Infiltratie door kwaadwillen

deel 2

Het is de nachtmerrie van iedere organisatie. Kwaadwillenden die bewust in dienst komen bij een bedrijf om hun snode plannen uit te voeren. De laatste weken halen regelmatig berichten het nieuws dat organisaties geradicaliseerde moslims in dienst hadden, of dat zij deze via andere organisaties inhuurden voor het leveren van diensten. Maar ook criminele organisaties en (buitenlandse) inlichtingendiensten hebben in het verleden laten zien doelbewust bedrijven te infiltreren om van binnenuit informatie te stelen of andere attractieve goederen.

Helaas is 'infiltratie' een verschijnsel dat er altijd geweest is en er ook altijd zal zijn. Koningen in de oudheid werden al vergiftigd met hulp vanuit de eigen hofhouding, en ook toekomstige security managers zullen altijd met dit verschijnsel rekening moeten blijven houden. Hoe beter fysieke- en ICT beveiligingsmaatregelen zijn, hoe waarschijnlijker het is dat tegenstanders zich op de slechtst beveiligde poort richten. En helaas is dat de menselijke poort. Naast het feit dat medewerkers die belast zijn met het uitvoeren van preemployment screening moeten werken met de handen op de rug gebonden, is iedere kandidaat - en dat is terecht - onschuldig tot dat het tegendeel bewezen is. Dit stelt de security manager wel voor een uitdaging.

Huiswerk Een criminele organisatie zal, als zij een organisatie willen infiltreren, zijn huiswerk goed doen. Op de kandidaat die direct solliciteert op een functie zal niets aan te merken zijn. Hij of zij zal een uitstekend CV hebben, de opleiding sluit goed aan op de gevraagde competenties en de werkervaring is te mooi om waar te zijn. Kortom, de droom van iedere lijnmanager. De VOG (Verklaring Omtrent het Gedrag) zal, als daar om gevraagd wordt, ook zonder probleem worden verstrekt. Helaas blijken dromen vaak bedrog. De goed voorbereide infiltrant heeft natuurlijk ook geen strafblad. Als een criminele organisatie al een fout maakt bij de voorbereiding om een bedrijf te infiltreren, dan zal een (buitenlandse) inlichtingendienst dat zeker niet doen. De security manager zal er helaas mee moeten leven dat een infiltrant waarschijnlijk met vlag en wimpel door een preemployment screening heen zal komen. Zelfs als dat screeningsprogramma gebruik maakt van 'verdachte indicatoren' omdat er sprake is van Insider Threat Profiling. Niet ontkrachte indicatoren, die mogelijk kunnen wijzen op een dreiging, zijn voor veel bedrijfsjuristen - gesteund door ondernemingsraden - niet voldoende om een kandidaat af te wijzen. Hij of zij heeft immers (nog) niets gedaan. En dat is ook terecht. Desondanks kan een dergelijke kandidaat die direct bij de organisatie in dienst komt, of die via een toeleverancier toegang tot het bedrijf krijgt, wel extra aandacht van de security manager krijgen.

Zwakste schakel Als een kandidaat onderwerp van onderzoek is tijdens een preemployment screening dan zijn er, specifiek voor het onderkennen van verdachte indicatoren die op infiltratie kunnen wijzen, wel een aantal aandachtspunten. Daarbij moet wel de kanttekening gemaakt worden dat iedereen die toegang krijgt tot een organisatie aan hetzelfde preemployment programma onderworpen dient te worden. Alleen personen screenen die in dienst komen van de organisaties, maar ingehuurde (tijdelijke) medewerkers en medewerkers van toeleveranciers niet heeft geen enkele zin. Zonde van het geld. Als een deel van de personen die toegang tot een organisatie hebben niet wordt gescreend, op welke functies zal een criminele organisatie dan zijn pijlen richten? Het is ook opmerkelijk om te zien dat organisaties managers soms goed screenen, maar bepaalde groepen (facilitaire) medewerkers niet, terwijl die zich vaak ongezien door de hele organisatie kunnen bewegen. Helaas wordt bij de inzet van screeningsinstrumenten, en het bepalen van screeningsprofielen, niet uitgegaan van een onderkende Aanvallers Methode van Operatie (AMO) zoals die door de tegenstander gebruikt wordt. Sterker, de meeste medewerkers die met preemployment screening belast zijn hebben geen flauw idee hoe tegenstanders te werk gaan als zij het bedrijf willen infiltreren. Misschien is het zelfs wel goed om, op een transparante wijze, het risico te accepteren dat een preeemployment screening niet de dreiging van infiltratie zal afvangen. Het is in ieder geval integer om dat te benoemen.

