De Standaard Operationele

deel 6

In de Standaard Operationele Procedure (SOP) komt de kennis over de tegenstander, de Aanvallers Methode van Operatie (AMO) en de daaraan verbonden verdachte indicatoren die waarneembaar zijn, samen met de beschrijving hoe de security profiler te werk moet gaan. De SOP beschrijft zowel 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. Immers, als er geen verklaring voor verdachte indicatoren gevonden wordt kan de dreiging, het AMO waar de indicatoren aan verbonden zijn, niet ontkracht worden. Een SOP gaat uit van 'de denkende mens' en is geen klassieke instructie voor de beveiliger op het niveau 'adem in, adem uit, want anders val je om'.

Bij het opstellen van een SOP is het belangrijk dat het eindresultaat, de procedure waarmee de security profiler moet gaan werken, past in de cultuur van de organisatie. Er is daarom geen vast voorgeschreven format. Wel is er een aantal minimumeisen waaraan een SOP moet voldoen. Uitgaande van 'de denkende mens' is het voor de security profiler van essentieel belang om te weten waarom hij op een bepaalde risicopositie werkzaam is. Niet, zoals in de klassieke beveiliging gebruikelijk was, om een deur te openen of te sluiten voor bezoekers. Bij proactieve beveiliging wordt de security profiler ingezet om een dreiging die voor een specifieke risicopositie onderkend is, door middel van red teaming, tijdig te onderkennen en vervolgens te mitigeren.
Dit vraagt om een andere dan de vroegere klassieke benadering. Als bij de opbouw van een SOP rekening wordt gehouden met de in dit artikel beschreven aandachtspunten dan voldoet de SOP ook meteen aan de eindtermen van het praktijkdiploma zoals die door de European Security Intelligence Foundation (ESIF) zijn opgesteld. Een kandidaat die het theorie- en praktijkdiploma predictive profiling van ESIF in zijn bezit heeft kan, als hij van onbesproken gedrag is en ook nog aan een aantal aanvullende eisen voldoet, ingeschreven worden als Certified Security Profiler (CSP) in het register bij de Stichting N'Lloyd. De CSP is niet de uitvoerende security profiler op operationeel niveau, maar de professional op tactisch niveau die de proactieve beveiligingscyclus weet te doorgronden en in zijn geheel binnen een organisatie kan implementeren.

Doelstelling Om zijn werk te kunnen uitvoeren moet de security profiler weten waarom hij op een bepaalde risicopositie werkzaam is. Iedere risicopositie - hoofdentree, expeditie, buitenterrein, cameraobservatieruimte - heeft een eigen SOP. Om de security profiler voldoende houvast te geven, zodat hij zijn werk naar behoren kan uitvoeren, is aan het begin van de SOP altijd een primaire- en secundaire doelstelling opgenomen. De eis is, als uitgegaan wordt van de exameneisen van ESIF, dat de doelstelling beschreven wordt in een volzin. De primaire doelstelling voor een beveiligingsmedewerker bij een warenhuis kan dan bijvoorbeeld beginnen met de woorden 'het voorkomen van diefstal van goederen' en de secundaire doelstelling met 'het voorkomen van agressie tegen medewerkers'. Als, en daar ligt de link met de cultuur van een organisatie, de veiligheid van medewerkers het belangrijkste is, dan heeft dit invloed op de omschrijving van de primaire en secundaire doelstelling.

AMO Voor een security profiler moet duidelijk zijn, op de locatie waar hij zijn werkzaamheden verricht, wat de voor die betreffende risicopositie onderkende Aanvallers Methodes van Operatie (AMO) zijn. Alleen als de security profiler weet met welk AMO hij te maken kan krijgen op een bepaalde risicopositie kan er door hem een gericht dreigingassessment worden gemaakt. Per risicopositie worden in een SOP minimaal vier en maximaal zes AMO's beschreven. Het is ook bij het opstellen van de AMO's van belang dat alle stappen van de criminele planningcyclus die een contactmoment opleveren afgedekt worden. Ook een AMO wordt meestal opgeschreven als volzin waarbij tussen haakjes staat op welke stap van de criminele planningcyclus de AMO betrekking heeft. Voor de security profiler die op operationeel niveau werkzaam is dient de beschrijving voldoende helder te zijn. Het AMO, de dreiging, is immers de reden waarom de security profiler op de betreffende risicopositie wordt ingezet.

