is verkregen tot het SWIFT betalingssysteem maakt de aanvaller een groot bedrag over op een externe rekening waarmee zijn einddoel is bereikt.

Het red team kan dit scenario simuleren door bijvoorbeeld 1 cent over te maken naar een van tevoren bepaalde rekening.

IN	Een statelijke actor weet toegang te krijgen tot een overheidsorganisatie door middel van een bekende kwetsbaarheid in een VPN-server. Er wordt een achterdeur geplaatst om toegang te behouden tot het interne netwerk van de aangevallen organisatie waarna er drie maanden geen netwerkactiviteit is.
THROUGH	Na drie maanden zonder activiteit wordt de eerder geplaatste achterdeur gebruikt om toegang te krijgen tot het interne netwerk om vervolgens informatie te verzamelen over alle medewerkers en systemen binnen de organisatie. Na een week van inactiviteit worden alle gedeelde netwerkmappen doorzocht op informatie met behulp van specifieke zoekwoorden. Daarbij wordt in een tekstbestand een opgeslagen wachtwoord van een medewerker gevonden waarmee toegang tot een werkplek wordt verkregen. Alle gevonden informatie wordt gekopieerd naar die werkplek en vervolgens verstuurd naar systemen van de aanvaller. Na drie weken is de aanvaller weer terug en probeert van een aantal accounts de wachtwoorden te raden die toegang hebben tot een specifieke server waar gerubriceerde informatie is opgeslagen. In één geval lukt dat en daardoor wordt toegang verkregen tot de server.
OUT	Maandelijks komt de aanvaller terug en doorloopt dezelfde stappen waarbij weer naar specifieke informatie wordt gezocht. Alle nieuwe informatie wordt via de werkplek van een medewerker verdeeld in kleine stukken en verstuurd naar servers van de aanvaller.

Het red team kan dit scenario simuleren zonder daarbij daadwerkelijk de gerubriceerde informatie te kopiëren. In plaats daarvan kan een zogenaamde vlag of dummy-bestand worden geplaatst op de specifieke server waarmee kan worden aangetoond dat toegang is verkregen. Daarnaast is de aanbeveling de red team oefening over een langere periode door te laten lopen, zodat de activiteit van de aanvaller zo realistisch mogelijk kan worden gesimuleerd.

Het aantal scenario's kan beperkt gehouden worden. Eén of twee is meestal voldoende. Bij een TIBER oefening (§1.9) worden doorgaans twee scenario's opgesteld vanuit dreigingsinformatie, en mag het red team zelf een derde creatief scenario bedenken.

1.11 Andere vormen van red team oefeningen

Red team oefeningen zijn er in soorten en maten. Je kunt zelf bepalen hoe specifiek of hoe uitgebreid je de oefening wilt maken. Twee keuzes hebben we nog niet benoemd, en dat zullen we hier doen.

1.11.1 Assumed breach vs volledig scenario

Bij een volledig scenario worden alle stappen van de kill chain doorlopen. Je kunt er echter voor kiezen om de IN fase over te slaan. Dit heet een assumed breach scenario. Je geeft daarbij het red team de initiële toegang tot jouw omgeving vanuit de redenering dat een aanvaller vroeg of laat toch binnen kan komen.

Je mist daarmee een spannende fase van de red team oefening, maar behoudt het belangrijkste onderscheidende element van zo'n oefening. De oefening zal in veel gevallen niet minder waardevol zijn. Als het budget of de doorlooptijd beperkt zijn, dan verdient een assumed breach scenario mogelijk de voorkeur. Daar staat tegenover dat het red team in de IN fase vaak informatie in publieke bronnen vindt. Dit kan bijdragen aan het bewustzijn van de organisatie over de mate van openbaarheid van hun informatie.

Ook bij een volledig scenario is het uit tijd- en kostenoogpunt aan te raden om het red team na een bepaalde tijd toegang te verschaffen zodat ze de volgende, vanuit oefeningsoogpunt belangrijkere, fases kunnen testen. Je kunt er namelijk van uitgaan dat een aanvaller met voldoende tijd uiteindelijk altijd binnen weet te komen. Maak vooraf afspraken met de aanbieder over wanneer (na hoe lang) het red team toegang krijgt. Deze manier van toegang verschaffen tot de omgeving is geen valsspelen, maar simpel een keuze in de oefening.

1.11.2 Rood of Paars

Een red team hoort nauwkeurig bij te houden wanneer ze welke acties onderneemt en wat de resultaten daarvan zijn. Omdat het doel van een red team oefening is om de organisatie te laten leren, zullen deze resultaten altijd gerapporteerd moeten worden.

Zo'n rapportage vertelt wat het red team heeft gedaan, welke verdediging ze omzeild hebben, welke kwetsbaarheden ze gevonden hebben, plus aanbevelingen om die op te lossen. De rapportage kan in de vorm van een rapport zijn, maar ook in de vorm een presentatie met een vraag- en antwoordsessie.

