Proactieve beveiliging: risico- of dreigingsbenadering

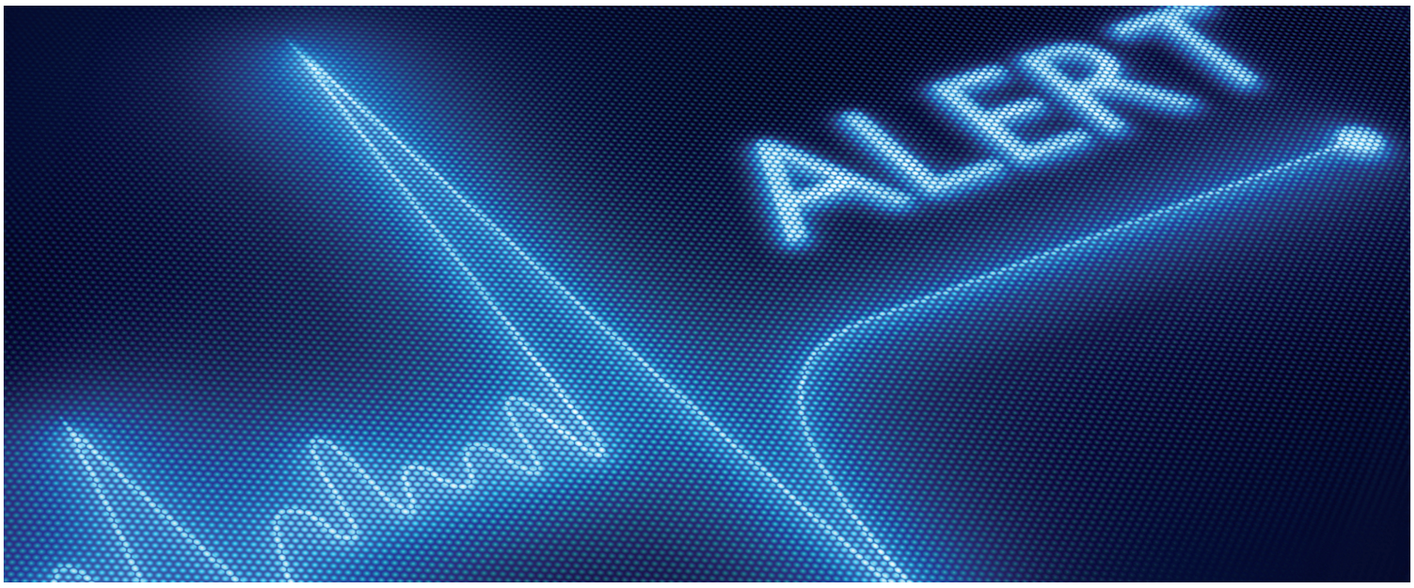
deel 8

Inmiddels weet u uit welke stappen de proactieve beveiligingscyclus bestaat, hoe de criminele planningscyclus er uitziet en aan welke eisen een SOP moet voldoen wil deze bruikbaar zijn voor de security profiler. In dit laatste artikel van de serie 'proactieve beveiliging' staat de vraag centraal of een organisatie die een proactief beveiligingsproces heeft ingericht vanuit een risico- of dreigingsbenadering werkt. Om deze vraag te beantwoorden is het belangrijk om het inhoudelijke verschil tussen de begrippen dreigingsanalyse, risicoanalyse en dreigingsassessment te kennen. Het gaat dan niet zo zeer om de gebruikte termen, maar om het inhoudelijke proces wat er achter schuil gaat gezien vanuit het perspectief van het proactieve beveiligingsproces.

