Insider Threat Security Prof

deel 1

Steeds opnieuw halen incidenten waarbij personeelsleden of vrijwilligers niet zo betrouwbaar bleken als gedacht de voorpagina van de krant. De ene keer is het een trainer bij een sportvereniging, daarna een medewerker die binnen een bedrijf gefraudeerd heeft en nu zijn enkele beveiligers van Geert Wilders in opspraak geraakt omdat zij er onwenselijke 'vrienden' op na blijken te houden aan wie 'mogelijk' informatie is verstrekt. Hoe kan het toch dat keer op keer de mechanismen die onbetrouwbare personeelsleden moeten identificeren - pre-employment screening en in-employment screening - falen?

Het antwoord op die vraag is net zo ontluisterend als simpel. Omdat bedrijfsjuristen en ondernemingsraden op de stoel van de rechter gaan zitten en de voor screening verantwoordelijke functionarissen verbieden om naar kwetsbaarheden van (toekomstige) personeelsleden of vrijwilligers te kijken waar criminele organisaties wel misbruik van maken. Het is daarom eerder geluk dan wijsheid als een mogelijke 'insider', die een dreiging kan opleveren voor een bedrijf of vereniging, vroegtijdig wordt geïdentificeerd. Helaas komen vaak alleen die personen tijdens een pre-employment screening naar boven die zo dom waren om in het verleden al een keer tegen de lamp te lopen. Als een strafbaar feit te lang geleden gepleegd is wordt er, mocht daar naar gevraagd worden, gewoon een VOG (Verklaring Omtrent Gedrag) verstrekt. Mocht uw bedrijf het instrument screening inzetten omdat er dan aan een compliancy verplichting wordt voldaan, en is het zolang er maar een 'tick-in-the-box' kan worden gezet niet belangrijk dat er zich incidenten blijven voordoen, sla dit artikel dan vooral over. Wilt u serieus werk maken van het onderwerp pre-employment en in-employment screening, dan is dit artikel wellicht wel interessant voor u. Zeker als u weet dat de meeste 'insiders' die een dreiging voor de organisatie opleveren 'first time' offenders zijn. Deze groep komt met vlag en wimpel door alle 'klassieke' pre-employment screeningen heen, ook al hebben de betreffende personen veel kwetsbaarheden waar kwaadwillenden gebruik van kunnen maken.

Bedreigingen In dit eerste artikel van de serie Insider Threat Security Profiling wordt stilgestaan bij de drie typen van bedreigingen die aan insiders verbonden zijn. In de volgende artikelen van deze serie zal aandacht worden besteed aan de benodigde maatregelen om kwetsbaarheden bij toekomstige en huidige personeelsleden te identificeren. Door op een transparante manier met het instrument screening om te gaan, en geïdentificeerde kwetsbaarheden bespreekbaar te maken, kan de inbreuk op de privacy van personeelsleden zelfs beperkt worden in vergelijking met de huidige wijze van screenen. Waar bij een klassieke benadering van een personeelslid afscheid genomen



filing

wordt als er risico's worden ontdekt kan, bij een op een juiste wijze geïmplementeerd Insider Threat Security Profiling programma, een personeelslid met de juiste begeleiding gewoon in dienst blijven. De vraag aan de klassieke bedrijfsjurist zou moeten zijn: wat is nu een grotere inbreuk op de privacy? Een persoon niet in dienst nemen en een medewerker ontslaan omdat er risico's zijn geïdentificeerd? Het is immers helemaal niet zeker of die risico's zich in de toekomst gaan manifesteren. Het probleem met de klassieke benadering is dat vanuit het risico-denken niet kan worden bewezen dat een medewerker betrouwbaar is. Een goed Insider Threat Security Profiling programma zal, zoals gebruikelijk als er gewerkt wordt vanuit een dreigingsbenadering, kwetsbaarheden identificeren en dreigingen ontkrachten. Door dit op een transparante wijze te doen, in samenspraak met de kwetsbare medewerker, hoeft er geen sprake te zijn van 'niet in dienst nemen' of 'ontslag'. Een goed Insider Threat Security Profiling programma heeft als neveneffect loyale medewerkers.

