Sollicitant met 'vuiltje' kan medewerker blijken

deel 5

Een insider threat programma dat als doel heeft het opsporen van medewerkers die iets fout hebben gedaan om deze vervolgens te straffen, zal er slechts toe leiden dat collega's hun kwetsbaarheden nog beter gaan verbergen. Een modern insider threat programma ziet medewerkers als te beschermen 'asset' en helpt hen met het doel te voorkomen dat er misstappen worden gemaakt door hen optimaal te informeren en bij de uitvoering te betrekken.

In dit laatste artikel van de serie Insider Threat Security Profiling wordt stilgestaan bij het implementeren van een programma om de dreiging die van medewerkers kan uitgaan effectief te mitigeren. Belangrijk is daarbij om eerst even stil te staan bij de cultuur van de eigen organisatie. Als in een bedrijf of instelling medewerkers worden afgerekend op gemaakte fouten, is het vrijwel ondoenlijk om een effectief insider threat programma te implementeren. Niemand zal immers vrijwillig melden dat hij of zij 'de fout in is gegaan', want dat heeft negatieve en verstrekkende gevolgen. Mogelijk zelfs ontslag. Binnen organisaties met een afrekencultuur zullen medewerkers, en daar vallen ook managers en directieleden onder, gemaakte fouten of niet integer gedrag proberen af te dekken. Dit gedrag maakt de medewerker en de organisatie helaas nog kwetsbaarder. Als de beerput dan eenmaal opengaat, is er geen houden meer aan. Los van mogelijke strafrechtelijke consequenties zijn grote koppen in de landelijke dagbladen niet ondenkbaar, met reputatieschade voor de organisatie of het bedrijf tot gevolg. Organisaties die pre-employment zien als compliance activiteit, en het nut van een insider threat programma om de in de risicoanalyse geïdentificeerde dreiging die van medewerkers kan uitgaan te mitigeren niet zien, verspillen iedere euro die zij aan een pre-employment screening uitgeven. Uitgangspunt van dit laatste artikel is dat de implementatie van een effectief insider threat programma alleen mogelijk is als de in de Nationale Richtlijn Pre-employment en In-employment beschreven stappen bewust zijn genomen of bewust, met risico-acceptatie, zijn overgeslagen.

Preventie Een essentieel startpunt van een effectief insider threat programma is het uitvoeren van een pre-employent screening waarbij de diepte en omvang van het onderzoek een relatie heeft met de door de organisatie uitgevoerde risicoanalyse. Bij het uitvoeren van het pre-employment onderzoek is kennis van indicatoren die kunnen wijzen op kwetsbaarheden die bij voldoende druk tot gevolg kunnen hebben dat medewerkers de fout in kunnen gaan onontbeerlijk. De benadering dat potentiële medewerkers bij kwetsbaarheden, of op basis van in het verleden gemaakte fouten, 'per definitie' afgewezen worden is een twintigste eeuwse benadering die niet strookt met de eisen die in de bovengenoemde Nationale Richtlijn staan. Informatie kan onjuist zijn, soms kan het relevant zijn om de context waarin iets heeft plaatsgevonden te kennen en mensen kunnen natuurlijk ook ten positieve veranderen. Iedere beslissing om een potentiële medewerker door middel van een pre-employment screening af te wijzen zal maatwerk moeten zijn. Natuurlijk is een doelstelling van een pre-employment screening om de organisatie te beschermen tegen mensen met kwade bedoelingen, maar het is ook goed dat wij ons blijven realiseren dat medewerkers die de fout ingaan en onbevoegde handelingen verrichten 85 procent zogenaamde first time offenders zijn. Potentiële medewerkers waar een 'vuiltje' aan zit, en die dit zelf tijdens een pre-employment screening bespreekbaar maken, kunnen wel eens zeer loyale medewerkers worden op het moment dat zij een kans krijgen. Nu is er natuurlijk nooit een per definitie goede of niet foute beslissing. Wil een insider threat programma effectief zijn, dan is het echter wel belangrijk dat er ruimte moet zijn voor maatwerk en beslissing op maat. De 'insider threat profiler' zal daarom ook de implicaties van zijn advies in de breedte moeten kunnen overzien.

Beschermen De werkgever is, als wij naar het Burgerlijk Wetboek kijken, verplicht om voor een veilige werkomgeving te zorgen. Als de werkgever had kunnen weten dat kwetsbaarheden die een medewerker heeft tot gevolg kunnen hebben dat die medewerker de fout in gaat, door interne of door externe druk, dan zal de werkgever die medewerker moeten beschermen. Dit kan alleen als de werkgever samen met de werknemer op zoek gaat naar de kwetsbaarheden die, als naar de risicoanalyse van de organisatie gekeken wordt, een dreiging kunnen opleveren. Deze kwetsbaarheden dienen dan op een transparante wijze bespreekbaar te worden gemaakt. Het uitgangspunt is dan niet dat medewerkers die kwetsbaarheden hebben ontslagen worden, zoals binnen de twintigste eeuwse benadering gebruikelijk was, maar dat er gekeken wordt hoe de medewerker met kwetsbaarheden geholpen kan worden zodat hij of zij bij interne of externe druk niet de fout in gaat.
Juristen zullen dan wellicht roepen dat dit een te grote inbreuk op de privacy van de medewerker is. Vaak zijn dit dezelfde juristen die, als iemand een kwetsbaarheid heeft of een keer de fout is ingegaan, namens de organisatie zo

wel eens zeer loyale



snel mogelijk afscheid willen nemen van die medewerker. Alsof dat geen inbreuk op de persoonlijke levenssfeer is? Ik zou de discussie willen omdraaien. De werkgever zou wel eens aansprakelijk kunnen zijn als hij had kunnen weten, en misschien wel had moeten weten, dat een medewerker gezien zijn risicopositie kwetsbaarheden had waardoor hij bij interne of externe druk onbevoegde handelingen kan gaan uitvoeren. Als de werkgever had kunnen weten, uitgaande van de risicoanalyse en geïdentificeerde dreigingen, dat de medewerker rekruteerbaar was en hij heeft daar niets aan gedaan, was er dan wel sprake van een veilige werkomgeving?

