deel 7

Implementatie SOP en training medewerkers

Na het vaststellen van de Aanvallers Methode van Operatie (AMO) en de verdachte indicatoren die waarneembaar zijn, wordt in de proactieve beveiligingscyclus de Standaard Operationele Procedure (SOP) opgesteld. Deze moet worden geïmplementeerd en vervolgens is het noodzakelijk de medewerkers regelmatig te trainen. Pas dan is de cyclus in zijn geheel doorlopen.

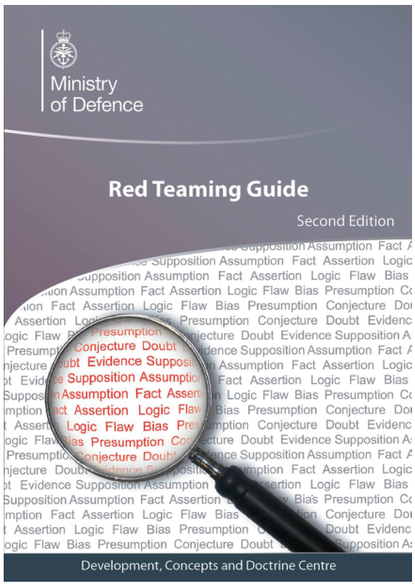
In het verleden was het gebruikelijk om, tot op het niveau 'adem in, adem uit want anders valt u om', instructies op te schrijven die beveiligingsmedewerkers zonder zelf na te denken moesten uitvoeren. De SOP die bij de proactieve beveiligingscyclus gebruikt wordt gaat echter uit van 'de denkende mens'. Dit is een beveiliger die zelf moet nadenken met als doel het manifest worden van dreigingen te voorkomen. Als een incident zich heeft voorgedaan, en de beveiliger is bezig met incidentmanagement, dan heeft beveiliging gezien vanuit de proactieve benadering eigenlijk gefaald. Uitgangspunt was immers het voorkomen van het manifest worden van dreigingen. Het proactief werken brengt ook met zich mee dat er constante training van beveiligers moet plaatsvinden. De uitgangspunten dienen duidelijk te zijn, maar ook de vaardigheden moeten aanwezig zijn om verdachte indicatoren daadwerkelijk te kunnen verklaren en dreigingen te ontkrachten. Dit vraagt, los van de training die als laatste plaatsvindt, ook om de beschikbaarheid van middelen. Middelen waarmee de beveiligingsmedewerker verdachte indicatoren kan waarnemen en middelen waarmee verdachte indicatoren kunnen worden ontkracht. Ook zal nagedacht moeten worden over de vraag hoe beveiligers ingezet moeten worden. Juist deze randvoorwaarden, inzet en middelen dienen bij de stap 'implementatie SOP' te worden ingevuld.

Management-summary

Tijdens de eerste stap van de proactieve beveiligingscyclus hebben wij kennisgemaakt met red teaming. Vervolgens zijn de Aanvallers Methode van Operatie (AMO) en de verdachte indicatoren die waarneembaar zijn geïdentificeerd. Daarna, in de vierde stap, is de SOP opgesteld. In de SOP staat beschreven hoe de security profiler te werk moet gaan, de wijze waarop een dreigingassessment dient plaats te vinden, alsook de manier waarop een toe te kennen classificatie gegeven moet worden en welke mitigerende (beveiligings) maatregelen noodzakelijk zijn als verdachte indicatoren niet verklaarbaar zijn. Bij niet verklaarde verdachte indicatoren kan een dreiging immers niet ontkracht worden. Nu zal, nadat alles op schrift is gesteld, de SOP ook geïmplementeerd moeten worden (stap vijf) en vervolgens is de training van de medewerkers noodzakelijk (stap zes). Pas dan is de cyclus in zijn geheel doorlopen en kan er, met een red teaming oefening, weer opnieuw worden begonnen.

