Mark Bergman

Ing. M. (Mark) Bergman RE CISSP CISA is gestart als zzp'er (zelfstandige zonder personeel), na ongeveer drieëneenhalf jaar bij KPMG te hebben gewerkt. Hij houdt zich onder meer bezig met IT-audits, *ethical hacking* en informatiebeveiligingsbewustzijn.

'Een cursist wil weten of ik ooit betrapt ben tijdens een klus'

Zondag 12 oktober, 22.00 uur

Het weekend is bijna voorbij en het voorbereiden van een dag *security awareness*-trainingen geven, begint weer. Samen met een collega geef ik trainingen bij een financiële instelling. Ik heb er zin in; de presentaties hebben als doel de medewerkers van de financiële instelling bewuster te maken van informatiebeveiliging. Mijn collega zal voornamelijk de theorie behandelen en ik vervul de fijne rol om gedurende de presentaties zoveel mogelijk voorbeelden uit mijn eigen praktijk aan te halen. Ik heb bijvoorbeeld veel opdrachten gedaan, waarbij ik door middel van *social engineering*-technieken (technieken om het vertrouwen van mensen te winnen en ze te misleiden) een pand van een klant binnendrong en gevoelige informatie probeerde te bemachtigen, meestal met succes. Uiteraard worden dergelijke onderzoeken alleen gedaan met expliciete toestemming van de klant.

Maandag 13 oktober, 8.30 uur

De wekker gaat relatief laat vandaag, want ik hoef pas om 9.15 uur op locatie te zijn om voorbereidingen te treffen voor de sessies. Ik besluit een onopvallend, donkerblauw pak aan te trekken. Meestal kies ik iets opvallends voor presentaties, maar je weet nooit of het vanwege de aard van de presentatie nuttig gaat zijn om niet op te vallen. Omdat ik maar een kwartier nodig denk te hebben voor mijn reis naar de klant, vertrek ik rond 9.00 uur. In de auto neem ik me nog stellig voor me netjes te gedragen, ik heb immers geen vrijwaringverklaring van de klant om het informatiebeveiligingsbewustzijn op de locatie te mogen testen, ik kom enkel voor een presentatie. Toch vallen mij ook op dergelijke dagen vaak veel zwakke plekken op, zonder dat ik deze mag benutten.

Zo tegen 9.15 uur staat de auto netjes geparkeerd en loop ik richting het pand waar ik moet zijn. Bij de voorgevel aangekomen, word ik door wat borden doorgestuurd naar de zijkant. Er is duidelijk een verbouwing gaande. Vriendelijk groet ik de twee beveiligers aan weerszijden van de openstaande deur, ik zet nog drie grote passen en een glimlach verschijnt op mijn gezicht. Deze glimlach wordt nog groter als ik me omdraai en zie dat ze een medewerker van de instelling vragen zijn pas te laten zien. Ik loop terug naar de beveiligers en vraag waar ik me als bezoeker moet melden. De heren kijken me wat verbaasd aan en een sputtert nog 'hoezo werkt u hier niet dan?'. Vervolgens word ik naar de receptie geleid door een van de beveiligers, die nog even toekijkt of ik me wel echt bij de balie aanmeld. Daarna haast hij zich weer terug naar de deur.

Als we rond 9.40 uur aankomen bij de zaal waar we zouden presenteren blijkt dat deze in gebruik is genomen door een ander team. Ik sluip naar binnen en krijg te horen dat de zaal zo vrij zal zijn, een meeting was een beetje uitgelopen.

Tegen 9.45 uur verzamelen de eerste deelnemers zich voor de zaal, de stemming lijkt wat nors, omdat ons publiek in eerste instantie geen zin heeft in een dergelijke verplichte sessie, mogelijk versterkt doordat het maandagochtend is. Onze voorgangers laten de zaal warm en muf achter en wij stromen met onze groep naar binnen. Uit ervaring weet ik dat de houding van de meeste mensen wel verandert na een paar leuke verhalen over wat we bij andere klanten hebben meegemaakt. Ruim een half uur later is het al raak: 'Meneer, leuk die verhalen maar dat gebeurt bij ons toch niet, wij hebben een goede beveiliging!'

