Red teaming als Protective Intelligence Instrument

deel 3

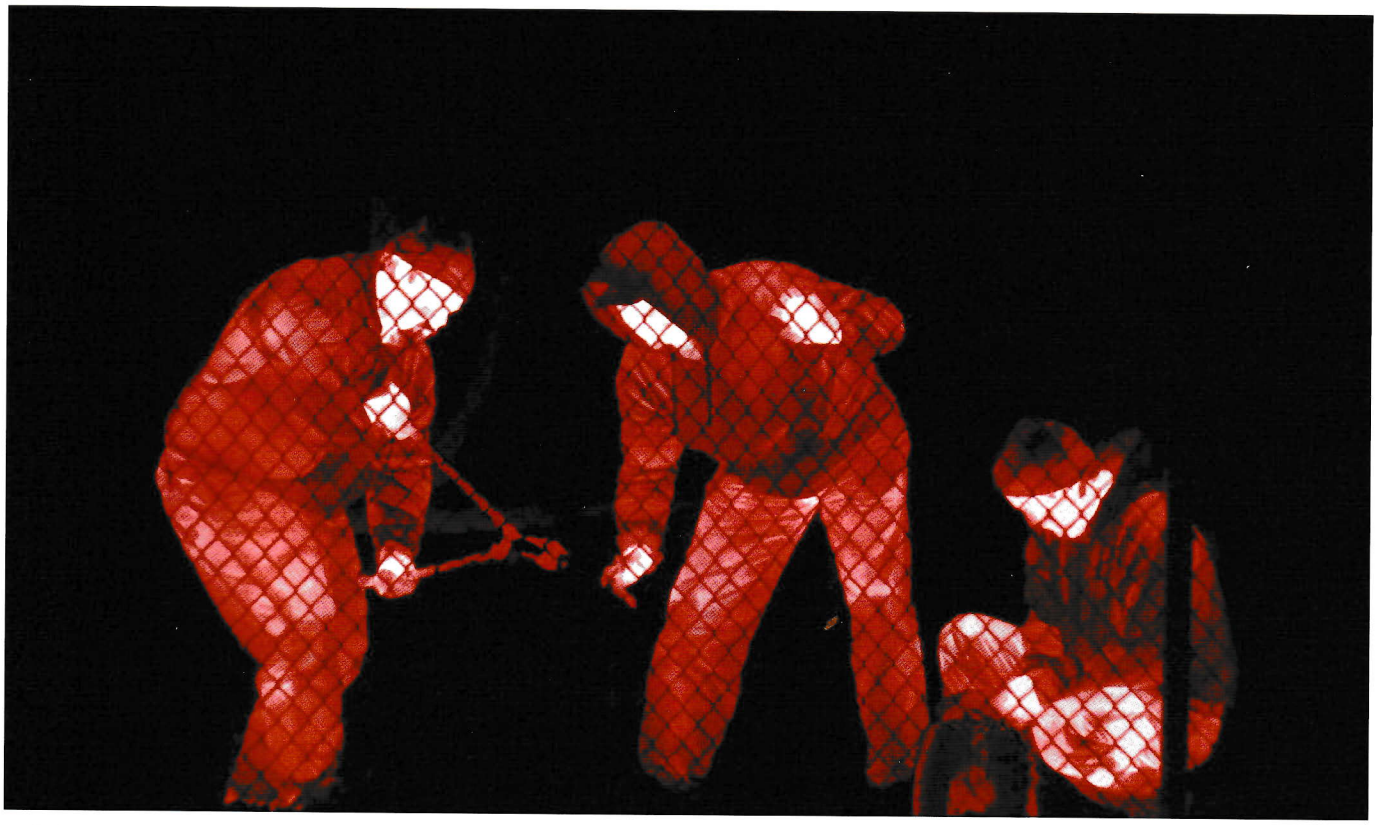
Door regelmatig in de huid van de tegenstander te kruipen kunnen security managers 'intelligence' genereren over de werkwijze van de tegenstander en over de kwetsbaarheid van de eigen organisatie. Dit artikel gaat in op de voorbereiding, uitvoering en randvoorwaarden van red teaming als Protective Intelligence Instrument. Ook wordt kort stilgestaan bij de relatie tussen de proactieve beveiligingscyclus op operationeel niveau, de dreigingsanalyse op tactisch niveau en de risicoanalyse op strategisch niveau.

