HOE DE ZES GEHEIMEN VAN HET OVERTUIGEN DE MYSTERY GUEST HELPEN

Steeds meer organisaties zien de bewustwording van medewerkers als een belangrijk onderdeel van informatiebeveiliging. Eén manier om een bijdrage te leveren aan awareness is door de inzet van een social engineer(1). In de praktijk krijgt deze social engineer vaak de titel 'mystery guest'. Dit artikel gaat in op de theorie van Cialdini en laat met voorbeelden zien hoe de mystery guest de psychologie van overtuiging in de praktijk inzet.

Wat is het doel van een mystery guest?

Bij een mystery guest-aanval wordt op verzoek van een opdrachtgever een locatie gecontroleerd aangevallen. Een mystery guest-aanval kan verschillende doelen hebben:

- inzicht krijgen in de mate waarin een bepaald doelobject weerstand kan bieden aan pogingen om onbevoegd toegang te krijgen tot bedrijfsmiddelen. Een doelobject kan bijvoorbeeld een fysieke locatie, een informatiesysteem of de paspoortenkluis zijn;
- meten van het huidige niveau van de weerbaarheid tegen social engineering;
- verhogen van de bewustwording van de medewerkers;
- meten van de effectiviteit van reeds genomen maatregelen;
- verkrijgen van inzicht in te nemen maatregelen;
- vergaren van (beeld)materiaal voor verdere bewustwordingscampagnes.

Om deze doelen te bereiken, maakt de mystery guest gebruik van de zes principes van Cialdini.

Zes overtuigingsprincipes van Cialdini

'Een brutaal mens heeft de halve wereld', zo luidt een oud spreekwoord. Natuurlijk moet een mystery guest over brutaliteit en lef beschikken: het is spannend om aan te vallen! Echter, van een mystery guest wordt meer gevraagd dan brutaliteit alleen, anders zou hij snel tegen de lamp lopen. Het doel van een mystery guest is om mensen te beïnvloeden tot het vrijgeven van informatie of het uitvoeren van handelingen. Met andere woorden: zaken die onder normale omstandigheden niet zouden gebeuren.

Robert Cialdini is hoogleraar psychologie en auteur van het boek 'Invloed: de zes geheimen van het overtuigen'. In dit boek presenteert hij zes wetenschappelijk onderbouwde overtuigingstechnieken uit de sociale psychologie. Deze technieken worden niet alleen gebruikt in de marketing, maar worden ook veelvuldig ingezet door mystery guests.

Figuur 1 – Overtuigen.

Wederkerigheid

Bij wederkerigheid maakt de mystery guest gebruik van het principe 'geven en nemen'. Wanneer jij iets voor een andere persoon doet, is deze sneller geneigd iets voor jou terug te doen. Dit geldt extra zwaar in het geval van een ongevraagde gunst. Dan ontstaat een schuldgevoel bij de ontvanger van de ongevraagde gunst, dat ertoe kan leiden dat deze persoon eerder in zal stemmen met het doen van een gunst die groter is dan de gunst die hij zelf heeft ontvangen.

"Als galant persoon houd ik de deur voor iedereen open. Natuurlijk vooral de deuren die niet zijn afgesloten. Ik doe dit om te zorgen dat een medewerker de volgende deur, die wel afgesloten is, voor mij open doet. Dit is meestal het geval, want het zou toch onaardig zijn om dan ineens te vragen wat iemand komt doen."

"Ik doe mij graag voor als helpdesk-medewerker. Ik zeg tegen een medewerker dat zijn device kuren vertoont en hij misschien al zijn werk kwijt raakt, maar dat ik hem natuurlijk kan helpen om dit te voorkomen! Als de medewerker mij zijn wachtwoord geeft, los ik het op en kan hij snel weer

André van Soest en Patricia van Schaik werken als consultants informatiebeveiliging bij LBVD. Zij voeren opdrachten uit voor grote en kleine organisaties in allerlei branches. Als mystery guests voeren zij veel aanvallen uit en passen hierbij de principes van Cialdini toe. André en Patricia zijn bereikbaar via avansoest@lbvd.nl en pvanschaik@lbvd.nl.

verder werken. Medewerkers met minder technische kennis gaan snel overstag en zijn blij dat je hen helpt, want stel je toch eens voor dat ze hun werk kwijt zijn."

Commitment en consistentie

Vreemd genoeg hebben mensen over het algemeen een sterke drang naar consistentie. Als een persoon een bepaalde beslissing genomen heeft, dan blijft deze er vaak consistent mee, of dat nu verstandig is of niet. Verder zijn mensen geneigd om in toekomstige situaties te handelen naar keuzes die ze eerder in soortgelijke situaties hebben gemaakt. Dit principe uit zich bijvoorbeeld in het feit, dat indien mensen op meerdere opeenvolgende vragen 'Ja.' hebben geantwoord, de kans groter is dat zij de eerstvolgende vraag op dezelfde manier zullen beantwoorden.