Tijdens de aanvalssimulatie is er nog een partij actief: het blue team, het security team van je eigen organisatie. Het blue team is (meestal) niet op de hoogte van de oefening, maar kan de activiteiten van het red team wel ontdekken en maatregelen nemen.

Een purple team oefening is een red team oefening waarbij de rapportage van het red team direct naast de bevindingen van het blue team wordt gelegd. Een purple team oefening kan gedetailleerder zijn in de aanbevelingen omdat wordt meegenomen wat het blue team gezien en gedaan heeft. De nadruk van een purple team training ligt op het trainen van het blue team.

Dit kan door achteraf de bevindingen naast elkaar te leggen, bijvoorbeeld in een gezamenlijke workshop. In zo'n workshop kunnen het red team en blue team gezamenlijk aanvullende beveiligingsmaatregelen

opstellen. Maar je kunt ook kiezen voor een intensievere variant waarin al tijdens de red team oefening tussen beide teams gecommuniceerd wordt.

Om het maximale uit de oefening te halen kan een purple team oefening geschikter zijn dan een red team oefening. Het vraagt aan de andere kant meer van het red team, en zeker meer van het blue team. Als het hoofddoel van de oefening niet het trainen van het blue team is, voegt het mogelijk te weinig waarde toe.

2 Voorbereiding

Een aanvalssimulatie is geen kwestie van even een red team inhuren en hun gang laten gaan. Om er het maximale uit te halen moet de organisatie van tevoren zijn huiswerk doen. Dat levert een betere vraagstelling op bij de aanbieder en meer controle over het proces. Je wilt niet overgeleverd zijn aan de grillen van een leverancier. De goede leveranciers zullen je bij de intake ook vragen naar de onderstaande zaken.

2.1 Is een red team oefening geschikt voor mij?

Een red team oefening zal niet in elke omstandigheid de beste keuze zijn. Afhankelijk van je doel, mogelijkheden en beveiligingsniveau kunnen andere opties verstandiger zijn.

De keuze voor een red team oefening zal *onder andere* afhangen van:

- Volwassenheid van de organisatie en de security;
- De huidige status van jouw maatregelen;
- Of security monitoring is ingericht.

2.1.1 Waarom géén red team?

Als je nog geen securitymaatregelen hebt genomen, dan verdient het de aanbeveling dat eerst te doen. De beste manier om hiermee te starten is het inrichten van een securitymanagementproces aan de hand van een standaard zoals ISO27001 of de Baseline Informatiebeveiliging Overheid (BIO).

Als je bezig bent met het implementeren van één of meer securitymaatregelen, zoals het opzetten van een SOC (Security Operations Center) of het uitrollen van nieuwe antivirussoftware, dan is dit niet het moment om een red team oefening te starten. Maak eerst de implementatie van de nieuwe maatregelen af, dan kunt je die vervolgens testen met een red team oefening.

Ook als je nog niet helder hebt wat jouw risico's en kroonjuwelen zijn, dan loont het om dat eerst boven water te krijgen voordat je aan een red team oefening begint.

Als je nog nooit een penetratietest of vulnerability assessment hebt laten uitvoeren dan is het mogelijk verstandiger om dat eerst te laten doen.

2.1.2 Waarom wél een red team?

Er kunnen verschillende redenen zijn om wel te kiezen voor een red team oefening. Bijvoorbeeld:

- Security monitoring is ingeregeld, en je wilt weten in hoeverre je daarmee in control bent;

- Je hebt verschillende securitymaatregelen genomen en wilt weten hoe de organisatie reageert op een gerichte aanval;
- Je wilt de bewustwording op bestuursniveau verhogen; er dient meer geïnvesteerd te worden in monitoring en detectie – vanwege de overkoepelende insteek van een red team oefening kan het een goed overtuigingsmiddel zijn;
- Je wilt de organisatie realistisch trainen.

In geval van twijfel over welke testvorm te kiezen is het aan te raden om je te laten adviseren welke aanpak op dit moment het nuttigst is voor jouw organisatie.

2.2 De kroonjuwelen van jouw organisatie

Wat zijn de kroonjuwelen van mijn organisatie?

Deze zal je koste wat het kost willen beschermen. Ze zijn het doelwit van hackers, en daarmee ook van het red team. Wat zijn de meest essentiële assets van de organisatie? Waar ligt het bestuur bij wijze van spreken 's nachts van wakker?

Denk daarbij niet aan techniek. Een incident waarbij een aanvaller domain administrator weet te worden, is op zichzelf nog geen ramp. Het kwijtraken van een klantenbestand, belangrijke ontwerpen, of manipulatie van de Industrial Control Systemen zijn dat wellicht wel. Dit is binnen jouw organisatie als onderdeel van een risicoanalyse wellicht al eens in kaart gebracht.

Welke maatregelen heb ik genomen om ze te beschermen?

De red team oefening is bedoeld om die maatregelen te testen. Dat betekent ook dat een red team oefening zinloos is als er nog geen of onvoldoende maatregelen genomen zijn. Een zekere mate van volwassenheid in het beveiligingsdomein is noodzakelijk. Is die er niet, dan zijn er waarschijnlijk betere manieren om het beveiligingsniveau te verhogen alvorens aan een red team oefening te beginnen.

