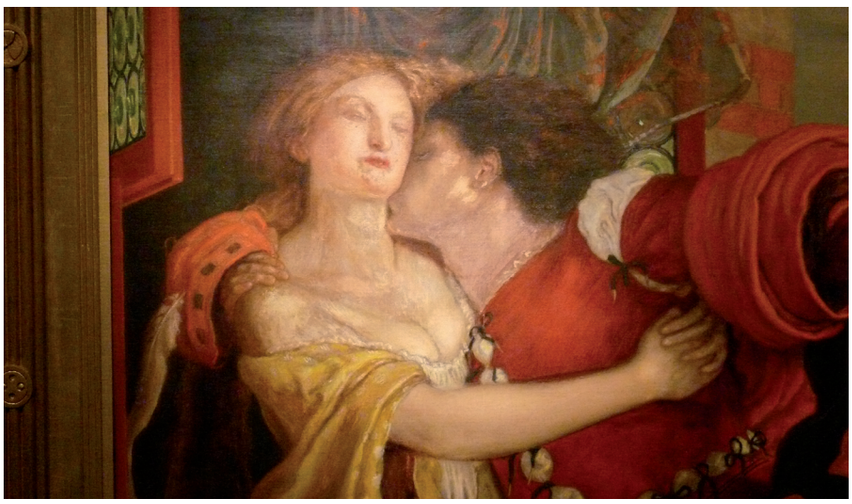
deel 4

Zakenreiziger onbewust mik

Zelfs de zakenreiziger of toerist die een veilig land zoals Groot-Brittannië bezoekt, loopt kans op ongewenste belangstelling van inlichtingendiensten. Wie denkt dat dit geen kwaad kan, onderschat de ernst van de problematiek. Veiligheid is natuurlijk een valide reden om communicatiekanalen en gegevensdragers te onderzoeken, maar soms staan er meer belangen op het spel. Ook in Groot-Brittannië en andere 'bevriende' landen.

Pierre Maron, voormalig topman van de Franse inlichtingendienst DGSE maakte er in het verleden al geen geheim van. Bevriende landen bestaan niet, landen hebben hoogstens 'tijdelijke' gemeenschappelijke belangen. Als de belangen wijzigen is de vriendschap over. De afgelopen jaren waren er duidelijke voorbeelden van bevriende landen, die op het oog gemeenschappelijke belangen hebben, maar intussen wel elkaar en elkaars staatshoofden bespioneerden. Een ieder die zich daarover verbaasd heeft, heeft zijn huiswerk niet goed gedaan.

Economisch welzijn Veel partijen zijn er echter redelijk transparant over. Heeft uw bedrijf concurrenten in Groot-Brittannië? Lees dan eens op de website van MI6 wat hun taakstelling is. Op de website staat namelijk, alsof het de gewoonste zaak is, dat het zorgen voor het 'economische welzijn' van het Verenigd Koninkrijk onderdeel van hun opdracht is. En dan de controle bij het inreizen van mobiele telefoons en laptops van Europese zakenmensen die naar de Verenigde Staten reizen. Zal dat nu echt plaatsvinden vanwege de terroristische dreiging? Gelukkig hoeft u zich geen zorgen te maken als uw telefoonaanbieder zijn servers in Canada heeft staan. Daarvan staat de data immers al op Noord-Amerikaanse bodem zodat de Amerikaanse overheid daar redelijk makkelijk bij kan komen. Zou dat misschien de reden zijn waarom de Franse overheid in 2007 al het gebruik van bepaalde telefoonmerken verboden heeft voor ambtelijke organisaties? En dan te bedenken dat tot op dit moment er alleen nog maar gesproken is over 'bevriende naties'. Landen die in de jaarverslagen van de Westerse veiligheidsdiensten worden genoemd en zonder politieke consequenties mogen worden bestempeld als 'de vijand', vallen nog buiten beschouwing. Hoe dan ook, de conclusie dat een medewerker op dienstreis informatie bij zich heeft die interessant kan zijn, kan zonder probleem getrokken worden. De vraag blijft wel of die medewerker zich dat bewust is. Heeft zijn werkgever eigenlijk wel de noodzakelijke maatregelen genomen om te voorkomen dat informatie in het nabije buitenland gecompromitteerd wordt?