"Ik zeg dat ik ingehuurd ben door de afdeling ICT, omdat er netwerkproblemen zijn en dat ik het probleem kom onderzoeken. Ik vraag aan de medewerker of hij ook last heeft van het trage netwerk. Als hij dit positief beantwoordt, laat ik een apparaatje zien (USB-keylogger) en vertel dat ik daarmee de netwerksnelheid kan meten en verbeteren. Dit zal het probleem van de medewerker oplossen. Ik vraag de medewerker om toestemming om het apparaatje aan te sluiten. Als het antwoord ook nu positief is, sluit ik het apparaatje aan en zeg dat de medewerker de PC moet afsluiten en weer moet inloggen. Mijn ervaring is dat de werknemer meewerkt, want hij heeft steeds meegewerkt en wil dat het probleem wordt opgelost. Hij heeft niet door, dat ik hiermee zijn gebruikersnaam en wachtwoord afvang."

"Ik gebruik het volgende principe om een medewerker af te leiden en zijn werkplek onbeheerd achter te laten, zodat een collega mystery guest toe kan slaan. De vraag 'Mag ik iets vragen?' wordt vrijwel altijd met 'Ja.' beantwoord. De vervolgvraag: 'Bent u bekend op deze gang?' heeft ook een grote kans om met 'Ja.' beantwoord te worden, aangezien de medewerker op de desbetreffende gang werkt. De derde vraag: 'Kunt u mij alstublieft laten zien waar de brandslang hangt?' zal waarschijnlijk ook positief worden beantwoord, wat maakt dat de medewerker onverwachts zijn werkplek verlaat. Mogelijk zonder de PC te vergrendelen en met vertrouwelijke documenten op het bureau. Nu kan de andere mystery guest toeslaan."

Sociale bewijskracht

Het derde principe speelt in op het feit dat als anderen iets doen, de kans groot is dat jij dit ook gaat doen. Niet alleen kinderen zeggen 'Maar hij deed het eerst!'. Het referentiekader van mensen, ook volwassen mensen, wordt beïnvloed door te kijken naar wat anderen (niet) doen of vinden. De effectiviteit van dit principe is mede afhankelijk van de onzekerheid van de medewerker.

"Ik vraag aan een medewerker of hij toegang tot de serverruimte heeft. Als hij daar positief op antwoordt, geef ik aan dat we alle kamers en ruimten hebben onderzocht op 'brandmelders, brandblussers en nooduitgangen'. Ik zeg dat collega's van de man daar al bij hebben geholpen en ik alleen nog moet kijken naar de voorzieningen in de serverruimte. Vaak loopt de medewerker mee naar de ruimte. Eenmaal in de ruimte kan de ene mystery guest bij de medewerker blijven en hem afleiden, terwijl de ander mogelijk malware kan installeren of een Raspberry PI kan plaatsen, zodat toegang vanaf buiten mogelijk is."

"Kan je de deur voor mij openen? Je collega heeft me net ook binnengelaten!"

"Wanneer we de specifieke opdracht krijgen om wachtwoorden te ontfutselen, maken we een lijst met fictieve wachtwoorden bij bestaande e-mailadressen. Deze lijst laten we aan medewerkers zien. Daarbij geven we aan dat hun collega's al wel hun wachtwoord hebben opgeschreven voor het onderzoek naar de kwaliteit van de wachtwoorden. Dit trekt de twijfelende medewerker vaak over de streep om toch zijn wachtwoord op te schrijven."

Sympathie

Een mystery guest wil mensen beïnvloeden tot het vrijgeven van informatie of het uitvoeren van handelingen. Het is dus belangrijk voor de mystery guest om mensen 'Ja' te laten zeggen. Cialdini stelt in zijn boek 'Influence', dat mensen eerder 'Ja' zeggen tegen personen die ze kennen en sympathiek vinden. Daarom maakt een mystery guest regelmatig gebruik van een aantal factoren die meer aantrekkelijk en sympathiek maken.

"Binnenkomen met een grote doos en zeggen: 'Ik heb mijn handen vol. Wil jij alsjeblieft even de deur voor mij openen? Mijn pas zit in mijn binnenzak.' Iedereen herkent de situatie dat je met volle handen voor een dichte deur staat en is graag behulpzaam."

hoe de zes geheimen van het overtuigen de mystery guest helpen

Fysieke aantrekkingskracht	Aantrekkelijke mensen zijn beter in het misleiden van mensen en het veranderen van de houding van mensen.
Gelijksoortigheid	Het blijkt dat mensen eerder geneigd zijn om in te gaan op een verzoek van iemand die net zo is als hijzelf.
Lof / vleierij	Het geven van complimenten kan sympathie opwekken. Een mystery guest past hier wel mee op, want als het voor de ander niet oprecht aanvoelt, kan het een tegengesteld effect hebben.
Vertrouwen	Wanneer het contact onder positieve omstandigheden plaatsvindt, kan herhaaldelijk contact de sympathie bevorderen.
Associatie	Wanneer je iemand wilt beïnvloeden, moet je de indruk wekken dat je op die persoon lijkt. Een social engineer zal zoeken naar overeenkomsten en hierop inspelen.

