

De criminele en terroristische planningscyclus

Als niet bekend is hoe tegenstanders te werk gaan en welke aanvalsmethode (AMO) zij gebruiken, dan is het lastig, zo niet onmogelijk om signalen die wijzen op de voorbereiding van een aanval waar te nemen en te mitigeren. Dit artikel gaat in op de acht stappen van de cyclus die criminelen, terroristen en ook inlichtingendiensten doorlopen.

Een voorwaarde voor proactief beveiligen is kennis van en over de tegenstander. Als niet bekend is hoe de tegenstander te werk gaat en welke aanvalsmethode er wordt gebruikt, ook wel de aanvalsmethode van operatie (AMO) genoemd, is het lastig, zo niet onmogelijk om een aanval waar te nemen en te mitigeren. Voorkomen is in een dergelijk geval al helemaal geen optie, omdat wij onze medewerkers niet kunnen vertellen waar zij op moeten letten. In een dergelijke situatie zal het eerste wat wij waarnemen de klap zijn waarmee onze tegenstander zich onbevoegd een weg naar binnen verschaft. Recente incidenten hebben laten zien dat als de tegenstander besluit om onze organisatie aan te vallen, en weet wat de beveiligingsmaatregelen zijn, de uitvoering veelal succesvol is. Zelfs de politie heeft op dit moment vaak, als de uitvoering van een aanval eenmaal begonnen is, het nakijken. Reden genoeg om in te gaan op de acht stappen van de cyclus die criminelen, terroristen en ook inlichtingendiensten doorlopen bij het 'onbevoegd menselijk handelen', zoals de Haagse Methodiek dat zo mooi noemt.

Acht stappen De criminele en terroristische planningscyclus, ook wel criminele en terroristische aanvalscyclus genoemd, bestaat uit acht stappen. Bij het bespreken van de stappen is de vraag voor de security manager of en zo ja welke stappen, vanwege een contactmoment, kunnen worden waargenomen? Een positief antwoord betekent immers dat wij beveiligingsmedewer-

kers kunnen trainen in het herkennen van indicatoren die gekoppeld zijn aan de werkwijze van onze tegenstander (AMO) en aan een specifieke stap van de planningscyclus. Het mag duidelijk zijn dat hoe eerder een mogelijke aanval wordt waargenomen, liefst in de voorbereidingsfase, hoe groter de ruimte is om deze succesvol te mitigeren.

Stap 1: Markeren van het doel

Onze tegenstanders zullen, buiten ons blikveld, de beslissing nemen om een onbevoegde handeling te gaan uitvoeren. Voor dit artikel gaan we uit van de wil van professionele criminelen om een overval te plegen. De eerste vraag die dan beantwoord moet worden door de crimineel is: welke organisatie kies ik als doelwit? Er zullen bij het beantwoorden van deze vraag een aantal opties de revue passeren. De kans is groot dat open bronnen en internet gebruikt worden om tot een shortlist te komen. Google Earth is bovendien onmisbaar als bron om de locatie te bepalen die de grootste kans met zich meebrengt om na de overval ook succesvol te kunnen vluchten. Immers, alleen de zelfmoordterrorist heeft er geen belang bij om ongeschonden het plaats delict te verlaten. De crimineel wil echter, om ook van de buit te genieten, weg komen. Deze eerste stap, waar onze tegenstander tot een keuze van het doelwit komt, kunnen wij niet waarnemen.

Stap 2: Informatie verzamelen

Zodra duidelijk is welke organisatie de crimineel wil overvallen zal er ook informatie moeten worden ingewonnen. Het moet immers duidelijk zijn, wil de

overval met succes kunnen plaatsvinden, hoe de situatie er ter plekke uitziet. Vragen die de crimineel in dit stadium wil beantwoorden hebben veelal te maken met: hoe kan ik het object benaderen, waar bevindt zich de te verkrijgen waarde of te stelen informatie, welke beveiligingsmaatregelen kom ik tegen en hoe kan ik na de actie vluchten? Om antwoorden op deze vragen te krijgen, zal de crimineel informatie nodig hebben. Hij verkrijgt deze informatie door middel van social engineering, door gebruik te maken van social media, open bronnen en door naar de te overvallen organisatie toe te gaan. Het bezoek van de crimineel is dan ook meteen het eerste contactmoment dat wij kunnen waarnemen. Omdat de crimineel nog niet bekend is met de gedragsnorm van onze organisatie en van de directe omgeving van onze organisatie is de kans groot dat hij zich afwijkend zal gedragen ten opzichte van deze norm. Voor onze beveiligingsmedewerkers, tenminste als zij getraind zijn in het herkennen van de afwijking van de norm in relatie tot de werkwijze van de tegenstander (AMO), geeft deze stap de grootste kans op ontdekking. Zeker als de crimineel medewerkers gaat benaderen om vragen te stellen.

Stap 3: Surveillance

Nadat de crimineel de basisinformatie in zijn bezit heeft, gaat hij zich verder toespitsen op het gedetailleerd in kaart brengen van beveiligingsmaatregelen en -procedures. Ook inzicht in de afloop van specifieke bedrijfsprocessen is noodzakelijk voor de crimineel, wil de overval met succes kunnen plaatsvinden. De derde stap van de cyclus is dan ook surveillance, ook wel gerichte observatie genoemd. Surveillance op locatie heeft tot doel om aanvullende informatie te verzamelen, welke niet verkrijgbaar is gebleken via eerder gebruikte bronnen of om bevestiging te vinden voor eerder verkregen informatie. De crimineel zal voor kortere of langere tijd onze organisatie goed in de gaten houden. Ook deze stap van de criminele en terroristische planningscy-

deel 2

clus is voor goed getrainde beveiligingsmedewerkers waar te nemen. De crimineel zal, als hij de organisatie gadeslaat, vroeg of laat fouten maken. Bij sommige objecten is het niet gebruikelijk dat er voor langere tijd auto's geparkeerd staan waar mensen in zitten, bij andere organisaties lopen mensen in de ochtend in een ander tempo langs dan in de middag. Wij als beveiligingsprofessionals kennen de norm van onze omgeving, en die norm kan per dag en per tijdstip, verschillend zijn. Onze tegenstander is niet of minder bekend met de norm en zal, hoe klein de afwijking soms ook is, signalen afgeven. Het is dan aan de door de security manager getrainde medewerkers om die afwijkingen van de norm, in relatie tot de geleerde modus operandi waar te nemen.

