Waarom stappen medewerk

deel 4

Interne fraude, diefstallen van bedrijfseigendommen of het bewust laten lekken van waardevolle informatie zijn helaas aan de orde van de dag. Hoe goed medewerkers vooraf ook zijn gescreend, er zullen altijd mensen zijn die over de grens gaan. Welke redenen zijn hiervoor te benoemen en hoe is dit gedrag vroegtijdig te herkennen om de schade zoveel mogelijk te beperken?

In het vorige deel van deze serie is uitvoerig stilgestaan bij rekrutering van medewerkers door kwaadwillenden. Het kernwoord was daarbij kwetsbaarheid. Een medewerker kan nog zo integer zijn, maar als een medewerker kwetsbaar is en de organisatie beschermt de medewerker niet tegen die kwetsbaarheid, dan is hij of zij een gemakkelijke prooi voor kwaadwillenden om te rekruteren en vervolgens als instrument in te zetten. In het vorige artikel is ook al even gerefereerd aan het 'Report to the Nations on Occupational Fraud and Abuse', wat de Association of Certified Fraud Examiners iedere twee jaar publiceert. Het laatste rapport uit 2016 is, voor wat betreft de beschreven kwetsbaarheden van medewerkers, redelijk consistent als ook naar de eerdere acht publicaties wordt gekeken. Persoonlijke problemen waaronder wijzigingen in de huiselijke sfeer, zoals scheidingen, en ook financiele problemen zijn een kwetsbaarheid waardoor medewerkers in de verleiding kunnen komen om verkeerde dingen te gaan doen ook als er geen sprake is van rekrutering. Als de interne druk maar groot genoeg is, en de omstandigheden laten het toe, kan de medewerker ook zelf besluiten om stoute en soms strafbare handelingen te gaan verrichten. Bij dit verschijnsel, de medewerker die zelf besluit om onbevoegde handelingen te gaan verrichten, staan wij in dit vierde artikel van de serie over insider threat stil.

Fraudedriehoek Bij het verklaren van het 'waarom' bij onbevoegde en soms zelfs strafbare handelingen uitgevoerd door medewerkers is de zogenaamde fraudedriehoek een handig hulpmiddel. Om de grens over te stappen, en gedrag te gaan vertonen dat als niet integer wordt gezien, zijn er drie factoren die volgens de theorie van de fraudedriehoek een rol spelen. De medewerker moet als eerste de gelegenheid hebben of krijgen om iets te doen wat eigenlijk niet de bedoeling is. Daarnaast is het ook belangrijk dat de medewerker de motivatie moet hebben, en soms zelf de noodzaak moet voelen, om een onbevoegde handeling uit te voeren. Als laatste zal de medewerker de handeling ook moeten kunnen rationaliseren, wat wil zeggen dat hij of zij de handeling voor zichzelf kan rechtvaardigen. Twee factoren die de keus van de medewerker ook beïnvloeden om de grens over te stappen, en die daarom in dit artikel ook worden benoemd, zijn de bedrijfscultuur en de zogenaamde tone-at-the-top van het management. De geschiedenis heeft ons immers geleerd dat goed gedrag, en helaas ook minder goed gedrag, door de medewerkers vaak wordt gevolgd en als excuus wordt gebruikt.