Het zal u niet verbazen dat het echte antwoord op de gestelde vraag, of proactieve beveiliging vanuit een risico- of dreigingsbenadering werkt, 'beide' is. Zowel de risicobenadering alsook de dreigingsbenadering komt terug binnen de proactieve beveiligingscyclus, maar dat heeft wel een nadere uitleg nodig. Het gaat er namelijk om de activiteiten die deel uitmaken van het proactieve beveiligingsproces en die zichtbaar worden in de verschillende stappen binnen de proactieve beveiligingscyclus, op de juiste plaats in de organisatie te positioneren. De beschreven cyclus laat namelijk alleen de activiteiten op het operationele niveau zien, niet de relaties met tactische en strategische processen. Dit is de reden dat in het laatste artikel van de serie proactieve beveiliging de verantwoordelijkheid van de security manager op tactisch niveau, het lijnmanagement (lees: de directie) op strategische niveau en de security profiler op operationeel niveau beschreven wordt. Waarom beginnen met de beschrijving van een tactisch product (dreigingsanalyse) in plaats van met een strategisch product (risicoanalyse) vraagt u zich wellicht af? Het antwoord daarop is dat er zonder dreigingsanalyse, die noodzakelijke input geeft voor de risicoanalyse, er geen goede risicoafweging kan worden gemaakt. De conclusie die getrokken kan worden als wij naar de dagelijkse praktijk kijken is, en soms is kort door de bocht gaan ook wel prettig, dat er eigenlijk weinig goede risicoanalyses zijn die de toets der kritiek kunnen doorstaan. Daarom moet de security manager altijd achteraf uitleggen waarom het 'weer' fout is gegaan.

Dreigingsanalyse De security manager is de professional binnen de organisatie die verantwoordelijk is voor het in kaart brengen van de specifieke bedreigers en de dreigingen die daarvan het gevolg zijn, die een gevaar vormen voor de belangen van de organisatie. Dit kunnen zowel externe alsook interne bedreigers zijn. Om een transparant overzicht te krijgen van de bedreigers stelt de security manager een dreigingsanalyse op. Deze analyse, die de noodzakelijke input voor een risicoanalyse vormt, dient duidelijkheid te geven over de capaciteit en de motivatie van de externe- en interne tegenstander ten opzichte van de organisatie. Omdat een dreigingsanalyse de tegenstanders alleen op een transparante wijze in kaart brengt wordt er nu nog geen uitspraak gedaan over de vraag wat de kans is dat een tegenstander zich tegen de organisatie zal gaan richten. Dit klinkt simpel, maar wat betekent dit nu voor de security manager? Om op tactisch niveau een dreigingsanalyse te kunnen opstellen, zal de security manager zijn externe- en interne tegenstanders moeten bestuderen. De security manager zal moeten weten hoe zijn tegenstander te werk gaat, welke middelen de tegenstander gebruikt, wat de incidenten zijn die zich de afgelopen jaren (extern en intern) hebben voorgedaan en hoe de trend er uitziet voor wat betreft de te verwachten ontwikkeling. Bovendien zal de dreigingsanalyse compleet moeten zijn, want niet beschreven tegenstanders of werkwijzen worden niet meegenomen in het vervolgtraject (de risicoanalyse). Dit maakt te meer duidelijk waarom red teaming en horizonscanning zo belangrijk zijn als de security manager niet steeds de vorige oorlog wil vechten met als gevolg steeds opnieuw moeten uitleggen waarom er zich weer een incident heeft voorgedaan. Als de security manager geen 'security intelligence professional' is, en niet over de noodzakelijke onderzoekscapaciteiten en het netwerk beschikt om op een transparante en herleidbare wijze de voor de analyse benodigde informatie te verwerven, is dit een zware klus. Op zich is het natuurlijk geen enkel probleem als de security manager de dreigingsanalyse niet zelf opstelt want een goede security manager verzamelt, zoals iedere goede leider, de juiste mensen om zich heen die het werk voor hem of haar kunnen doen.