2.3 Definieer het doel van de red team oefening

Wat is het gewenste eindresultaat van de red team oefening?

Waar wil ik de red team oefening voor gebruiken, wanneer is het een succes?

De scope en vorm van een red team oefening zal afhangen van het uiteindelijke doel. Die doelen kunnen heel gevarieerd zijn, maar moeten wel helder zijn vóór je een red team oefening aanvraagt. Mogelijke doelen zijn:

- Gaten in jouw monitoring en detectie opsporen;
- Jouw monitoring en detectie verbeteren;
- De effectiviteit van jouw SOC onderzoeken;
- Onbekende risico's identificeren (aanvallers denken immers anders);
- Awareness creëren binnen de organisatie of bij de directie;
- Aantonen dat jouw organisatie in control is;
- Het management overtuigen dat er meer bewustzijn en budget nodig is voor security;
- Jouw blind spots identificeren.

Bedenk dat een red team oefening voor veel van de doelen hierboven een hulpmiddel is, geen wonderpil. Vaak zul je ook andere instrumenten in moeten zetten om zo'n doel volledig te halen.

Welke vorm van red team oefening sluit het beste aan bij mijn doel?
De vorm die je kiest (zie §1.11) zal afhangen van de gewenste resultaten, maar ook van budget (§2.5) en beschikbare tijd (§2.6).

2.4 Dreigingsbeeld vaststellen

Waar moet ik bang voor zijn?
Verschillende managementtrainingen maken gebruik van een rollenspel, waarbij een acteur die ene collega naspeelt die het bloed onder je nagels vandaan haalt. Door het naspelen van een zo reëel mogelijke situatie leren we hoe we het beste kunnen reageren. Zo'n rollenspel werkt alleen als we de acteur van tevoren inlichten over de situatie en het gedrag van de betreffende collega. Hoe meer informatie we verschaffen, hoe reëler de acteur de situatie kan neerzetten en hoe groter het leereffect.

Het red team is de acteur in uw aanvalssimulatie. Ook hier geldt dat meer startinformatie zorgt voor een betere oefening. Wat zijn de reële dreigingen? Waar liggen mijn zwaktes? Wie moet het red team spelen? Een ransomware-crimineel die het netwerk wil platleggen? Een statelijke actor die op bepaalde informatie uit is?

Het helpt om vooraf **samen met het red team** tot een zo nauwkeurig mogelijk dreigingsbeeld te komen. Je kunt dit zelf opstellen, maar je kunt het ook laten doen door de red team provider, of zelfs door een derde partij.

Het vooraf verschaffen van deze informatie lijkt misschien op valsspelen maar is integendeel juist een hulpmiddel waardoor het red team de simulatie beter kan uitvoeren. Een red team oefening is geen wedstrijd tussen Rood en Blauw, maar een manier om met de beschikbare tijd en middelen een optimaal resultaat te halen. De keuzes die je maakt hebben invloed op de test en het budget.

2.4.1 Actoren

Wie heeft het op mij gemunt?
Welke actoren zijn actief op basis van het profiel van je organisatie/industrie, en hoe gaan die te werk (gericht, ongericht, etc.)? Wat voor resources hebben zij tot hun beschikking (tools, geld, tijd)? Wat zijn hun doelstellingen?

2.4.2 Scope

Welke aanvalsvormen wil ik uitsluiten?
Een van de keuzes die je maakt, is of fysieke aanvalsvectoren wel of niet meegenomen moeten worden. Fysieke aanvallen komen voor (een Wi-Fi-antenne op de parkeerplaats, een Raspberry Pi in het netwerk inpluggen) maar zijn zeldzaam en vaak gebonden aan een bepaald soort actoren. Wellicht kunnen ze in jouw scenario uitgesloten worden.

2.5 Budget

Wat is mijn budget?

Stel een realistisch budget vast in overeenstemming met jouw wensen.

Kies met een beperkt budget bewust voor een beperkte scope.

Hoewel verschillende aanbieders verschillende prijzen zullen hanteren, willen we toch een zeer ruwe indicatie geven van de kosten die verbonden zijn aan een red team oefening. We doen dat in de vorm van de tijd die de verschillende onderdelen van een red team oefening kosten. De werkelijke tijdsduur kan afwijken van de indicatieve duur – dit hangt onder meer af van de gekozen scenario's en einddoelen.

Fase	**Tijdbesteding**
Voorbereiding / rules of engagement opstellen	1 dag - 1 week
Threat intelligence	1 week - 4 weken
Red team oefening IN fase	2 weken - 8 weken
Red team oefening THROUGH fase	2 weken - 8 weken
Red team oefening OUT fase	1 week - 4 weken
Rapportage	1 week - 2 weken
Purple teaming sessie (achteraf)	1 dag - 2 weken

2.6 Planning

Wanneer moet de oefening plaatsvinden?
Hoe lang kan de oefening ongeveer duren?
Wanneer mag niet geoefend worden?