Red teaming is de eerste stap van de proactieve beveiligingscyclus. De doelstelling van een red teaming-oefening is het identificeren van de werkwijze van de tegenstander, de aanvallersmethode van operatie (AMO), waarmee de te beveiligen organisatie te maken kan krijgen. Nadat de hele proactieve beveiligingscyclus is doorlopen, krijgen wij opnieuw met de stap red teaming te maken. Echter, deze tweede keer komt er nog een doelstelling bij. Het gaat nu niet meer alleen om het ontdekken van 'nieuwe' AMO's, maar ook om het kijken of de eerder ontdekte AMO's, waar security medewerkers op getraind zijn, daadwerkelijk worden ontdekt en conform de standaard operationele procedure (SOP) worden afgehandeld. Er wordt dan ook gekeken of de training van de medewerkers effectief is geweest. Belangrijk bij het uitvoeren van een red teaming-oefening is, zeker voor wat betreft het ontdekken van nieuwe AMO's, dat alle stappen van de criminele planningcyclus worden doorlopen die een contactmoment opleveren: informatie verzamelen, surveillance (observatie), training (dry run) en waar mogelijk ook de uitvoering. Hoe gaat een red team te werk om haar doelstelling te halen?

Informatie verzamelen Het red team zal in eerste instantie relevante informatie moeten verzamelen over de aan te vallen organisatie. Deze is veelal beschikbaar in open bronnen. Het betreft hier informatie over de processen die aangevallen moeten gaan worden (terrorisme) of over processen waar waarde uit onttrokken moet gaan worden (criminaliteit). Het kan dan gaan om fysieke waarde, maar ook om elektronische waarde of informatie. Daarnaast zal het red team zich ook moeten verdiepen in de werkwijze van voorgangers bij eerdere aanslagen, overvallen, diefstallen of spionage-acties. Veel van de activiteiten binnen de stap 'informatie verzamelen' zijn te vangen onder de noemer 'desk research'. Het contactmoment binnen deze stap van de criminele planningcyclus is het moment waarop de verzamelde informatie getoetst moet worden. Het is voor het red team, ter beantwoording van de vraag of zij verder gaan (haalbaarheid) met het aanvallen van het gekozen doel, belangrijk om vast te stellen dat de verzamelde informatie juist is. Het red team moet dus gaan vaststellen, door daadwerkelijk te gaan kijken, of de locatie en omgeving van het doelwit overeenkomen met de informatie die uit open bronnen is verkregen. Tevens zal in dit stadium vastgesteld moeten worden of de processen waar 'de criminele organisatie' zich op gaat richten daadwerkelijk nog zo zijn gepositioneerd als verwacht. Voor wat betreft de uitvoering van de actie zal ook gekeken moeten worden of deze realiseerbaar is met gebruikmaking van eerder bedachte AMO's of dat er inmiddels, gezien de verzamelde informatie, betere en gemakkelijkere AMO's denkbaar zijn.

Observeren (surveillance) In deze fase, waarin de beslissing genomen is daadwerkelijk een bepaalde organisatie te gaan aanvallen, wordt de aandacht door het red team gericht op de (beveiligings)processen die de crimineel moet omzeilen om bij zijn doel uit te komen. De crimineel, in dit geval het red team, zal nu structurele observaties moeten gaan uitvoeren om de relevante processen te doorgronden. Voor het red team is het in deze fase belangrijk (nieuwe) AMO's te vinden waarmee surveillance en observaties het beste uit te voeren zijn. Ook zal nagedacht moeten worden hoe het beste mensen zijn te benaderen voor het stellen van vragen, indien dit nodig zou zijn. In bepaalde situaties ontkomt het red team er niet aan om medewerkers van de organisatie te benaderen om antwoorden op vragen te krijgen die niet door middel van observaties te verkrijgen zijn. Het is dan ook de bedoeling, waar nodig, dat het red team daadwerkelijk contact met de organisatie en haar medewerkers gaat maken. De criminele organisatie doet dit immers ook om de benodigde informatie op tafel te krijgen. Waar in de voorgaande fase, informatie verzamelen, de crimineel - in dit geval het red team - nog geheel niet bekend was met de norm (gedrag) in de directe omgeving van de aan te vallen organisatie, zal het nu al iets gemakkelijker zijn om op te gaan in het normale beeld. Dit zal echter, waar contact gemaakt moet worden, nog wel lastig zijn. Wat het red team immers nog niet weet, is welke vragen normaal zijn om te stellen en welke vragen argwaan zullen opwekken.

Trainen (dry-run) Het derde en laatste contactmoment voor de daadwerkelijke uitvoering van een actie, die



ook door het red team doorlopen moet worden, is het testen van de (beveiligings)maatregelen van de aan te vallen organisatie. Het is belangrijk om, op basis van de (nieuwe) gekozen AMO, te bepalen hoe de organisatie reageert. Het zal ook in deze fase zijn dat de crimineel - het red team - ontdekt dat, afhankelijk van de reactie van de aan te vallen organisatie, het gekozen AMO moet worden bijgesteld of dat het in zijn geheel niet zinvol is om de actie te gaan uitvoeren. In deze fase van de dry-run heeft de organisatie de kans om aan het red team - de crimineel - het signaal af te geven dat zij onderkend zijn. De kans echter dat beveiligingsmedewerkers een nieuwe AMO die getest wordt daadwerkelijk onderkennen is klein. Zij zijn immers nog niet getraind op deze AMO. Vanuit het oogpunt van red teaming prima. Het gaat immers ook om het ontdekken van nieuwe door criminelen te gebruiken werkwijzen, zodat daar gericht op getraind kan worden. Het 'missen' van een nieuw AMO, een AMO die nog niet uitgeleerd is, is geen schande.