Verantwoordelijkheid In het SOP zal ook duidelijkheid gegeven moeten worden voor wat betreft de verantwoordelijkheid die de security profiler heeft. Uit de beschrijving van verantwoordelijkheden moet blijken dat de security profiler de persoon is die een dreigingassessment dient uit te voeren, een

Procedure



classifcatie moet bepalen en bij een niet ontkrachte dreiging het juiste afhandelingsprotocol moet opstarten. Belangrijk is dat wordt vastgelegd dat supervisors of managers, aan wie de security profiler verantwoording moet afleggen, een gegeven classificatie nooit kunnen verlagen. De security profiler heeft immers iets waargenomen, en dat mag nooit gebagatelliseerd worden. Een classificatie kan wel verhoogd worden. Het kan namelijk gebeuren dat een persoon, waar een dreiging van uit kan gaan, pas verdachte indicatoren laat zien als hij dichter bij zijn doelwit komt. Uitgangspunt bij al het handelen, en dat moet ook vastgelegd worden in een SOP, is 'worst case' scenario's.

Dreigingassessment De SOP zal duidelijkheid moeten geven over de vraag op welke wijze een dreigingassessment uitgevoerd dient te worden. Een veel gebruikte zinsnede is dat de security profiler actief 'zoekt naar verdachte indicatoren bij personen, goederen en voertuigen die zich in de directe omgeving van een organisatie bevinden en/of ophouden (zichtlijn)'. Daarbij is het van belang dat aangegeven wordt dat de security profiler verdachte indicatoren zoekt 'op het vlak van de identiteit van personen, de reden van aanwezigheid, gebruikte identificatiemethoden (paspoort, rijbewijs), houding, gedrag, kleding, meegevoerde goederen en materialen (tassen, bagage)'. In het SOP zal ook moeten worden aangegeven dat de security profiler gevonden verdachte indicatoren moet proberen te ontkrachten (het vinden van een goede verklaring) en/of aanvullende verdachte indicatoren te vinden door middel van 'security questionning', vragen naar ID en/of (aanvullende) documentatie en het uitdelen van extra prikkels door middel van de zichtbare aanwezigheid van beveiliging. Het gaat niet om het bewijzen dat er sprake is van een dreiging. Doelstelling is immers zo snel mogelijk een dreiging te ontkrachten zodat de aandacht weer op de omgeving gevestigd kan worden.

Classificatie Naar aanleiding van gevonden verdachte indicatoren en gestelde vragen zal door de security profiler een classificatie gegeven moeten worden. In de meest simpele vorm is dat 'dreiging' of 'geen dreiging'. Er wordt ook wel eens door organisaties met het toekennen van nummers gewerkt waarbij er een classificatie is voor 'geen verdachte indicatoren', 'ontkrachte indicatoren' en 'niet ontkrachte indicatoren'. Bij objecten met een hoog risico komt wel eens voor dat er nog een speciale classificatie is die aan personen wordt toegekend die naar speciale gebieden toe gaan. Het toekennen van een classificatie is belangrijk omdat de classificatie bepaalt welk controleniveau noodzakelijk is. Als een passagier op de luchthaven Ben Gurion in Israël een lage classificatie krijgt, dan komt hij of zij redelijk gemakkelijk door de veiligheidscontrole heen. Een hoge classificatie zal vaak de inzet van meer techniek tot gevolg hebben, zoals speciale x-ray machines en sniffers, om uit te sluiten dat de passagier gevaarlijke goederen bij zich heeft. In sommige gevallen zal er wellicht op de stoel in het vliegtuig, naast de passagier met een hoge classificatie, een air marshall worden neergezet. Immers, een hoge classificatie wil zeggen dat er geen verklaring ▸

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



voor verdachte indicatoren gevonden is met als gevolg een niet ontkrachte dreiging. In de SOP dienen alle classificaties en uit te voeren controles uitgeschreven te staan.