Een red team oefening vraagt tijd en capaciteit van de organisatie. Daar moet met de planning rekening mee worden gehouden om de organisatie niet op de verkeerde momenten te veel te belasten. Ook moet vastgesteld worden wanneer het red team **niet** mag aanvallen. Hoewel daarmee enigszins in realisme wordt ingeboet kan het toch verstandig zijn om ze tijdens het weekend, of tijdens *Patch Tuesday*, even te laten stoppen.

Ook over de doorlooptijd moet nagedacht worden. Een langere doorlooptijd geeft het red team de gelegenheid om de activiteiten meer te spreiden. Het security team heeft meer gelegenheid om de activiteiten van het red team te detecteren. Aan de andere kant geeft dit het red team de mogelijkheid om door de spreiding van activiteiten minder op te vallen. Afhankelijk van het gekozen scenario kan dit een betere benadering van de werkelijkheid zijn.

3 Leverancier selectie

Bij een formele aanbestedingsprocedure is het van belang een heldere uitvraag te doen. Hoe beter je weet wat je wilt, des te specifieker is je offerteaanvraag en des te beter kun je offertes tegen elkaar afwegen. In het voorgaande hoofdstuk beschreven we wat je zelf moet voorbereiden, hier wat je kunt vragen van de leverancier.

3.1 De offerte aanvraag

Voor je een offerte aanvraagt zul je het voorwerk uit hoofdstuk 2 grotendeels afgerond moeten hebben. Aanbieders kunnen een betere offerte uitbrengen als de volgende zaken in *generieke* termen al in de uitvraag zijn vermeld:

- Wat is het doel van de red team oefening?
- Waar ben ik bang voor?
- Wat zijn de kroonjuwelen van mijn organisatie?[12]
- Wat is mijn budget?
- Welke maatregelen wil ik testen?
- Welke vorm moet de red team oefening hebben?
- Hoe uitgebreid wil ik testen? Hoeveel scenario's wil ik testen?
- Wie levert de dreigingsinformatie en hoe specifiek moet deze zijn?
- Wat zijn de gewenste eindproducten (rapportage, workshop, etc.)

Het antwoord op een aantal van deze vragen wil je misschien niet zomaar delen. In dat geval kun je de aanbieders om een geheimhoudingsverklaring vragen.

Aanbieders begrijpen dat het bovenstaande wensenoverzicht indicatief is en er in overleg verfijningen en aanpassingen kunnen worden aangebracht. Om misverstanden te voorkomen is het wel aan te raden om de uiteindelijke afspraken met de aanbieder op papier vast te leggen.

Tip: Neem vooraf contact op met de aanbieders en bespreek je wensen en wat zij te bieden hebben. Niet alleen geeft dit een goede basis voor de offerteaanvraag, maar het geeft aanbieders ook de mogelijkheid om zich terug te trekken als blijkt dat zij niet kunnen aanbieden wat jij wil.

[12] Vanzelfsprekend zal je hier de nodige voorzichtigheid in acht nemen. Kroonjuwelen deel je niet met Jan en alleman. Het volstaat om een beeld te verschaffen van de *aard* van de kroonjuwelen.

3.2 Vragen aan de aanbieder(s)

Niet alleen jij moet je huiswerk doen, ook de aanbieder moet kunnen aantonen dat hij zijn huiswerk gedaan heeft. Hieronder een aantal vragen die je aanbieders kunt stellen om de serieuze aanbieders van de cowboys te onderscheiden.

De antwoorden op deze vragen kunnen vooraf gegeven worden, maar zouden ook terug te vinden moeten zijn in de offerte.

3.2.1 Generiek dreigingsbeeld

Vraag de aanbieder naar het huidige dreigingsbeeld.

Een serieuze aanbieder moet direct kunnen vertellen wat het huidige dreigingslandschap is, en voor welke actoren en aanvalsmethodieken het meest gevreesd moet worden. Ze zullen over het algemeen geen dreigingsbeeld klaar hebben liggen voor jouw specifieke branche en locatie, aangezien dit maatwerk is.

3.2.2 Voorbeeldrapportage

Vraag de aanbieder om een voorbeeldrapportage.

Dat geeft inzicht in wat en hoe uitgebreid er gerapporteerd wordt en hoe dat aansluit bij jouw wensen. De aanbieder zal in de voorbeeldrapportage allicht bepaalde delen hebben verwijderd om de privacy van een eerdere klant te beschermen.

Een rapportage dient voldoende informatie te bevatten voor het blue team om de aanvalsstappen terug te zoeken in hun systeem. De rapportage moet niet alleen bevatten wat het red team gedaan heeft, maar ook wanneer.

Een rapportage hoeft geen document te zijn, maar kan ook in de vorm van een presentatie gegeven worden. In dat geval kan de aanbieder als voorbeeld een slidedeck van zo'n presentatie kunnen laten zien.

3.2.3 Framework

Vraag de aanbieder welk framework of kader hij gebruikt om de scenario's aan op te hangen.