Het laten uitvoeren van de verschillende stappen die een red teaming oefening doorloopt, maar zeker de stap waarbinnen een dry-run wordt uitgevoerd door beveiligingsmedewerkers zelf, is essentieel. Immers, de medewerker die zelf heeft ervaren wat het met je doet om onbevoegde handelingen te gaan uitvoeren zal de signalen en gedragingen die daar bij horen, en die vaak niet te verbergen zijn, ook gemakkelijker bij anderen gaan herkennen. Nu kan een beveiligingsmedewerker, omdat hij bekend is, natuurlijk niet bij een red teaming oefening tegen de eigen organisatie worden ingezet. Daarom is het belangrijk om met een aantal partners samen te werken om elkaars organisatie structureel te gaan red teamen. Voorwaarde is wel dat al deze partners, voor wat betreft de implementatie van de pro-actieve beveiligingscyclus, het zelfde niveau hebben.

Uitvoeren Het laatste contactmoment, waarop eventueel interventie nog steeds mogelijk is, betreft 'het begin' van de uitvoering. Dit zal het red team ook moeten meenemen in de oefening. Het red team kan, afhankelijk van de organisatie, ook de opdracht krijgen om daadwerkelijk een diefstal of overval te simuleren. Het spreekt voor zich dat dit om een grondige voorbereiding vraagt waarbij de veiligheid, zowel van het red team alsook van de medewerkers die gewoon bezig zijn met hun werkzaamheden, voorop staat. Dit betekent, omdat medewerkers van de organisatie niet vooraf mogen weten dat er een oefening gaat plaatsvinden, dat er altijd 'safety officers' aanwezig zijn die kunnen ingrijpen. Nu hoor ik u denken, dit kan niet en dit is te gevaarlijk. Een kleine anekdote. In november 2012, in de week dat er vanuit de Gaza strook raketten op Tel Aviv werden afgeschoten, hebben de twee auteurs van dit artikel een red teaming oefening uitgevoerd in Israël. De opdracht was om daadwerkelijk een bom, met alle onderdelen, bij een goed beveiligde locatie naar binnen te smokkelen. De beveiliging, die bewapend was, wist niet dat er een oefening zou gaan plaatsvinden. Alleen de security managers en de safety officers waren van de oefening op de hoogte. De ervaring voor zowel de beveiliging, als het red team dat een missie moet uitvoeren, is enorm. Zeker als er achteraf een gezamenlijke evaluatie plaatsvindt. Het leerpunt van deze oefening was dat, als de noodzakelijke veiligheidsmaatregelen in acht worden genomen, ook de uitvoeringsfase in een red teaming opdracht kan worden meegenomen. Zeker als de gevaarzetting, zoals wij die in Nederland kennen, lager is dan in Israël.

Protective Intelligence Daar waar het vaak lastig is om detailinformatie te krijgen over eerdere incidenten, als deze al bekend zijn want veelal worden deze niet gedeeld, geeft red teaming een prachtig beeld wat tegenstanders kunnen doen als zij de motivatie en de capaciteit hebben om de organisatie aan te vallen. Tevens maakt een goed uitgevoerde red teaming-oefening duidelijk waar de kwetsbaarheden van de organisatie liggen. In die zin is red teaming dus eigenlijk een operationeel ▸

ABONNEREN
Beveiliging
managementblad
voor veiligheidsadviseurs en security professionals
?
BEL VOOR MEER INFORMATIE
ABONNEESERVICE
T: +31 (0) 20 3122073
abonneren@beveiliging.nl