Inzet van beveiligers Bij de implementatie van de SOP is een belangrijke vraag wat de onderkende Aanvallers Methode van Operatie voor een bepaalde risicopositie zijn. De beveiliger - security profiler - wordt immers ingezet om dreigingen in een vroegtijdig stadium te onderkennen zodat hij of zij deze vervolgens probeert te ontkrachten of te mitigeren. Dit betekent dat de security profiler naar buiten moet treden en proactief contact zoekt met onbekende personen die een aan een Aanvallers Methode van Operatie te koppelen verdachte indicator laten zien. De reactie van een dergelijke persoon op het moment dat hij of zij wordt aangesproken, en ook de reactie van eventuele handlangers in de directe omgeving op dit aanspreken, kunnen niet door één beveiliger worden waargenomen. Bovendien brengt proactief contact leggen, natuurlijk sterk afhankelijk van de onderkende Aanvallers Methode van Operatie, ook een veiligheidsrisico met zich mee. Proactief beveiligen wordt daarom altijd door minimaal twee beveiligers uitgevoerd. Tevens is het van belang om ▸





na te denken over de wenselijkheid van de combinatie geüniformeerde beveiliger en beveiliger in burger. Kwaadwillenden kunnen sneller door beveiligers in burger worden waargenomen dan door beveiligers in uniform. Dit komt omdat de beveiliger in burger van buiten naar binnen kijkt, zonder dat kwaadwillenden hem waarnemen, en de beveiliger in uniform kijkt van binnen naar buiten. Dat geeft een heel ander plaatje. Bovendien kan een beveiliger in burger, die niet wordt waargenomen, zien of mensen hun gedrag veranderen als er een beveiliger in uniform langsloopt. Ook dat kan een indicatie zijn.

Waarnemen en ontkrachten Om te kunnen waarnemen zijn, ook weer sterk afhankelijk van de onderkende Aanvallers Methode van Operatie, middelen nodig om de security profiler te ondersteunen. Dit kunnen detectiepoortjes, x-raymachines of camerasystemen zijn (niet limitatief). Een cameraobservant kan de functie van een beveiliger in burger ook overnemen en kijken, als de geüniformeerde beveiliger rondloopt of mensen aanspreekt, wat er gebeurt. Zowel met de persoon die wordt aangesproken alsook in de directe omgeving. Bovendien kunnen bepaalde technische middelen ook gebruikt worden om dreigingen te ontkrachten op het moment dat er voor verdachte indicatoren geen verklaring gevonden kan worden. Denk daarbij bijvoorbeeld aan de inzet van detectiepoortjes in gevangenissen. Enerzijds worden deze gebruikt om niet wenselijke voorwerpen te vinden. Anderzijds kunnen detectiepoortjes op locaties waar het niet wenselijk is om iedereen er door heen te laten lopen ook worden ingezet om alleen die personen aan de controle te onderwerpen die onverklaarbare indicatoren laten zien. Vanuit een ‘worst-case-scenario’ is er dan immers sprake van een dreiging. Als wij ‘vuurwapens’ als dreiging hebben geïdentificeerd, dan weten wij van de persoon die door het detectiepoortje loopt zonder dat deze een signaal afgeeft in ieder geval zeker dat hij of zij geen vuurwapen bij zich heeft dat voor direct gebruik geschikt is.