Gebruikt de aanbieder een formeel kader of werkt hij volgens 'een eigen' model of zonder kader?

3.2.4 Scenario's

Vraag de aanbieder hoe zij voor realistische scenario's zorgen, of hoe ze daarbij helpen.

Een realistisch aanvalsscenario bouw je over het algemeen niet alleen. Als je gaat voor een generiek scenario, dan zal de aanbieder deze als het goed is al hebben klaarliggen. Voor een meer specifiek

scenario is samenwerking tussen opdrachtgever een aanbieder nodig. Beiden bezitten relevante kennis die de ander niet heeft.

3.2.5 Competentie

Vraag de aanbieder zijn competentie aan te tonen

Een goede aanbieder zal graag zijn competentie aantonen. Je wilt de volgende zaken weten van een potentiële aanbieder:

Certificering, opleidingen, publicaties

Met recente certificeringen, opleidingen en publicaties kan de aanbieder aantonen dat de leden van het red team hard werken om bij te blijven in een snel veranderende wereld. Er zijn veel verschillende opleidingen. Opleidingen die een praktijkgedeelte (en praktijktoets) bevatten verdienen de voorkeur boven theoretische opleidingen. Niet alle opleidingen zijn op maat gemaakt voor red team oefeningen, en géén certificaat betekent niet automatisch dat de leden níet goed getraind zijn. Vraag ook naar praktijkervaring.

Vraag naar publicaties van de aanbieder. Publicaties tonen aan dat de aanbieder een volwaardig lid is van de 'community', en nieuwe technieken en kwetsbaarheden met andere partijen deelt.

Referenties

Vraag of de aanbieder je in contact kan brengen met voorgaande klanten, bij voorkeur in dezelfde sector. Van hen kun je meer horen over de aanpak van de aanbieder.

Screening

Als geheimhouding noodzakelijk is heb je mogelijk als extra eis dat de medewerkers van de aanbieder een veiligheidsonderzoek hebben gehad of Verklaring Omtrent het Gedrag (VOG) kunnen tonen.

3.3 Offertes beoordelen

Een offerte dient antwoord te geven op de geformuleerde vragen en wensen. Let daarnaast op de volgende criteria:

Aanpak en planning

Hoeveel tijd denkt de aanbieder nodig te hebben? Is dit helder beargumenteerd? Is duidelijk omschreven hoe men gaat testen? Zijn de verschillende fases van de test beschreven?

Omgang met gevoelige informatie

Meldt de offerte hoe de aanbieder omgaat met gevoelige informatie? Wordt melding gemaakt van een geheimhoudingsverklaring, verwerkersovereenkomst en bewaartermijn?

De offerte hoeft dit niet uit te spellen. Je kunt hierover ook in een latere fase afspraken maken met de door jou gekozen aanbieder.

Prijs

Je moet de prijs afwegen tegen de kwaliteit van het aanbod. Als het doel is om het securityteam te trainen en een laaggeprijsd aanbod gebruikt geen formeel model en rept niet over een rapportage of evaluatie, dan voldoet dit aanbod niet aan je eisen.

Scenario's

De gebruikte scenario's zullen niet uitgeschreven staan in de offerte, maar het aantal scenario's en de diepte ervan wel. Realistische scenario's horen bij de prijs inbegrepen te zijn.

Kwaliteit van de offerte

Adresseert de offerte alle bovengenoemde punten in een overzichtelijk geheel of heeft de aanbieder deze gegevens buiten de offerte om verstrekt? We herhalen hier een aantal van de bovenstaande punten.

- Referenties;
- Certificering, opleidingen, link naar publicaties;
- Screening, geheimhouding;
- Voorbeeld-rapportage;
- Het voorgestelde kader;
- Generiek dreigingsbeeld.

Tip: nodig aanbieders uit om de offerte toe te lichten en vragen te beantwoorden.

4 Afspraken maken

Je hebt jouw huiswerk gedaan en uit de aanbieders een leverancier geselecteerd, wat nu? Voor de uitvoering van de red team oefening gaat beginnen zullen nog een aantal afspraken met de leverancier moeten worden gemaakt.

4.1 Wanneer uitvoeren?

Spreek met de leverancier een startdatum en doorlooptijd af. De oefening drukt ook op jouw resources en kan daarmee business impact hebben – wanneer past het in de planning? Andersom wil je met een red team de realiteit zo goed mogelijk simuleren en daarom misschien niet het 'rustigste' moment kiezen.

4.2 Juridisch kader

Het is sterk aan te raden om voorafgaand aan de red team oefening juridische afspraken te maken. Beide partijen nemen risico's die afgedekt moeten worden. In de meeste gevallen is een standaard overeenkomst voldoende, maar ook hier is soms maatwerk noodzakelijk. Elementen van het juridisch kader (denk aan de vrijwaringsverklaring) kunnen ook al in de offerte worden opgenomen.