Infiltratie In deze serie die ingaat op pre-employment en in-employment screening wil infiltratie zeggen dat een criminele organisatie, terroristische organisatie of (buitenlandse) inlichtingendienst een persoon bij uw organisatie laat solliciteren met als doel daadwerkelijk in dienst te worden genomen. Dit is natuurlijk de ultieme insider. De organisatie die dit initieert is op de hoogte met de stappen binnen het sollicitatietraject, en ook met de onderdelen van een eventueel pre-employment screeningsprogramma. De kwaadwillende medewerker die solliciteert heeft precies het CV waar uw organisatie naar op zoek is. Een vaak gehoorde uitlating is, vooral als het achteraf fout is gegaan, 'eigenlijk was de kandidaat te mooi om waar te zijn'. Naast het prachtige CV zal deze kandidaat ook geen strafblad hebben. De referenties zullen zijn of haar kandidatuur ook zeker ondersteunen. Kortom, de infiltrant zal zonder problemen door de klassieke pre-employment procedure komen. De professionals die verantwoordelijk zijn voor het uitvoeren van de screening hebben geen schijn van kans, hun handen zijn op hun rug gebonden door de bedrijfsjuristen en de ondernemingsraad, maar als er achteraf iets 'fout' gaat is het wel duidelijk waar de zwarte piet wordt neergelegd.
In het tweede artikel van deze serie zal, met inachtneming van privacy en vigerende regelgeving, beschreven worden hoe door middel van security profiling mogelijke infiltranten onderkent kunnen worden. Geeft dit een honderd procent zekerheid dat kwaadwillenden niet met voorbedachte rade uw organisatie binnen komen? Nee, zeker niet. Maar de professional die met screening bezig is heeft in ieder geval een kans. Dit in tegenstelling tot de klassieke benadering. Een neveneffect is dat tegenstanders van uw organisatie, bij een voor hun onvoorspelbare methodologie, wel drie keer zullen nadenken of infiltratie de moeite waard is. Het kost namelijk veel tijd en geld om dit goed voor te bereiden.

Rekrutering De medewerker die eenmaal is aangenomen, en die een vast contract heeft of op termijn krijgt, is voor tegenstanders - criminele organisaties, terroristische organisaties en (buitenlandse) inlichtingendiensten - het meest interessante doelwit. Er hoeven geen gecompliceerde voorbereidingen te worden getroffen om iemand binnen uw organisatie te laten infiltreren, het is voldoende om bij huidige personeelsleden kwetsbaarheden te vinden waar misbruik van gemaakt kan worden. Een medewerker die iets geheim wil houden voor zijn familie, een medewerker die financiële problemen heeft vanwege een recente scheiding of een gefrustreerde medewerker die weer een bevordering is misgelopen hebben allemaal een bepaalde kwetsbaarheid. Er zijn natuurlijk nog veel meer aanknopingspunten en daar zoeken de tegenstanders van uw organisatie naar in de privésfeer van de werknemer - sportvereniging en in het café - of door uitlatingen op social media. Een Insider Threat Security Profiling programma identificeert, op dezelfde wijze als de tegenstanders van de organisatie doen, kwetsbaarheden bij medewerkers of vrijwilligers. Alleen maakt de professional die binnen uw organisatie deze kwetsbaarheden identificeert geen misbruik van de bevindingen, maar hij of zij maakt deze bespreekbaar. Door vervolgens afspraken te maken met de betreffende medewerker kan een dreiging die van een kwetsbaarheid uitgaat worden ontkracht en kan, in het verlengde daarvan, de betrouwbaarheid van een medewerker worden vastgesteld. Daarnaast is het mogelijk om eerder signalen op te vangen van een tegenstander die probeert deze kwetsbaarheden bij medewerkers of vrijwilligers te exploiteren; de medewerker wordt in plaats van dreiging voor de organisatie een belangrijke bron van informatie. Helaas mogen veel professionals die zich met screening bezighouden van bedrijfsjuristen en ondernemingsraden niet werken op basis van een dergelijke dreigingsbenadering, zoals tegenstanders van de organisatie wel doen. ▸

De professionals die verantwoordelijk zijn voor het uitvoeren van de screeningen hebben bij klassiek uitgevoerde onderzoeken geen schijn van kans om kwaadwillenden te identificeren. Hun handen zijn op door de bedrijfsjuristen en de ondernemingsraad op de rug gebonden, maar als er achteraf iets 'fout' gaat is het wel duidelijk waar de zwarte piet wordt neergelegd.



