Wat als uw medewerker kwe door criminelen?

deel 3

Waarom zou een criminele organisatie, een terroristische organisatie of een (buitenlandse) inlichtingendienst de moeite nemen om binnen uw organisatie te infiltreren als uw organisatie al kwetsbare medewerkers in dienst heeft die gemakkelijk te rekruteren zijn? Een interessante medewerker is wellicht al kwetsbaar, of kan kwetsbaar worden gemaakt, waardoor er 'alleen' nog even op het goede knopje gedrukt hoeft te worden om uw organisatie in het hart te treffen.

Zelfs de meest integere medewerker kan, als de druk maar op de juiste wijze wordt opgevoerd, kwetsbaar worden en door kwaadwillenden als instrument worden ingezet. De huidige wijze van pre-employment-screening en in-employment-screening, gebaseerd op het kijken naar gedrag in het verleden en integriteit in het verleden, geeft geen enkele weerstand tegen professionele organisaties die gebruik maken van kwetsbaarheden van medewerkers in het heden. Door het niet hebben van een programma voor 'insider threat profiling' lopen organisaties dus grote risico's.

First time De klassieke manier van pre-employment-screening is, als er ook geen in-employment-screening plaatsvindt, eigenlijk zonde van zowel tijd als geld. Zeker als wij ons realiseren dat circa 85 procent van de incidenten met medewerkers, waar het instrument screening weerstand tegen moet bieden, veroorzaakt wordt door 'first time offenders'. Als de basis van een screeningsprogramma dan ook nog rust op de pijlers 'gedrag in het verleden' en 'integriteit', zal de domme crimineel die in het verleden al een keer tegen de lamp is gelopen wel opvallen. Maar professionele kwaadwillenden kunnen ook een kwetsbare medewerker rekruteren die nog nooit iets verkeerds heeft gedaan. Voor sommige organisaties zal dat een geaccepteerd risico zijn, zeker als budgetten niet toereikend zijn om een insider threat profiling-programma te implementeren. Organisaties met een hoger risicoprofiel, omdat zij bijvoorbeeld voor kwaadwillenden interessante informatie of waarde bezitten, moeten zich dus goed afvragen of de huidige wijze van screenen nog voldoende waarborgen geeft. Een veel gehoord argument om niet over te gaan op het kijken naar kwetsbaarheden bij medewerkers als onderdeel van een screening is dat 'het een grote inbreuk op de privacy geeft'. Maar is dat wel zo? Of roepen de juristen, waar wij vakinhoudelijk mee te maken hebben, maar wat omdat er nog geen goede uitleg is gegeven waarom screening noodzakelijk is?

Juridisch kader Laten wij eens kijken naar het Burgerlijk Wetboek (Boek 7, Artikel 658). Daarin staat met zoveel woorden dat de werkgever verplicht is om 'zodanige maatregelen te tref-

Management-summary

De werkgever is wettelijk verplicht om zijn werknemers een veilige werkomgeving te bieden. Dat betekent feitelijk ook dat de werknemer beschermd moet worden tegen criminelen die het op hem of haar hebben voorzien, vanwege de bevoegdheden van de werknemer binnen de organisatie. De werknemer kan bijvoorbeeld chantabel zijn of worden gemaakt om zo gedwongen te worden bedrijfsgeheimen prijs te geven. Met pre- en in-employment-screening zijn kwetsbaarheden aan het licht te brengen waarvan criminelen gebruik zouden kunnen maken. Op deze wijze wordt dus in belangrijke mate bijgedragen aan een veiligere werkomgeving.