Uitgangspunten concept Nadat duidelijk is hoe de inzet van de beveiligers gaat plaatsvinden, en welke middelen er noodzakelijk zijn, komen wij bij de laatste stap van de proactieve beveiligingscyclus: de training van medewerkers. In eerste instantie zal de theorie moeten worden overgebracht. Een security profiler kan het werk niet doen als hij of zij de Aanvallers Methode van Operatie en de daaraan gekoppelde verdachte indicatoren niet paraat heeft. Immers, een security profiler die niet weet welke verdachte indicator hij wil verklaren en welke Aanvallers Methode van Operatie er ontkracht moet worden kan nooit de juiste vragen aan de persoon stellen waar hij mee in gesprek gaat. Ook het stellen van vragen - security questioning - is een vak dat geleerd moet worden. Daarnaast zal de security profiler ook exact moeten weten wanneer hij welke classificatie moet geven en wat de aan de classificatie verbonden beveiligingsmaatregelen zijn om de niet ontkrachte dreiging weg te nemen of te verminderen. Naast de benodigde theorie zal er ook veel in de praktijk geoefend moeten worden. Zowel met het leren van de te stellen vragen bij bepaalde indicatoren alsook het doorlopen van de ‘drills’ waarbij de juiste beveiligingsmaatregelen worden getroffen bij niet ontkrachte dreigingen. Een security profiler kan, juist gezien de noodzakelijke training, pas zelfstandig worden ingezet als hij of zij bij een red teaming oefening na afloop of aan het einde van de training heeft laten zien verdachte indicatoren waar te kunnen nemen, de juiste vragen te kunnen stellen om deze te verklaren en ook bij niet ontkrachte dreigingen de juiste mitigerende maatregelen te kunnen treffen.

Uitdagen medewerkers De security profiler kan zijn werk alleen goed blijven doen als hij of zij voortdurend wordt uitgedaagd en geprikkeld. Enerzijds gebeurt dit vanwege het feit dat er voortdurend red teaming plaatsvindt omdat de cyclus steeds opnieuw doorlopen wordt. Daarnaast heeft ook de directe supervisor een belangrijke rol omdat hij of zij regelmatig aan de security profiler dient te vragen welke indicator er verklaard moest worden en aan welke Aanvallers Methode van Operatie de indicator verbonden was. Bovendien kan de supervisor tijdens de reguliere dienst ook zelf op kleine schaal oefeningen initiëren. Dit kan heel simpel door bezoekers te vragen ID-bewijzen om te wisselen of om aan bezoekers te vragen zich op een bepaalde ‘verdachte’ manier te gedragen. Ook kan er een object worden neergezet om te kijken hoe er op achtergelaten voorwerpen wordt gereageerd. Gaat de security profiler meteen escaleren of, ter ontkrachting van een dreiging, eerst kijken wat er op camerabeelden te zien is. Wellicht dat daar uit blijkt dat er een logische verklaring is. De dagelijkse debriefing is dan een uitstekend moment om de oefeningen te evalueren. De supervisor zal vervolgens ook minstens een keer per halfjaar, liefst een keer per kwartaal, moeten toetsen of de security profiler de geïdentificeerde Aanvallers Methode van Operatie met daaraan gekoppelde verdachte indicatoren nog paraat heeft.

Dreiging en risico Bij het beschrijven van de stappen van de proactieve beveiligingscyclus zijn de woorden dreiging en risico regelmatig gevallen. In de praktijk lijken deze woorden vaak door elkaar heen te lopen. Ook de woorden risicoanalyse, dreigingsanalyse en dreigingassessment lijken aan inflatie onderhevig. In het volgende en laatste artikel van de serie proactieve beveiligingscyclus zullen dreiging en risico worden gepositioneerd. Deze positionering zal dan plaatsvinden vanuit het Israëlische gezichtspunt omdat het concept, zoals deze in de serie beschreven is, uit Israël komt. Proactieve beveiliging gaat er vanuit dat een dreiging ‘0’ of ‘1’ is, een dreiging is er of is er niet, net zoals je niet een beetje zwanger kunt zijn. Zodra er sprake is van ‘hoog’, ‘laag’ of ‘0,78’ wordt er gewerkt vanuit de risicobenadering. Dit is een ander concept. De praktijk laat zien dat deze twee concepten, dreigingbenadering en risicobenadering, elkaar niet uitsluiten. Sterker nog, zij vullen elkaar aan als er bewust gebruik van gemaakt wordt en beide goed gepositioneerd zijn.

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