Gelegenheid Bij de gelegenheid om onbevoegde handelingen uit te voeren, zoals die vaak vanuit de fraudedriehoek omschreven wordt, is het centrale woord 'kans'. De vraag die de medewerker voor zichzelf moet beantwoorden is 'hoe groot is de kans als ik iets doe wat niet mag om daarmee weg te komen?'. Hoe makkelijk is het om bijvoorbeeld wat spullen uit het magazijn mee te nemen zonder dat het opvalt? Kans is in deze context dus eigenlijk de 'pakkans' die de medewerker vooraf ervaart. De pakkans bij diefstal of fraude gepleegd door medewerkers is veelal direct te relateren aan de controlemechanismes die een organisatie heeft geïmplementeerd. Als het niet opvalt dat bedrijfseigendommen verdwijnen, omdat er geen goede administratie is en eigenlijk niemand weet wat de voorraad zou moeten zijn, dan is het aanneembaar dat een medewerker een zeer lage pakkans zal ervaren. Bovendien kunnen er ook verschillen optreden binnen een bedrijf. Op bepaalde onderdelen kan er een sluitende controle en goede administratie aanwezig zijn, terwijl deze op andere plekken ontbreekt. Zo zal in een ziekenhuis de controle op en de administratie van aanwezige medicijnen prima in orde zijn terwijl, als het cam-

ers over de grens?



pingseizoen begint, toch het bestek uit het bedrijfsrestaurant op onverklaarbare wijze vermindert. Het gaat bij gelegenheid daarom vaak niet alleen om de pakkans, maar ook om de verwachte gevolgen mocht de medewerker tegen de lamp lopen. Een vork of een mes minder in het bedrijfsrestaurant is niet erg. Toch? hoek beschreven wordt, de druk die de medewerker ervaart om iets te doen. Als een medewerker financiële problemen heeft, zoals bijvoorbeeld grote schulden die hij of zij eigenlijk niet meer kan aflossen of een verslaving die veel geld kost, dan is het niet verstandig om deze medewerker handelingen te laten uitvoeren waar contant geld bij aanwezig is. Of om die medewerker te laten werken op een afdeling waar hij of zij overboekingen kan doen en de administratie kan manipuleren. Dat is de kat op het spek binden. Het lastige is alleen dat organisaties vaak niet weten of een medewerker de motivatie heeft, of de daadwerkelijke noodzaak ervaart, om onbevoegde handelingen uit te voeren. Nog steeds worden bedrijven verrast door fraude en diefstal. Hoe vaak horen wij niet dat het zo een goede medewerker was, vader of moeder van twee lieve kinderen, die al meer dan twintig jaar bij de organisatie werkte. En er was nooit iets aan de hand. Dit roept dan, als er wat afstand van de casus genomen wordt, wel meteen de vraag op hoe goed de organisatie haar medewerkers nog kent?

Bij rationalisatie gaat het er om dat de medewerker zijn of haar onbevoegde handeling voor zichzelf kan rechtvaardigen.

Motivatie Naast dat de medewerker de kans moet hebben om een onbevoegde handeling uit te voeren zal hij of zij ook de noodzaak moeten voelen om dat te doen. De noodzaak is, zoals die vaak in het kader van de fraudedrie-

Vaak zijn medewerkers in deze tijd toch niet meer dan een (tijdelijk) personeelsnummer. Zeker als de menselijke maat binnen het bedrijf of de instelling is verdwenen neemt de motivatie toe om een greep uit de kas te doen, zeker bij ▸



persoonlijke problemen die onoplosbaar lijken. Om terug te grijpen op de indicatoren zoals die in het 'Report to the Nations on Occupational Fraud and Abuse' staan beschreven, weet de organisatie het als die zich voordoen bij een medewerker? Vaak niet, want op dit moment is het begrip 'privacy' zelfs een excuus om zich als werkgever niet meer op individueel vlak met de medewerker en zijn of haar persoonlijke problemen bezig te houden. Dat levert echter wel een risico op.