Romeo en Julia Is spionage een oude dreiging in een nieuw jasje? Of toch niet? De oude boeken over spionage en de werkwijze van inlichtingen- en veiligheidsdiensten zouden eigenlijk verplichte literatuur moeten zijn voor security managers en studenten die security management studeren. Soms lijkt het er wel op dat de hedendaagse 'wereldburger' enigszins naïef is geworden. Tijdens congressen en seminars is het heel leerzaam om in een bar van het hotel te gaan zitten en te observeren. De Westerse zakenman zit dan gezellig aan de bar, soms alleen en soms in het gezelschap van collega's. Hij gaat helemaal op in gesprekken met andere barbezoekers. En dan ineens komt 'Julia' binnen, of soms ook 'Romeo', en begint het spektakel. Geanimeerde gesprekken, waarbij ook de nodige wijn wordt geschonken, zorgen voor een leuke avond. Hoe vaak hoor je dan niet 'ik heb zo leuk zitten praten' en 'Julia' (of Romeo) was 'echt geïnteresseerd in wat ik nu precies

punt van spionagediensten?



voor werk doe'. Soms krijgt het leuke gesprek ook nog een vervolg op de hotelkamer. Tenminste, daar mag je vanuit gaan als twee mensen de hotellift instappen terwijl er één zeker geen kamer in het hotel heeft. Dan, jaren later, is er 'ineens' die mooie 'Polaroid'-foto. Bij het zien van zo'n tafereel komt altijd weer die scène uit Flodder naar boven: 'Wilt u de auto betalen met cash of met creditcard?' En dan is het antwoord: 'Nee, met Polaroid.'
Uiteraard zijn het zeker niet alleen de mooie, macho of charismatische types die dit spionagewerk doen. Juist, en misschien nog wel vaker, gaat het om onopvallende types met een alledaags uiterlijk of voorkomen. Mensen waar je makkelijk langs kijkt worden voor deze doeleinden ingezet. Om een lang verhaal kort te maken, de oude werkwijze om aan informatie te komen wordt nog steeds gebruikt. Het is alleen nog lastiger geworden om tijdig te onderkennen dat de medewerker doelwit is van kwaadwillenden die informatie willen stelen omdat de oude beproefde werkmethoden nu ook ondersteund worden door gebruik van techniek. Echter door de huidige techniek blijkt het steeds lastiger te zijn informatie op computers geheim te houden. De menselijke factor blijft daarmee nog steeds enorm belangrijk.

Onderweg Inlichtingen- en veiligheidsdiensten weten veelal al lang voordat iemand afreist dat hij of zij onderweg is. Voor de overheidsdiensten mag ook de hedendaagse professionele criminele organisatie gelezen worden. Sommige hedendaagse criminele organisaties hebben al bijna dezelfde middelen en mogelijkheden om zichzelf toegang te verschaffen tot informatie als de reguliere overheidsdiensten. Kunt u zich, vanuit travel security, beveiligen tegen het weglekken van informatie over reisbewegingen van uw medewerkers? Het antwoord daarop is eigenlijk negatief.
In veel systemen van luchtvaartmaatschappijen, hotels en soms ook lokale taxibedrijven staan uw medewerkers, voorzien van aankomst en vertrekdatum, met naam en toenaam genoemd. Een creditcard op naam van het bedrijf maakt de herkenbaarheid voor kwaadwillenden zelfs nog iets beter. En wat dacht u van het huidige social media-gebruik van de gemiddelde burger? Wat kunt u dan doen om uw medewerker goed voor te bereiden op de dreiging van spionage? Het toverwoord is voorlichting. Belangrijk is dat uw medewerker weet, en nog beter, beseft wat hem of haar mogelijk te wachten staat en wat de indicatoren zijn waaraan herkend kan worden dat een gesprekspartner op informatie uit is (of erger). Daarnaast is het belangrijk, als uitvloeisel van het informatiebeveiligingsbeleid van uw organisatie, om voor een dienstreis te bepalen welke informatie wel of niet gecompromitteerd mag worden. Gaan de smartphone en laptop mee naar het buitenland? Dan mag de security manager er vanuit gaan, als de medewerker een target was, dat alle informatie(bronnen) waar deze apparaten toegang toe geven gecompromitteerd zijn. Dit is, zo zal een ieder begrijpen, een leuke uitdaging voor de security manager om dit aan het (top)management van het bedrijf te vertellen. Het (top)management wil namelijk maar één ding: de smartphone meenemen.