Een juridisch kader zal onder meer de volgende elementen omvatten:

- Scope: Wat wordt wel en wat wordt niet getest? Denk hierbij aan uw IT-leveranciers, IP-ranges, uw procesautomatisering, etc. Uitsluitingen worden bij voorkeur expliciet opgenomen;
- Vrijwaring: Het uitvoeren van een red team oefening is zonder toestemming van de opdrachtgever strafbaar. Beide partijen gaan een overeenkomst aan waarbij het red team gevrijwaard wordt van vervolging. Je geeft het red team toestemming om in te breken op en te bewegen binnen de systemen. Waar van toepassing moeten de IT-leveranciers ook toestemming geven;
- Aansprakelijkheid: De opdrachtgever mag ervan uitgaan dat de leverancier de opdracht op een verantwoordelijke en zorgvuldige wijze uitvoert. Als de leverancier bewust of onbewust buiten de afspraken om schade aanricht dan zal zij hier echter in de regel zelf voor aansprakelijk zijn. Afspraken over aansprakelijkheid dienen vooraf vastgelegd te zijn.
- Verwerkersovereenkomst: In sommige scenario's verwerkt het red team persoonsgegevens en zal zich daarbij aan de AVG moeten houden. Ook over de opslag en verwerking van andere gegevens dienen afspraken te worden gemaakt;
- Geheimhoudingsverklaring: gevoelige informatie die door jou verstrekt of tijdens de oefening gevonden wordt, mag niet gedeeld worden met derden;
- Bewaartermijnen: Binnen welke termijn wordt de data door de leverancier vernietigd.

Tip: Betrek uw juridische afdeling hierbij.

4.3 Vastleggen en delen resultaten

Een red team hoort tot in detail vast te leggen wat ze heeft gedaan. De pogingen en resultaten worden op zo'n manier vastgelegd dat de oefening goed kan worden geëvalueerd. De volgende zaken worden gedeeld:

- Logboek: een beschrijving van de acties die het red team heeft uitgevoerd, met bijbehorende tijden. De red team mantra is: "Als er geen log is, hebben er geen acties plaatsgevonden.";
- Bewijsvoering: De verslaglegging van het red team moet gedetailleerd genoeg zijn om het blue team in staat te stellen om achteraf na te gaan wat wanneer gebeurd is en dat te correleren aan de signalen die ze op dat moment kregen;
- Presentatie/workshop achteraf (of, bij purple teaming, eventueel tussentijds).

4.4 Aanvalscenario's

Wat zijn goede potentiële aanvalsscenario's?

Niet alles kan getest worden in een red team oefening, en je wilt niet dat het red team lukraak aanvalt. Het loont om in overeenstemming met de leverancier aanvalsscenario's op te stellen. Het aantal scenario's kan beperkt gehouden worden. Eén of twee is meestal voldoende. Bij een TIBER oefening (§1.9) werden twee scenario's opgesteld op basis van dreigingsinformatie en mag het red team zelf een derde geavanceerder scenario bedenken.

4.5 Rules of engagement

Rules of Engagement zijn heldere afspraken die door de deelnemende partijen van tevoren worden vastgelegd. Hierdoor weet iedereen waar hij aan toe is en loopt de oefening, ook als er onvoorziene omstandigheden zijn, soepeler. Ook zijn er aan een red team oefening risico's verbonden, die je wilt beheersen door goede afspraken te maken.

De volgende zaken zou je moeten terugzien in de *Rules of Engagement*:

Doel van de oefening	Zie §2.3
Organisatie(onderdeel) in scope	Mogen ketenpartners worden aangevallen? Worden leveranciers (veel organisaties hebben hun ICT uitbesteed) betrokken? Hoe?
Kroonjuwelen	Welke kroonjuwelen of doelen wordt getracht tijdens de red team oefening toegang toe te krijgen? Dit bepaalt mede wanneer de oefening is afgerond.
Technische scope	Wat is de IP-range van de organisatie (om te voorkomen dat per ongeluk de verkeerde organisatie wordt gehackt)?

	Mag de procesautomatisering (OT) van de organisatie worden aangevallen?
Planning	Wanneer wordt de test uitgevoerd? Tijdens kantooruren of ook daarbuiten? Weekends? Feestdagen? Zijn er relevante *change windows* of andere redenen om op bepaalde dagen van de ICT af te blijven?
Wel en niet toegestane activiteit(en)	Mogen bijvoorbeeld fysieke middelen worden gebruikt?
Wie is op de hoogte	Wie weten wel en wie weten niet dat de oefening plaatsvindt? (Zorg hierbij dat de juiste mensen op de hoogte zijn om snel te kunnen de-escaleren.)
Teams en contactinformatie	Om snel kunnen schakelen in voorziene en onvoorziene situaties.
Communicatie	Zijn de helpdesk/SOC op de hoogte van de test? Zijn leveranciers op de hoogte? Wat is de frequentie van communiceren? Welke communicatiekanalen (regulier, escalatie)? Wat moet met wie gecommuniceerd, wat niet?
Vertrouwelijkheid	Welke informatie mag wel en niet uitgewisseld worden tussen de verschillende teams?
Escalatiepad	Wanneer gaat het white team escaleren? Waar ligt de beslissingsbevoegdheid voor een go/no go op vervolgacties?
Verslaglegging	Hoe en wanneer vindt verslaglegging plaats?
Voortijdig afbreken	Wanneer wordt de test afgebroken (denk aan calamiteiten, of het bekend worden van een Citrix-bug tijdens de oefening)?