Zelfs niet als de organisatie zijn werknemers daardoor niet op een adequate wijze bescherming geeft tegen door criminele gebruikte bekende methodieken. Toch opmerkelijk, de bedrijfsjurist en de ondernemingsraad die niet willen dat de organisatie haar 'duty-of-care' verplichting naleeft.

Helaas komen vaak alleen die personen tijdens een op de klassieke wijze uitgevoerde pre-employment screening naar boven die zo dom waren om in het verleden al een keer tegen de lamp te lopen.

In het derde artikel van deze serie zal uitvoerig worden stilgestaan bij de instrumenten die kunnen worden ingezet om kwetsbaarheden te onderkennen en de daaraan gekoppelde dreigingen te ontkrachten. Daardoor is de betrouwbaarheid van een medewerker vast te stellen en, in het verlengde daarvan, is er sprake van meer loyaliteit naar de organisatie.

Insider Natuurlijk zijn er ook medewerkers die, door een gebeurtenis die zich in hun leven voordoet, zelf over de streep stappen en strafbare feiten gaan plegen zoals fraude, diefstal of het lekken van informatie. Deze medewerkers hebben geen relatie met een externe tegenstander zoals bij infiltratie of rekrutering wel het geval is. Deze medewerkers gaan zelf in de fout en zullen zich 'crimineel' gaan gedragen. Een Insider Threat Security Profiling programma zal, omdat het zich ook richt op professionele tegenstanders, een medewerker die vanwege 'interne' kwetsbaarheden of door intern ervaren druk in de fout gaat ook eerder onderkennen. Omdat een dergelijk programma gebruik maakt van indicatoren die te koppelen zijn aan onbevoegde handelingen en kwetsbaarheden is het zelfs waarschijnlijk dat voorkomen kan worden dat een medewerker in 'de fout' gaat. Het Insider Threat Security Profiling programma werkt immers ook als een soort 'early warning' systeem. Juist omdat alle maatregelen transparant worden ingezet en kwetsbaarheden in een vroegtijdig stadium besproken worden. Een organisatie die op een bewuste manier met Insider Threat Security Profiling omgaat is een sociale en betrokken organisatie. Niet een organisatie met een angstcultuur waarin kwetsbaarheden, en fouten, niet bespreekbaar zijn.
In het vierde artikel van deze serie zal besproken worden hoe er omgegaan kan worden met de insider die zelf besluit onbevoegde handelingen te gaan plegen. Het is beter om een medewerker tegen het zetten van een misstap te beschermen dan om achteraf te zeggen 'wij wisten wel dat er iets niet in de haak was'. Helaas is dit wel een veelgehoorde opmerking bij organisaties die slechts screenen om aan te tonen dat zij 'compliant zijn' met bepaalde regelgeving.

Implementatie Nadat dit jaar in de volgende drie artikelen van deze serie stilgestaan is bij het theoretische kader zal, in een viertal aanvullende artikelen, ook het woord aan voor-aanstaande professionals gegeven worden die inmiddels onderdelen van een Insider Threat Security Profiling programma geïmplementeerd hebben of die onderwijs op dit vlak geven. Ook zal, om beter voorbereid het gesprek met bedrijfsjuristen en ondernemingsraden aan te kunnen gaan, met een op dit gebied gespecialiseerde jurist gesproken worden. Er mag meer dan vaak gedacht wordt. Zolang het maar transparant, proportioneel, subsidiair en uitlegbaar is. Een op de juiste wijze geïmplementeerd Insider Threat Security Profiling programma voldoet aan alle eisen van de door de VBN en ASIS Benelux Chapter, in de Nationale Richtlijn Pre-employment en In-employment Screening 2012-2017, beschreven eisen.

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