Werkverleden Kan er nu helemaal, als er gebruik wordt gemaakt van Insider Threat Profiling, geen indicatie gevonden worden die op infiltratie kan wijzen? Het antwoord daarop is nee, er zijn wel degelijk 'verdachte indicatoren' die aan AMO's te koppelen zijn waardoor er wel degelijk over een dreiging gesproken kan worden die van een medewerker uitgaat. Al is het alleen maar omdat, als er naar aanleiding van gevonden indicatoren met een (toekomstig) medewerker gesproken wordt, hij of zij geen goede antwoorden kan geven. Vaak gaat het niet kunnen geven van goede antwoorden ook samen met het vinden van nieuwe indicatoren waardoor een dreiging niet ontkracht kan worden en er vragentekens blijven voor wat betreft betrouwbaarheid en loyaliteit van de medewerker. Om verdachte indicatoren te vinden, die een gesprek in het kader van preemployment screening tot gevolg moet hebben, is een door een toekomstig medewerker in te vullen

den



vragenlijst essentieel. Belangrijk is om in deze vragenlijst onderwerpen op te nemen die controleerbaar zijn. En nog belangrijker is het om die controle dan ook daadwerkelijk uit te voeren. Wat zijn nu indicatoren waar een insider threat profiler op kan aanslaan? Bij het werkverleden zijn voormalig werkgevers interessant die niet meer bestaan, zeker als dat er meer zijn. Ook het uitgaven- en inkomstenpatroon, en dan met name de relatie tussen beide, zijn interessant. Dat een toekomstig medewerker een hoog uitgavenpatroon heeft is geen enkel probleem zolang maar duidelijk is hoe hij of zij, als het van de norm afwijkt, het kan bekostigen.

Afwijkend gedrag Het is al eerder gezegd, de kans dat de insider threat profiler tijdens een preemployment screening een infiltrant kan onderkennen is klein. Zeker als deze profiler met een goed voorbereide tegenstander te maken krijgt. Veel organisaties stellen zich daarnaast ook op het standpunt dat de insider threat profiler moet bewijzen dat een toekomstig medewerker niet betrouwbaar is, en dat kan niet. De insider threat profiler kan alleen adviseren om bij twijfel niet in te halen als er verdachte indicatoren gevonden zijn en deze, tijdens een gesprek, niet kunnen worden verklaard waardoor een geïdentificeerd AMO - lees dreiging - niet ontkracht kan worden. Meestal zal in zo'n geval een medewerker gewoon in dienst komen. Gelukkig keren daarna de kansen. De infiltrant is, zodra hij binnen de organisatie aan de slag gaat, op het thuisgebied van de insider threat profiler. Incidenten in het verleden, weliswaar nadat een incident zich heeft voorgedaan, laten zien dat als er sprake is geweest van infiltratie er achteraf over de betrokken onbetrouwbare medewerker door vrijwel iedereen gezegd wordt 'Ik wist wel dat er iets niet klopte'. Dit betekent dat er dus waarneembare verdachte indicatoren zijn, afwijkend gedrag, die aan dit AMO te koppelen zijn. De insider threat profiler zal aan de hand van zijn of haar kennis de organisatie, managers en medewerkers, moeten voorlichten over waarneembaar afwijkend gedrag. Het is dan ook belangrijk dat iedereen binnen de organisatie zich realiseert dat iedereen verantwoordelijk is voor veiligheid. Het motto moet dan zijn dat bij twijfel bepaald gedrag worden gemeld.

Verdachte Is dan meteen iedereen verdacht die zich afwijkend gedraagt? Nee, natuurlijk niet. En moet iedere medewerker die verdachte indicatoren laat zien meteen op gesprek bij de insider threat profiler? Nee, ook dat niet. Maar het is voor de cultuur binnen een organisatie goed dat als mensen zich ineens anders gaan gedragen dan verwacht dit wel bespreekbaar wordt gemaakt. Al is het alleen maar om vast te stellen of iemand een probleem heeft waar hij of zij door de organisatie mee geholpen kan worden. De impact van incidenten, zeker als daar een infiltrant bij betrokken is, is vaak zo groot dat achteraf zeggen 'ik wist wel dat er iets niet in de haak was' niet verantwoord is. In een organisatie met een open discussie cultuur, waar alles bespreekbaar is en medewerkers elkaar op gedrag aanspreken, is het lastig vertoeven voor een infiltrant met een opdracht. Het feit dat er sprake is van een dergelijke cultuur, in combinatie met het feit dat preemployment screening en inemployment screening belangrijk gevonden worden, kunnen criminele organisaties er wel toe bewegen een ander 'target' te kiezen. Toch blijft dit, infiltratie, lastig te onderkennen. In het volgende artikel van deze serie staan wij stil bij het onderwerp rekrutering. Op dit vlak, het onderkennen van de kwetsbaarheden die tot rekrutering kunnen leiden, stijgen de kansen van de insider threat profiler.

■ Berndt Rif MSc MBA MSec
Redactie@beveiliging.nl
■ Allon Knetemann
aknetemann@chameleonassociates.com