5 Uitvoering

Niet alleen het red team is aan het werk tijdens de uitvoering van de aanvalssimulatie. Het blue team (het security team van jouw organisatie) zal al of niet een aantal activiteiten van het red team waarnemen en daarop acteren. Dat kan gevolgen hebben voor de uitvoering. Het red team verschaft het white team, de 'spelleiding', reguliere status updates. Het white team ziet toe op de juiste communicatie en stuurt bij waar dat nodig is:

- Beheersen escalatie. Als het white team observeert dat het blue team de activiteiten van het red team ontdekt heeft en gaat escaleren dient deze escalatie beheerd te worden – het white team zal het blue team op de hoogte stellen van de test. De test wordt niet afgebroken maar verandert van focus, aangezien het blue team er nu vanaf weet;
- Leg-up. Als de IN fase van de aanvalssimulatie te lang dreigt te duren is het verstandig om het red team toegang te geven om alsnog de THROUGH en OUT fases van de aanval uit te kunnen voeren. Hoewel het op zich goed nieuws is dat het team er niet in kwam, moeten we ervan uitgaan dat een aanvaller met voldoende geduld vroeg of laat altijd binnen zal komen;
- High-risk fixen tijdens de uitvoering. Het kan voorkomen dat tijdens de oefening kwetsbaarheden worden gevonden die directe actie vereisen. In dat geval zal het red team het white team op de hoogte brengen.

6 Opvolging

Een red team oefening wordt afgesloten met kennisoverdracht. Het doel is immers om te leren van de oefening. Na afloop vindt dan ook een bespreking met het blue team plaats. De vorm en diepgang van deze bespreking is van tevoren afgesproken. Het kan een rapport of presentatie zijn (een presentatie is levendiger, interactiever en kun je niet in de la stoppen), maar ook een meerdaagse workshop in het geval van een purple team oefening.

Het red team laat sporen achter op het netwerk: malware, sessies, instellingen. Ze leveren hier na afloop een overzicht van zodat de organisatie dit kan opruimen. Dit kost de opdrachtgever achteraf tijd, die ook ingepland dient te worden.

6.1 Het vervolg

Behalve een bespreking met het Blue Team zullen - ook op directieniveau – nog meer acties moeten plaatsvinden om de lessen van de oefening optimaal te benutten:

- Interne evaluatie – wat heeft de red team oefening opgeleverd, wat hadden we verwacht en waar schrokken we van? Wat hebben we geleerd?
  Omdat een red team oefening als voornaamste doel heeft om de organisatie te verbeteren dient de oefening altijd gekoppeld te worden aan een gedegen evaluatie. Zonder zo'n evaluatie gaat een groot deel van het leereffect verloren;
- Opvolging resultaten – de resultaten van de red team oefening zijn de basis voor acties die de opdrachtgever zal moeten uitvoeren om het securityniveau te verhogen. Zonder deze acties is het nut van een red team oefening beperkt. De uitkomsten van de red team oefening worden naast de Security Roadmap gelegd en deze wordt geüpdatet waar dat nodig is;
- Lessons learned delen – laat de lessen van de red team oefening niet binnen het kleine gremium blijven waarin het is uitgevoerd. De uitkomsten van de red team oefening kunnen gebruikt worden als basis om awareness te creëren, zowel bij de directie als organisatiebreed.
  Deel de lessen ook extern, met partnerorganisaties of in de sector. ISACs[13] zijn hier uitermate geschikt voor. Er zijn te veel aanvallen om op security te concurreren. Vroeg of laat krijgt elke organisatie met een aanval te maken. Het delen van de geleerde lessen maakt onze samenleving als geheel weerbaarder. Het aantal organisaties met angst om (gefixte) kwetsbaarheden te delen neemt gelukkig af; delen is juist een teken van een volwassen organisatie.

[13] ISAC: Information Sharing and Analysis Center: een non-profit organisatie met als doel het delen van dreigingsinformatie.

Een red team oefening kan een uitstekend middel zijn om organisatiebrede awareness te creëren.

"Wij blijven de resultaten uitdragen, aan de raad van bestuur, aan de ondernemingsraad, op de werkvloer, en we zien overal de monden openvallen. Als gevolg van de red team oefening en de presentatie van de resulteren is onze awareness over de hele linie zichtbaar verbeterd."

7 Terminologie

Een korte omschrijving van een aantal termen die in dit whitepaper worden gebruikt. Voor meer terminologie verwijzen we je door naar het Cyber Security Woordenboek[14].