e tsbaar is voor rekrutering



fen' die redelijkerwijs nodig zijn om te voorkomen dat de werknemer bij de uitoefening van zijn taken schade lijdt. De werkgever is bovendien aansprakelijk 'jegens de werknemer' als die werknemer in de uitoefening van zijn werkzaamheden schade lijdt, tenzij de werkgever aantoont dat hij de verplichting om voor een veilige werkomgeving te zorgen is nagekomen. Dit is dus heel interessant. Neem een bij een organisatie werkzame professional, die verantwoordelijk is voor screening. Deze mag niet naar kwetsbaarheden van werknemers kijken, omdat dit een zogenaamde te grote inbreuk op de privacy maakt. Het mag dus ook niet als het bedoeld is om een medewerker te beschermen tegen kwaadwillenden die medewerkers willen rekruteren door van dergelijke kwetsbaarheden gebruik te maken. Dan gaat de wereld er ineens heel anders uitzien. De medewerker wordt ontslagen wegens 'het lekken van informatie'. Dit lekken gebeurde echter omdat hij onder druk werd gezet door een criminele organisatie vanwege bepaalde kwetsbaarheden die bij de werkgever bekend hadden kunnen zijn. De medewerker kan dan ineens zijn werkgever aansprakelijk stellen omdat deze niet voor een veilige werkomgeving heeft gezorgd.

Interessante vraag Daarnaast kan er de vraag gesteld worden over de afweging tussen het belang van de veiligheid van de organisatie (lees: de overige medewerkers) versus de eventuele inbreuk op de privacy van de medewerker. Zeker indien deze medewerker als onderdeel van dezelfde groep wellicht mag verwachten dat zijn/haar veiligheid op eenzelfde wijze geborgd wordt. En iedere keer dat er een nieuwe casus bijkomt, die laat zien hoe onze tegenstanders te werk gaan bij het rekruteren van medewerkers (criminele organisaties, terroristische organisaties en buitenlandse inlichtingendiensten), hoe lastiger het voor een werkgever wordt om te zeggen 'ik had het wel kunnen weten, maar ik ben bewust niet op zoek gegaan naar door kwaadwillenden te gebruiken kwetsbaarheden van mijn medewerkers, want dat is een te grote inbreuk op de privacy'. De interessante vraag is dan: was de rekrutering geen grote inbreuk op de privacy? En het ontslag? Heeft dat geen gevolgen voor de persoonlijke levenssfeer van de werknemer die al 35 jaar bij de organisatie werkte?

Kwetsbaarheden Als het gaat om het creëren van een veilige werkomgeving, naar welke kwetsbaarheden zou er binnen een pre-employment en in-employment screening-programma dan gekeken moeten worden? En waarom moet daar naar gekeken worden? Om met het laatste te beginnen: niet om sollicitanten af te wijzen of bestaande medewerkers te ontslaan, maar juist om deze groep weerbaar te maken. Door het bespreekbaar maken van kwetsbaarheden en het laten zien hoe kwaadwillenden daar gebruik van kunnen maken, wordt de werksituatie veiliger. Als de betreffende medewerker, of sollicitant, ziet dat een kwetsbaarheid niet tot ontslag, respectievelijk afwijzing leidt, zal deze persoon ook loyaler worden ten opzichte van de organisatie. Dit geeft een win-win-situatie. De vraag blijft dan nog wel naar welke kwetsbaarheden de werkgever moet kijken tijdens een pre-employment of in-employment-screening. Dat antwoord is simpel. Naar die kwetsbaarheden waar kwaadwillenden aantoonbaar gebruik van (kunnen) maken. In het kader van dit artikel worden de drie belangrijkste kwetsbaarheden besproken.

Persoonlijke problemen Het 'Report to the Nations on Occupational Fraud and Abuse', wat de Association of Certified Fraud Examiners iedere twee jaar publiceert, geeft aan wat de kwetsbaarheden zijn die aanwezig waren bij gerapporteerde incidenten wereldwijd. Het laatste rapport uit 2016 is, voor wat betreft de beschreven kwetsbaarheden, ▸



redelijk consistent als ook naar de eerdere acht publicaties wordt gekeken. Persoonlijke problemen waaronder wijzigingen in de huiselijke sfeer, zoals scheidingen, zijn een kwetsbaarheid waardoor medewerkers in de verleiding kunnen komen om verkeerde dingen te gaan doen. Dit is ook, als naar casussen op het vlak van rekrutering gekeken wordt, een kwetsbaarheid waar misbruik van gemaakt wordt door kwaadwillenden. Als een werknemer, die in een dergelijke situatie verkeert, door zijn kwetsbaarheid een target kan worden voor kwaadwillenden in het kader van zijn functie binnen de organisatie heeft de werkgever dus, omdat hij dat had kunnen en moeten weten, een taak als het gaat om het creëren van een veilige werkomgeving. Of niet? Interessant voer voor juristen in het kader van aansprakelijkheid.