Stap 4 en 5: Planning en verkrijgen middelen

Na het verzamelen van informatie en het uitvoeren van de surveillance zal de crimineel zijn daadwerkelijke actie gaan uitwerken. Dit doet hij op een voor ons niet waar te nemen locatie. Het maken van plannen en het nadenken over de benodigde middelen, wat de vierde stap in de cyclus is, kan de security professional niet waarnemen. Nadat de plannen zijn gemaakt, en het criminele draaiboek het licht heeft gezien, zal de crimineel of terrorist zich de materialen gaan verschaffen om het idee tot uitvoering te brengen. Dit is de vijfde stap van de cyclus. De organisatie die als doelwit is uitgekozen, en vanuit dat perspectief benaderen wij de cyclus, kan dit niet waarnemen. In sommige gevallen kan het aanschaffen van middelen wel door anderen worden

waargenomen, maar die zullen er veelal niet op aanslaan. Tenzij iemand ineens hele grote hoeveelheden kunstmest gaat kopen. Dan is de kans wel aanwezig dat er alarm wordt geslagen bij de overheid. Iets waarop security professionals echter niet kunnen en mogen vertrouwen.

Stap 6: Oefening en training

De criminele organisatie die een professionele overval wil uitvoeren zal haar actie niet van toeval laten afhangen. Zij zal, net zoals dat bij de overheidsdiensten die ons bij een incident te hulp schieten gebruikelijk is, gaan trainen. Onderdeel van deze training is ook de zogenaamde dry-run. Dit is een oefening op locatie waarbij gekeken wordt of een uitgedachte werkwijze (AMO) succesvol kan zijn. Doelstelling van de dry-run is het kijken hoe de organisatie die wordt aangevallen reageert op afwijkingen. Afhankelijk van de reacties kunnen de plannen dan door de criminele organisatie worden bijgesteld en verbeterd. Deze stap in de criminele en terroristische planningscyclus is waarneembaar. Zeker als wij ons realiseren dat incidenten die zich voordoen, zoals bijvoorbeeld een inbraakalarm dat afgaat of een achtergelaten tas, een test kunnen zijn om te bepalen hoe onze beveiligingsprocedures in de praktijk worden toegepast. Dit maakt het niet reageren op een alarm of een waargenomen normafwijking, vanuit het oogpunt 'het zal toch wel weer niets zijn', erg gevaarlijk. De kans dat het begin van een daadwerkelijke uitvoering dan wordt waargenomen is dan ook erg klein. Een crimineel die dit ontdekt zal zijn geplande aanval zeker doorzetten.

Stap 7 en 8: Uitvoering en vlucht

En toen was er de klap. Op de vraag aan de security manager of hij dit niet heeft

zien aankomen is het antwoord vaak negatief. Op zich logisch. Want als beveiligingsmedewerkers niet getraind zijn om afwijkingen van de norm te herkennen die horen bij de fasen informatie verzamelen, surveillance of een dry-run, zullen zij het zeker niet zien. Een gemiste kans. Zeker als wij de incidenten van de laatste tijd evalueren. Als professionele criminelen aan de uitvoering beginnen, de zevende stap in de cyclus, slaagt de actie in bijna alle gevallen. Onze tegenstander weet immers precies wat hij tegenkomt en hij is daar ook goed op voorbereid. De laatste en achtste stap, de vlucht, zal dan hoogst waarschijnlijk ook succesvol zijn. Als wij pas tijdens het begin van de uitvoering waarnemen dat er iets gaande is, en dan gaan alarmeren, weet de crimineel exact hoeveel tijd er is voordat de politie ter plaatse komt. Op dit moment zien wij ook dat de crimineel op voorhand rekening houdt met het feit dat een confrontatie met de politie onderdeel van het draaiboek is. De hedendaagse crimineel, met een automatisch vuurwapen, is geen partij meer voor de politieagent op straat.

Hoe nu verder? Het waarnemen van de stappen informatie verzamelen, surveillance en de dry-run geeft ons als security professionals de kans tijdig mitigerende maatregelen te nemen om een eventuele dreiging af te wenden. Zeker als wij aan onze tegenstander laten merken dat hij gezien is. Waarschijnlijk zal de crimineel of terrorist nog wel verder gaan met zijn plan om een overval uit te voeren, maar niet bij onze organisatie. De kans op vroegtijdige ontdekking is dan te groot. In het volgende artikel zal de eerste stap van de proactieve beveiligingscyclus worden uitgewerkt. Doelstelling van de proactieve manier van beveiligen is het waarnemen van dreigingen in een vroegtijdig stadium zodat mitigatie nog mogelijk is. Liefst het al waarnemen van de dreiging in de fase van informatie verzamelen en surveillance, maar in ieder geval als er sprake is van een dry-run. De security professional wil een overval voorkomen en dat kan nog als de crimineel al in de voorbereidende fase wordt waargenomen. De klassieke beveiliging, die zich richt op *target hardening* en alarmering op het moment dat er zich een incident voordoet, is niet meer van deze tijd.

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