Aanvalsscenario	Beschrijving (in grote lijnen) van de stappen en doelstellingen van de aanvallers.
APT	Advanced Persistent Threat – een threat actor die langere tijd in het netwerk aanwezig is en actief detectie probeert te vermijden. APT's worden vaak in verband gebracht met statelijke actoren.
Awareness	De mate waarin je medewerkers zich bewust zijn van digitale dreigingen, de risico's die ze lopen en wat ze kunnen doen om die risico's te verminderen.
Blue team	Het blauwe team: het securityteam dat zich verdedigt tegen dreigingen en aanvallen. Het blue team is de verdediger in de aanvalssimulatie.
ICS	Industrial Control System, een controlesysteem om fysieke processen aan te sturen.
ISAC	Information Sharing and Analysis Center: een non-profit organisatie met als doel het verzamelen en delen van dreigingsinformatie.
Kill Chain	Modellering van de hele aanvalsoperatie met alle daaronder vallende stappen.
Red team	Het rode team: een onafhankelijke groep die vanuit het perspectief van een dreiging of aanvaller die met toestemming van de organisatie een aanval simuleert met als doel om de beveiliging van de organisatie te verbeteren. Het red team is de aanvaller in de aanvalssimulatie.
Threat Actor	Binnen een red team kun je verschillende dreigingsactoren simuleren, waaronder APT's.

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

Threat Intelligence (dreigingsinformatie)	Informatie over actuele (gerichte) dreigingen, om het aanvalsscenario's zo realistisch mogelijk te maken.
White team	Het witte team: een groep die verantwoordelijk is voor het overzicht, en optreedt (de-escaleert) als er iets misgaat. Het white team is in staat om crises als gevolg van de oefening maar buiten de scope van de oefening snel op te lossen. In het white team zit iemand van het red team en iemand van het blue team. Het white team is de 'spelleiding' in de aanvalssimulatie.

8 Checklist Red Teaming

8.1 Voorbereiding

Voor je begint aan een red team oefening dien je op de volgende vragen antwoord te kunnen geven.

- ☐ Is een red team oefening op dit moment het meest geschikt voor mijn organisatie?
- ☐ Wat zijn de kroonjuwelen van mijn organisatie?
- ☐ Welke maatregelen heb ik genomen om ze te beschermen?
- ☐ Wat is mijn gewenste eindresultaat van de red team oefening?
- ☐ Welke vorm van red team oefening sluit het beste aan bij mijn doel?
- ☐ Waar moet ik bang voor zijn?
- ☐ Wie heeft het op mij gemunt?
- ☐ Welke aanvalsvormen wil ik uitsluiten?
- ☐ Wat zijn goede potentiële aanvalsscenario's?
- ☐ Wat is mijn budget?
- ☐ Wanneer mag de oefening starten, hoelang mag ze duren, wanneer mag niet geoefend worden?

8.2 Leverancier selectie

Let bij het kiezen van een geschikte leverancier op de volgende zaken:

- ☐ Vraag de aanbieder naar het huidige dreigingsbeeld;
- ☐ Vraag de aanbieder om een voorbeeldrapportage;
- ☐ Vraag de aanbieder welk kader hij gebruikt om de scenario's aan op te hangen;
- ☐ Vraag de aanbieder hoe zij voor realistische scenario's zorgen, of hoe ze daarbij helpen;
- ☐ Vraag de aanbieder naar een generiek scenario;
- ☐ Vraag de aanbieder zijn competentie aan te tonen;
- ☐ Heeft de aanbieder de test en de tijdsduur helder en onderbouwd omschreven?
- ☐ Zijn er afspraken te maken over het omgaan met gevoelige informatie?
- ☐ Zijn prijs en kwaliteit in balans?
- ☐ Nodig de aanbieder uit zijn offerte toe te lichten en vragen te beantwoorden.

8.3 Afspraken maken

Maak de volgende afspraken met de leverancier:

- ☐ Wanneer start de oefening, wat is de doorlooptijd;
- ☐ Juridisch kader voor de oefening en de data: vrijwaringsverklaring, verwerkersovereenkomst, geheimhoudingsverklaring, bewaartermijnen;
- ☐ Hoe worden resultaten gedeeld;
- ☐ Rules of engagement: hoe wordt de oefening uitgevoerd, wat mag wel en niet, hoe vindt de communicatie plaats;
- ☐ Vastleggen van het escalatiepad.

8.4 Uitvoering

Let bij de uitvoering op de volgende zaken:

- ☐ Communicatie via white team;
- ☐ Escalatie als nodig – blue team ontdekt de aanval voortijdig;
- ☐ Leg up – red team heeft hulp nodig bij IN fase;
- ☐ High risk fixen – red team vindt een kwetsbaarheid die directe actie vereist.

8.5 Opvolging

Na de uitvoering start de opvolging met:

- ☐ Kennisoverdracht – verslaglegging / presentatie van het red team;
- ☐ Evaluatie – wat heeft de oefening voor de organisatie opgeleverd;
- ☐ Acties – wat moeten we doen naar aanleiding van de uitkomsten;
- ☐ Opruimen van de sporen van de oefening;
- ☐ Uitdragen – lessons learned delen binnen en buiten de organisatie.