Financiële problemen Problemen in huiselijke sfeer kunnen ook vaak financiële problemen tot gevolg hebben. Een medewerker die geld nodig heeft is een makkelijke prooi voor kwaadwillenden die hem of haar aan geld kunnen helpen. Ook op dit punt komt dan weer de vraag naar voren: als deze kwetsbaarheid een risico geeft op basis van het functieprofiel en de toegang tot informatie bij de organisatie, welke verantwoordelijkheid heeft de werkgever dan als het gaat om het beschermen van zijn of haar medewerker? Een passend antwoord is er niet, al is het alleen maar omdat dat een niet te ontdekken pad is wat als uitgangspunt heeft het beschermen van de medewerker tegen rekrutering uit hoofde van zijn functie bij de organisatie. Onderdeel van de pre-employment en inemployment-screening zal dan in ieder geval een financiële check moeten zijn waarin gekeken wordt naar de vraag of het inkomstenpatroon en uitgavenpatroon in overeenstemming zijn. Ook het kijken naar 'schulden' maakt dan deel uit van het onderzoek.

Verborgen geheimen Het meest gevoelige onderwerp is altijd de door medewerkers verborgen gehouden kwetsbaarheden. Kwaadwillenden die een medewerker willen rekruteren, en bereid zijn om daar geld en tijd aan te besteden, vinden de 'geheimen' altijd. Er zijn ook casussen waaruit blijkt dat medewerkers in een compromitterende positie worden gebracht juist om het geheim, waar druk mee kan worden uitgeoefend, te creëren. Als een medewerker, vanwege zijn positie, dermate interessant is voor kwaadwillenden, wat doet de organisatie er dan aan om die medewerker tegen dergelijke acties te beschermen? Ook op deze vraag zal een insider threat profiling-programma antwoord moeten geven. Vergeet daarbij niet dat de insteek nog steeds is dat de werkgever de verplichting heeft om voor een veilige werkomgeving te zorgen. Het gaat dus niet om het afwijzen van sollicitanten of het ontslaan van medewerkers met een vuiltje, maar om het weerbaar maken van werknemers tegen dreigingen die kwetsbaarheid uitbuiten. Uiteindelijk heeft de professional, die zich met screening bezighoudt, geen moreel oordeel over gedrag zolang dit niet strafbaar is. Wat iemand in zijn vrije tijd doet is voor eigen rekening en ook eigen keuze. Belangrijk is wel dat er geen misbruik van 'gedrag' gemaakt kan worden omdat de werknemer er met niemand over kan praten. Ook hier ligt dus een taak voor de werkgever voor wat betreft het creëren van een veilige werkomgeving.

Vervolg Als de werkgever had kunnen en moeten weten dat kwaadwillenden gebruik maken van kwetsbaarheden van werknemers, om deze werknemers te rekruteren gezien de positie die zij binnen het bedrijf innemen, dan heeft de werkgever op basis van het Burgerlijk Wetboek een verplichting om deze werknemers te beschermen. Antwoorden hoe deze verplichting precies zijn vertaling moet krijgen richting een pre-employment en in-employment-screening zijn niet te geven. Dit zal per bedrijf en per risicoprofiel verschillen.

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

In december wordt in het volgende artikel van deze serie stilgestaan bij de medewerker die zelfstandig besluit om onbevoegde handelingen te gaan verrichten. Hoe kan dit risico tijdens een screening tijdig worden onderkend? In het laatste artikel van deze serie, maart 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.