Met een brede glimlach op mijn gezicht vertel ik hoe ik slechts een uurtje eerder langs de beveiliging ben gelopen en eigenlijk al in het pand stond zonder me eerst aan te melden. Vervolgens pak ik een stapeltje papier dat voor me op tafel ligt, nog van de vorige vergadering – het blijkt een presentatie*handout* te zijn vol met gevoelige informatie.

Vooral de ervaringen die ik heb opgedaan in de Verenigde Staten, waar ik samen met een Amerikaanse collega een social engineering- en ethical hackingtest deed, doen het ook deze keer weer goed. Bij die klant lukte het om drie dagen door de panden te lopen en gevoelige ruimtes te betreden,

zonder betrapt te worden. Zo rond 12.00 uur is de eerste sessie voorbij en het is, zoals altijd, goed om te zien dat de mensen zich toch weer hebben vermaakt.

Maandag 13 oktober, 12.00 uur

De pauze gebruik ik om wat te eten en een aantal telefoontjes te plegen. Ook na de pauze blijkt de zaal in gebruik te zijn, dit keer echter voor de rest van de middag. Vol verbazing bellen we de secretaresse van onze klant en ze wijst ons een andere zaal toe. Ik vang de mensen op bij de eerste zaal, terwijl mijn collega naar de andere zaal gaat. Een kwartier na de aanvangtijd loop ik ook naar de zaal en hoop ik maar dat er niemand meer dan een kwartier te laat zal komen. Dit keer is de sessie weer totaal anders; weliswaar gebruiken we dezelfde *slides,* maar het gaat om andere mensen en daardoor ook om andere voorbeelden. De voorbeelden die ik geef, selecteer ik namelijk niet vooraf, maar pas ik aan op de vraag of de situatie. Iemand wil weten of ik ooit betrapt ben tijdens een klus. Ik heb ooit een onderzoek gedaan bij een *telecom provider,* waarbij ik op weg naar buiten bijna werd betrapt, dus aan het einde van mijn test. Met veel moeite heb ik de beveiliging toen weten te overtuigen dat het om een flauwe grap ging. Vervolgens liet de beveiliging me toch lopen.

Deze groep heeft daarnaast erg veel vragen over het gebruik van USB-sticks en andere technische zaken. Ook hier hebben we genoeg ervaring mee, maar helaas zijn we beiden niet volledig op de hoogte van het beleid bij de klant om overal een sluitend antwoord op te hebben. Wel is ons tijdens deze sessie duidelijk geworden dat de beleidsstukken elkaar vaak tegenspreken. Zo mogen er geen USB-sticks gebruikt worden voor opslag, maar was er wel een omruilactie voor IT-middelen waarbij de medewerkers een USB-stick cadeau kregen als back-up-middel.

Maandag 13 oktober, 17.00 uur

De laatste deelnemers staan nog even na te praten, maar de sessies zitten er voor vandaag weer op. Ik herinner me mijn goede voornemen van deze ochtend en ga dus niet nog een rondje door het pand lopen, maar begeef me naar de uitgang. Ook op de terugweg neem ik mijn vaste sluiproute en om 17.30 uur ben ik weer heerlijk thuis. Daar verruil ik mijn pak voor wat vrijetijdskleding en klap ik mijn laptop weer open. Uren boeken, facturen schrijven en nog even kijken of de facturen van de maand augustus nu eindelijk betaald zijn. Ik verbaas me er nog even over dat klanten het een sport lijken te vinden om een betalingstermijn van 30 dagen op te rekken naar 45. Mijn vriendin is nog niet thuis, dus ik wandel nog even naar een supermarkt om voor het eten te zorgen.

Maandag 13 oktober, 19.30 uur

Het eten is op en de dag lijkt erop te zitten. Wel pak ik nog even mijn tas in. Ik heb een klant in de provincie Groningen waar ik vier dagen in de week werk. Dit betekent dat morgen mijn wekker om 06.15 uur gaat en ik hoop dan voor 8.30 uur in de buurt van Groningen te zijn. Pas vrijdagavond rond 20.00 uur zal ik weer thuis zijn. ■