Risicoanalyse Het lijnmanagement is verantwoordelijk voor het accepteren van risico's die het primaire proces van



de organisatie bedreigen. Het accepteren van risico's is uitdrukkelijk geen verantwoordelijkheid van de security manager. De security manager is wel verantwoordelijk voor het aanleveren van de juiste input, een dreigingsanalyse, zodat het lijnmanagement op basis van alle beschikbare informatie kan besluiten risico's te accepteren of, als zij risico's niet wenst te accepteren, de security manager de opdracht te geven deze te mitigeren. Als de dreigingsanalyse niet volledig was, waardoor er wellicht bij de besluitvorming een achteraf verkeerde beslissing genomen is, dan zal de security manager daar op aangesproken worden.
Daarnaast heeft de security manager ook een probleem als hij niet geaccepteerde risico's moet mitigeren en deze opdracht van het lijnmanagement aanneemt, terwijl hij niet voldoende middelen (budget) heeft om specifieke dreiging op het operationele niveau af te vangen. Daar waar het lijnmanagement in de risicoafweging de kans- en impactvraag meeneemt, is deze voor de security manager niet van belang. Bij niet geaccepteerde risico's, waarvoor de in de dreigingsanalyse beschreven werkwijze van tegenstanders input was, kan een security manager de dreiging die aan het risico ten grondslag lag alleen mitigeren met de juiste middelen en voldoende budget. Wordt een risico door het lijnmanagement niet geaccepteerd, maar er worden ook niet voldoende middelen vrijgemaakt om die maatregelen in te voeren die de werkwijze van de tegenstander afblokken, dan zal de security manager het restrisico moeten rapporteren.
Daar waar een security manager aangesproken wordt op een manifest geworden risico, vanwege een dreiging die een incident tot gevolg heeft gehad, kan dit maar twee oorzaken hebben.
De security manager heeft het restrisico, vanwege een te beperkt budget, niet gerapporteerd of heeft ten opzichte van de werkwijze van de tegenstander de verkeerde beveiligingsmaatregelen geïmplementeerd. Dan kan de vraag gesteld worden, en dat blijkt vanzelf uit de opgestelde dreigingsanalyse die de input voor de risicoanalyse was, kent de security manager zijn tegenstander wel?

Het vaststellen van de risicoanalyse, met een inschatting van de kans dat een dreiging zich voordoet, is een verantwoordelijkheid van het lijnmanagement en niet van de security manager.

Dreigingsassessment De security profiler heeft het, binnen het proactieve beveiligingsproces, relatief gemakkelijk. Hij of zij hoeft geen 'kansinschatting' te maken, maar hoeft alleen te bepalen wel (1) of geen (0) dreiging op basis van de Standaard Operationele Procedure (SOP). Kortom een relatief eenvoudig assessment, de uitslag is zwart of wit. In het SOP staat immers, per risicopositie, de relevante Aanvallers Methode van Operatie (AMO) beschreven die ontkracht moet worden. Daar waar een dreiging, het AMO, niet ontkracht kan worden staat in de SOP ook beschreven welke aanvullende beveiligingsmaatregelen ter mitigatie genomen dienen te worden. Ook hier komt het belang van de door de security manager opgestelde dreigingsanalyse weer naar voren. Als de security manager de tegenstander niet kent of heeft onderkend, op basis van incidenten uit het verleden of red teaming oefeningen waarbij het ook gaat om het vinden van nieuwe AMO's, zal de security profiler daar in zijn dreigingsassessment ook geen rekening mee kunnen houden. Het AMO staat immers niet beschreven in de SOP. Dit maakt ook meteen duidelijk waarom veel organisaties, die besluiten op een proactieve wijze te gaan beveiligen, hun eigen teleurstelling al hebben georganiseerd. Daar waar al sprake is van de implementatie van alle stappen van de cyclus zal uiteindelijk, als er zich toch incidenten voordoen, de security manager moeten uitleggen waarom het heeft kunnen gebeuren. Waarom? Vanwege het feit dat het proces, waarbij een juiste dreigingsanalyse als input voor de risicoanalyse wordt gebruikt, niet is ingericht. De verantwoordelijkheid voor het wel of niet accepteren van risico's, en ter beschikking stellen van voldoende middelen om dreigingen te mitigeren, is niet op een transparante wijze bij het lijnmanagement neergelegd. Rest alleen de vraag nog maar: wil de security manager het niet of kan de security manager het niet?

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