intelligence instrument waarmee de security manager zelf de informatie kan genereren die hij extern moeilijk kan krijgen. Daarmee is de security manager die niet wist dat er iets kon gebeuren, omdat het hem niet door externen waaronder de politie verteld is, verleden tijd. De security manager die met een AMO wordt geconfronteerd die hij nog niet kende, of die merkt dat beveiligingsmaatregelen tegen bekende AMO's niet werken, omdat hij geen red teaming oefeningen organiseert, heeft zijn werk dan gewoon niet goed gedaan. De security manager 'nieuwe stijl', die wel voortdurend bezig is met het kijken naar AMO's en de weerstand van de organisatie hiertegen, maakt de dreigingen op voorhand bekend bij het management van de organisatie. Als het management aangeeft dat dreigingen niet hoeven te worden gemitigeerd, en de daaraan verbonden risico's accepteert, is zij ook meteen probleemeigenaar. Daar waar dreigingen manifest worden, en het risico geaccepteerd wordt, valt de security manager niets te verwijten. Ook het niet hebben van voldoende budget is geen probleem meer van de security manager, dit is immers ook risicoacceptatie door het management, omdat er niet afdoende maatregelen tegen dreigingen zijn genomen. Wat de security manager nog wel is aan te rekenen, is het niet onderkennen van nieuwe AMO's of het niet signaleren dat beveiligingsmaatregelen tegen onderkende AMO's niet effectief zijn. Red teaming is in feite niets anders dan een in de Amerikaanse literatuur beschreven 'vulnerability assessment'. Met dit verschil dat het beschreven assessment veelal een literatuur- en documentenonderzoek is, terwijl een red team daadwerkelijk in de praktijk op zoek gaat naar de kwetsbaarheden.

Dreigingsanalyse De proactieve beveiligingscyclus, waarvan red teaming de eerste stap is, is een proces op operationeel niveau. Er is echter ook een relatie met de dreigingsanalyse die op tactisch niveau binnen de organisatie is uitgevoerd en de risicoanalyse van de organisatie die op strategisch niveau is vastgesteld. De dadergroepen die in de vastgestelde risicoanalyse zijn geïdentificeerd, en waarvan de organisatie niet accepteert dat zij succesvol de belangen van de organisatie mogen aantasten, zijn het beginpunt van red teaming. De resultaten van een red teaming oefening hebben in eerste instantie tot doel de vervolgstappen binnen de proactieve beveiligingscyclus mogelijk te maken en vast te stellen op welke wijze de in de risicoanalyse geïdentificeerde dadergroepen hun doel kunnen bereiken. In die zin is red teaming wat in de Verenigde Staten ook wel een 'vulnerability assessment' wordt genoemd. Dit blijkt uit het feit dat de resultaten ook gebruikt worden binnen de dreigingsanalyse als blijkt dat de organisatie onbekende of onwenselijke kwetsbaarheden heeft. De dreigingsanalyse op tactisch niveau, die naast de input vanuit de red teaming oefening ook tot doel heeft eventuele nieuwe dadergroepen te identificeren, dient vervolgens weer als input voor de risicoanalyse. Aan het einde van deze serie over de proactieve beveiligingscyclus zal in een apart artikel worden stilgestaan bij de positionering van de proactieve beveiligingscyclus op operationeel niveau ten opzichte van de strategische risicoanalyse en de tactische dreigingsanalyse.

Theorie en praktijk Wanneer red teaming wordt uitgevoerd, zoals dit binnen de methodiek oorspronkelijk is bedoeld, dan wordt het red team tijdens een live oefening niet ingeperkt. In de praktijk krijgt het red team vaak wel kaders mee. Wanneer aan het red team kaders worden meegegeven - en het team beperkt is in hetgeen mag worden uitgevoerd - loopt de organisatie het risico AMO's en hieraan verbonden verdachte indicatoren te missen. Tegenstanders hebben immers ook geen kader waaraan zij zich hebben te houden. Zij zijn creatief en het red team moet dat ook kunnen en mogen zijn. Een belangrijke randvoorwaarde voor een red teaming oefening is dat er sprake moet zijn van een veilige omgeving. Dit betekent dat er een safety officer toezicht moet houden op de uitvoering van de oefening en die, waar nodig, kan ingrijpen. Ook zal voor het red team duidelijk moeten zijn welke stap uit de planningscyclus in de oefening wordt uitgewerkt. Het is gebruikelijk dat, gezien de verstoring die dit teweeg brengt en ook vanwege de gevaarzetting, de uitvoeringsfase - de diefstal, de overval of de aanslag - slechts in zeer uitzonderlijke gevallen onderdeel is van een red teaming-oefening. Dit is op zich niet erg. Immers, proactieve beveiliging is er juist op gericht dat de tegenstander de uitvoeringsfase niet bereikt vanwege het feit dat hij al in de voorbereiding wordt onderkend. In de vervolgstappen van de proactieve beveiligingscyclus, het onderkennen van AMO's en verdachte indicatoren, komt ook naar voren hoe belangrijk de evaluatie van een red teaming-oefening is. In het volgende artikel van de proactieve beveiligingscyclus wordt ingegaan op de vraag hoe de resultaten van red teaming worden verwerkt tot bruikbare AMO's waar de organisatie mee kan gaan werken om de weerbaarheid te vergroten.

■ Berndt Rif MSc MBA MSec, Berndt.Rif@beveiliging.nl
Marie-Louise Ruijs BBA,
MarieLouise.Ruijs@promundo.nl