Welkomstcomité De medewerker die 'voor aankomst' is geïdentificeerd als 'interessant' mag zich verheugen op een echt welkomstcomité. Nadeel is alleen dat het comité zich niet zal voorstellen. Dit maakt training en voorlichting van medewerkers, ook als zij met gevoelige informatie naar zogenaamde bevriende landen reizen, erg belangrijk. Het probleem is alleen dat vanwege het ontbreken van een referentiekader over dit onderwerp, want spionage is immers een onderwerp uit de periode van de Koude Oorlog, voorlichting al snel gezien wordt als 'spannend' verhaal. Vaak gehoorde opmerkingen zijn dan dat de dreiging sterk overdreven wordt, of dat de medewerker best 'voor zichzelf kan zorgen'. 'Nu was die meneer of mevrouw naast mij in het vliegtuig wel te vertrouwen, ik vloog immers met een Westerse maatschappij, maar de taxichauffeur die mij naar het hotel bracht niet', aldus een medewerker.
Het is goed dat iedereen zich weer ▸



herinnert dat Air France in het verleden betrapt is op het plaatsen van afluisterapparatuur in de businessclass en dat Boeing nog niet zo lang geleden aan een land in Azië een vliegtuig heeft afgeleverd vol met afluisterapparatuur. Deze voorbeelden maken duidelijk dat als een medewerker tijdens de reis al interessant is, het welkomstcomité echt zal staan te wachten. Belangrijk is dat de medewerker in ieder geval weet dat zoiets voorkomt en dat hij of zij dan weet wat wel en wat niet te doen. Het toverwoord is wederom voorlichting.

Verblijf Medewerkers die interessante informatie bij zich hebben, of die vanwege hun positie interessant zijn, moeten zich zeer bewust zijn van de technieken en tactieken die gebruikt worden door inlichtingdiensten, veiligheidsdiensten, criminele organisaties of een combinatie daarvan om op illegale wijze informatie te verkrijgen of om de integriteit van een persoon aan te tasten. Het verdient dan voorkeur om, waar mogelijk, niet alleen te reizen als medewerkers zich niet goed genoeg bewust zijn van de dreiging of als zij voor het eerst naar een voor hen onbekende locatie gaan. Belangrijk is ook dat medewerkers gevoelige informatie altijd bij zich houden. De kluizen in hotels zijn echt niet veilig. Als het hotelpersoneel een noodcode heeft om deze te openen, hebben de 'professionals' die informatie zoeken deze ook.
Daarnaast zijn er legio voorbeelden dat besproken informatie, soms via de telefoon en soms ook alleen tussen personen op een hotelkamer, uitlekt. Daar kan maar één reden aan ten grondslag liggen: afluisterapparatuur. En als er afluisterapparatuur op een hotelkamer geplaatst kan worden, dan is het plaatsen van een videocamera ook echt geen probleem. Op die manier wordt de oude vertrouwde Polaroid vervangen door een dvd'tje. Een recent voorbeeld hiervan is wat er in augustus 2016 gebeurde. In een hotel in Sydney waar het alom bekende All Blacks rugbyteam van Nieuw-Zeeland verbleef tijdens de Bledisloe Cup werd in de kamer van één van de All Blacks afluisterapparatuur gevonden. Moet de medewerker nu overal spoken gaan zien? Nee, beslist niet. Maar de security manager moet de medewerker voordat hij op reis gaat wel voorbereiden om mogelijke dreigingen en/of verdachte situaties te herkennen. Dit is natuurlijk ook weer afhankelijk van het land waar de reis naar toegaat. Daarnaast zal in sommige gevallen het bedrijf ook, als risico's duidelijk zijn, de eigen verantwoordelijkheid moeten nemen. Dat betekent bepaalde apparatuur niet meegeven of medewerkers niet alleen laten reizen.

■ Berndt Rif MSc MBA MSec, Redactie@beveiliging.nl
Miranda Coppoolse, M.Coppoolse@live.nl