Verdachte indicatoren Een mogelijk AMO kan in een vroegtijdig stadium worden onderkend aan de hand van verdachte indicatoren. De door de security profiler te gebruiken indicatoren dienen in de SOP te worden opgeschreven. Idealiter staan de verdachte indicatoren per AMO beschreven. Het is daarbij heel goed mogelijk dat bepaalde verdachte indicatoren bij meerdere AMO's voorkomen. In de praktijk blijkt het voor security profilers lastig om met heel veel verdachte indicatoren te moeten werken. Het is daarom van belang om indicatoren enigszins abstract op te schrijven om zodoende het aantal te beperken. Een totaal van tussen de vijftien en 25 verdachte indicatoren, voor zes AMO's samen, is ideaal. Het feit dat indicatoren abstract worden opgeschreven zorgt ervoor dat de security profiler blijft nadenken.
De verdachte indicatoren die gebruikt worden zijn niet geheim. De gedachte is immers dat iemand die weet dat hij of zij een onbevoegde handeling gaat uitvoeren zichzelf nooit helemaal onder controle heeft. Er is altijd 'lekkage'. Om vertrouwen in dit uitgangspunt te krijgen is het zelf deelnemen aan red teaming-oefeningen van essentieel belang. Iedereen die in de praktijk 'aan de criminele kant heeft gestaan', al is het maar tijdens een oefening, heeft aan den lijve ondervonden dat de wetenschap van 'bad intent' normafwijkend gedrag tot gevolg heeft.

Uitgangspunten Het is belangrijk om een aantal uitgangspunten expliciet op schrift te stellen. Er kan dan gedacht worden aan de eerdere opmerkingen over 'worst case scenario' alsook aan het feit dat een gegeven classificatie niet kan worden verlaagd door een supervisor of manager. Wat ook goed is om in een SOP te melden, is dat 'niet verklaarde verdachte indicatoren met als gevolg een niet ontkrachte dreiging' niet meer losgelaten mogen worden (worst case). Dit wil echter niet zeggen dat bij een niet ontkrachte dreiging een persoon 'verdachte' wordt. In tegendeel, een niet ontkrachte dreiging wil helemaal niet zeggen dat er iets gaat gebeuren. Dit betekent dat, als het om een persoon gaat, deze zo min mogelijk last mag hebben van de aanvullende beveiligingsmaatregelen die getroffen worden. Wij hebben immers met een 'onschuldige burger' te maken die, als hij of zij dat wil, ook mag liegen als de security profiler vragen gaat stellen. Uiteindelijk heeft de security profiler een probleem als een dreiging niet ontkracht kan worden, niet de persoon die verdachte indicatoren laten zien. De security profiler zal derhalve creatief te werk moeten gaan en communicatief vaardig moeten zijn om de juiste antwoorden te krijgen zodat hij kan 'loslaten'. In de praktijk is het onderstaande auteurs nooit overkomen dat zij een AMO niet konden ontkrachten of dat, uitgaande van een worst case scenario, niet afdoende mitigerende beveiligingsmaatregelen konden worden getroffen. Zolang er binnen de SOP maar ruimte wordt gegeven om ook 'out-of-the-box' te blijven denken. Bovendien is een SOP een levend document. Als uit een red teaming-oefening blijkt dat er een nieuw AMO moet worden opgenomen, omdat het realistisch en uitvoerbaar is, dan zal de SOP moeten worden aangepast.

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