Rationalisatie Bij rationalisatie gaat het er om dat de medewerker zijn of haar onbevoegde handeling voor zichzelf kan rechtvaardigen. De kans is er om wat geld of goederen mee te nemen. De noodzaak is er ook, want de medewerker heeft privé de nodige problemen en heeft acute geldproblemen. Het enige wat de medewerker nu nog nodig heeft is een goed argument om zijn gedrag te rechtvaardigen. Veel gehoorde argumenten liggen vaak op het vlak van 'er is mij jarenlang een promotie onthouden terwijl andere collega's wel volop kansen kregen', of 'mijn leidinggevende zorgt prima voor zichzelf en neemt ook af en toe wat dingen mee naar huis en last but not least 'iedereen neemt toch wel eens iets van het bedrijf mee'. Natuurlijk zijn er nog veel meer rechtvaardigingsgronden te bedenken, maar belangrijk is dat de voor het insider threat programma verantwoordelijke functionaris zich realiseert dat door medewerkers ervaren relatieve deprivatie vaak de noodzakelijk rechtvaardiging geeft om de grens over te stappen. Met relatieve deprivatie wordt in deze context bedoeld dat een medewerker van mening is dat hem of haar ten onrechte iets is onthouden terwijl 'anderen' binnen de organisatie dat wel krijgen. Dit kan liggen op het vlak van promoties, beloningen, bonussen of zelfs kan het zo simpel zijn dat de medewerker van mening is dat hem of haar een complimentje wordt onthouden.

Bedrijfscultuur Als het om gelegenheid of rationalisatie gaat is er, zeker binnen bedrijven die veel met fraude en derving te maken hebben, vaak wel een relatie met de bedrijfscultuur te leggen. De medewerker die zich daar aan strafbare feiten schuldig maakt is niet opgevallen op het moment dat hij of zij zijn onbevoegde handelingen pleegde. Of eigenlijk, de indicatoren zijn wel waargenomen maar niemand heeft er iets mee gedaan. Achteraf horen wij namelijk altijd 'ik wist het wel' of 'ik vond zijn of haar gedrag wel vreemd'. Hoe komt het dan toch dat niemand verantwoordelijkheid heeft genomen om iets te zeggen of te vragen? Het antwoord is vaak even simpel als ook ontluisterend: niemand voelde zich verantwoordelijk. Een problematische bedrijfscultuur, waar medewerkers een nummer zijn geworden voor het (top)management en waar het motto is 'ieder voor zich en god voor ons allen', heeft hoger risico op insider threat dan een organisatie met een familiegevoel. Dit is wel iets om rekening mee te houden als besloten wordt om een insider threat programma te gaan ontwikkelen en implementeren. Daarbij is de tone-at-the-top erg belangrijk. Medewerkers zijn niet gek. Als het (top)management in de nieuwjaarstoespraak over 'wij' spreekt, en de nadruk ligt op samenwerking, maar de medewerkers zien dat niet terug in voorbeeldgedrag, dan maakt dit het voor de medewerker gemakkelijk om zijn of haar eigen 'niet integere gedrag' te rationaliseren. Wij, als medewerkers, staan al jaren op de nullijn en er is geen budget voor een afdelingsuitje. Het (top)-management krijgt bonussen en organiseert leuke feesten voor zichzelf. Waarom zou ik ook af en toe niet even iets voor mijzelf mogen meenemen? Vanuit de organisatie krijg ik niet eens meer een kerstpakket. Herkenbaar?

Een greep in de kas door een medewerker. Hadden wij dit niet kunnen zien aankomen?

Vervolg Nu mag bedrijfscultuur nooit een reden zijn voor een medewerker om strafbare (onbevoegde) handelingen te gaan verrichten. Helaas levert een bedrijfscultuur wel argumenten aan de medewerker, zeker met de fraudedriehoek in het achterhoofd, om de grens over te stappen. Daar zal, als de organisatie het onderwerp insider threat wil adresseren, wel rekening mee gehouden moeten worden. In het laatste artikel van deze serie, april 2018, wordt het insider threat profiling programma beschreven dat noodzakelijk is om alle geïdentificeerde bedreigingen tijdig te onderkennen waarbij de werkgever de in het Burgerlijk Wetboek opgelegde verplichting nakomt om voor een veilige werkomgeving te zorgen.

■ Berndt Rif MSc MBA MSec
Redactie@beveiliging.nl