Integriteit In het einde van twintigste eeuw en het begin van deze eeuw moest iedereen vooral integer zijn. In een bedrijf met alleen maar integere medewerkers zou niemand meer onbevoegde handelingen uitvoeren. Dit is een mooi wensbeeld, maar de praktijk is weerbarstiger. Een persoon kan nog zo integer zijn, maar als hij diep in de schulden zit en er geen eten meer op de plank komt, of als externen maar genoeg druk uitoefenen en gebruik maken van kwetsbaarheden, dan zal zelfs de meest integere persoon gedrag gaan vertonen dat niet wenselijk is. Voor een effectief insider threat programma is het meten van integriteit aan de voorkant niet echt interessant. Belangrijker is om een medewerker te leren kennen en vervolgens als de medewerker 'ineens' gaat veranderen of 'ineens' afwijkend gedrag gaat vertonen daar aandacht aan te besteden. Dat betekent dat de collega's en de eigen lijnmanager, waar de medewerker mee te maken heeft, het vangnet zijn dat kan voorkomen dat iemand zich onwenselijk gaat gedragen.

Een modern insider threat programma probeert te voorkomen dat er misstappen worden gemaakt door medewerkers optimaal te informeren en bij de uitvoering te betrekken.

Voorwaarde is dan wel dat waargenomen afwijkingen van de norm bespreekbaar worden gemaakt. Hoe vaak horen wij niet achteraf, als het fout gegaan is, 'ik wist het wel, Piet gedroeg zich vreemd▸



de laatste tijd'. Preventie, en ook het beschermen van de medewerker zodat hij niet over de streep stapt, vragen in een dergelijke situatie om actie. Benoem de afwijking en maak het bespreekbaar. In die zin is in-employment screening niet meer iets wat iedere drie, vijf of tien jaar herhaald wordt door 'een specialist' die ergens in een ivoren toren zit. In een 'weerbaar bedrijf' of een 'weerbare organisatie' is persoonlijke aandacht en interesse voor de collega de meest effectieve maatregel van een insider threat programma. Daarmee zijn wij weer terug bij cultuur. Het waarnemen van afwijkingen, het je verbazen als mensen zich ineens anders gaan gedragen en het vervolgens bespreekbaar maken van wat je hebt gezien, zijn de fundering van een effectief insider threat programma.

Transparantie Om een effectief insider threat programma te implementeren is het van belang dat alle medewerkers, door middel van regelmatige awareness campagnes, bijgepraat worden over dreigingen en risicovolle kwetsbaarheden. Daarnaast dienen medewerkers ook goed op de hoogte te zijn wat er van hen verwacht wordt als zij indicatoren waarnemen bij collega's die op mogelijke kwetsbaarheden kunnen wijzen. De organisatie zal vervolgens, in het kader van de transparantie, het daadwerkelijk bespreekbaar maken van kwetsbaarheden moeten faciliteren. Uitgangspunt zou daarbij moeten zijn dat als een medewerker zelf een misstap bespreekbaar maakt hij of zij daar niet op afgerekend wordt. Het signaleren en erkennen van fouten is de eerste stap om naar een mogelijke oplossing te komen. Dit vraagt om een geheel nieuwe benadering waarbij het menselijke aspect centraal komt te staan. De vraag zal dan ook altijd moeten zijn 'wat kunnen wij als organisatie van een misstap leren, en hoe kunnen wij voorkomen dat er weer een misstap gemaakt wordt?'. Alleen dan gaat de lerende organisatie hand in hand met de lerende mens.

Loyaliteit De medewerker die fouten mag maken, en misschien wel sterker, de medewerker waarvan kwetsbaarheden ter sprake komen voordat hij een misstap heeft gemaakt met als doel die medewerker te helpen heeft een prachtig resultaat. Die medewerker wordt een loyale medewerker in tegenstelling tot die medewerker die een draai om zijn oren heeft gekregen omdat hij of zij een fout heeft gemaakt. Een goed insider threat programma ziet medewerkers als te beschermen asset en helpt medewerkers met het doel te voorkomen dat er misstappen worden gemaakt. Een slecht insider threat programma spoort medewerkers op die iets fout hebben gedaan, straft deze medewerkers en zorgt ervoor dat andere collega's hun kwetsbaarheden of al gemaakte misstappen nog beter gaan verbergen. Op die manier organiseert de organisatie of instelling haar eigen teleurstelling. Een insider threat programma dat niet heeft weten te voorkomen dat medewerkers misstappen maken, of niet heeft weten te voorkomen dat een medewerker op basis van zijn of haar kwetsbaarheden een instrument voor kwaadwillende buitenstanders is geworden, heeft gefaald. Het bedrijf of de organisatie is er dan ook niet in geslaagd om haar zorgverplichting, zoals die in het Burgerlijk Wetboek staat, na te komen (Art. 7:658). Een modern insider threat programma probeert, door medewerkers optimaal te informeren en bij de uitvoering te betrekken, te voorkomen dat er misstappen worden gemaakt. Tijd voor een nieuwe benadering.

■ Berndt Rif MSc MBA MSec
Redactie@beveiliging.nl