"Wanneer ik binnenkom, bied ik bij de receptie direct mijn excuses aan en zeg dat er vorige week al een inspectie heeft plaatsgevonden. Helaas zijn bij een computerstoring alle gegevens gewist, waardoor de inspectie over moet. Ik zeg zuchtend, dat het altijd gedoe is met de computers en vraag of ze het herkennen. Na dit praatje zeg ik, dat het niet nodig is om de facilitaire medewerker weer van zijn werk te houden om mij te begeleiden; als de receptiemedewerker mij toegang geeft, loop ik even snel door het gebouw, en is het zo geregeld."

"Ik houd van vleierij en zeg dingen als: 'Wat heb je een leuke bril of toffe schoenen."

"Ik rook al jaren niet meer, maar als mystery guest steek ik graag een sigaretje op. De rookplek is een makkelijke ingang; andere rokers doen altijd de deur voor je open."

"Ik doe er alles aan om mij te kleden als de mensen in de organisatie. Ik heb hiervoor diverse outfits; van bouwhelmen tot legerkleding en laboratoriumjassen. Eenmaal binnen groet ik iedereen op een vrolijke manier, alsof ik niets te verbergen heb. Het liefst eet ik mee in de kantine, daarna 'hoor je erbij'. Ik merk dat de gesprekken met mensen die mij in de kantine hebben gezien veel eenvoudiger gaan, en dat ik sneller mijn doel bereik."

Autoriteit

Autoriteit heeft alles te maken met gezag. Uit diverse onderzoeken is gebleken, dat mensen geneigd zijn om gehoor te geven aan autoriteit. In de meeste gevallen zonder daar zelf bij na te denken. Een mystery guest maakt veelvuldig misbruik van dit principe, ook bij de keuze van de dekmantel. Er wordt vaak voor een autoritaire dekmantel gekozen. Een bekend voorbeeld is het uitvoeren van een inspectie. Bij voorkeur in opdracht van een (nog hogere) autoriteit.

"Wanneer mensen assertief zijn en vragen of ik iets of iemand zoek, geef ik aan dat ik geen hulp nodig heb en bezig ben met een onaangekondigde inspectie. Na deze boodschap draai ik mijn lichaam af en ga door met waar ik mee bezig was. De meeste mensen schrikken van deze autoritaire reactie en vragen niet meer door."

"Ik noem vaak de directie van het desbetreffende bedrijf als opdrachtgever en zeg dat deze mij heeft ingehuurd om een inspectieronde uit te voeren. Ik zeg erbij, dat de directie heeft gevraagd om het te melden als mensen niet meewerken. De namen van de directie staan meestal op de website/LinkedIn-pagina van de organisatie en wanneer het nodig is, gebruik ik ze. Deze aanpak werkt het beste bij grotere organisaties. Ook dan is het zaak dat je wegblijft van de directievloer."

Schaarste

Bij dit principe zijn mensen geneigd om zaken die moeilijk(er) te verkrijgen zijn, waardevoller in te schatten. Ondanks dat dit principe door een mystery guest beduidend minder wordt toegepast dan de andere vijf principes, wordt het wel degelijk toegepast.

Bij het versturen van phishing e-mails wordt het principe veel gebruikt. Mensen zijn bereid persoonsgegevens af te staan, als ze kans maken op een aanbieding, concertkaartjes of een bijna uitverkocht product.

hoe de zes geheimen van het overtuigen de mystery guest helpen

Mystery guest	Wederkerigheid	Commitment	Sociale bewijskracht	Sympathie	Autoriteit	Schaarste
	6 overtuigingsprincipes van Cialdini					
Commercieel	+	+	+	+	++	+++
Overheden	+++	+++	++	+++	+++	++
Onderwijs	++	+	+	-	+	+

Legenda: - helemaal niet, + minst toepasbaar, ++ gemiddeld toepasbaar, +++ meest toepasbaar

Figuur 2 - Overtuigingsprincipes van Cialdini.)

"Wij sturen een phishing e-mail naar medewerkers, waarin staat dat de organisatie iets extra's wil doen voor de medewerkers vanwege hun inzet de afgelopen periode. Wij lokken de medewerkers met de mededeling dat er een beperkt aantal gratis kaarten beschikbaar is voor een theatervoorstelling in de buurt van de vestigingsplaats van de organisatie. Wil men gebruik maken van de aanbieding, dan dient men op de link te klikken voor meer informatie over data en voorwaarden."

"Door phishing USB-sticks op parkeerplaatsen te leggen, over hekken bij bedrijven te gooien, op te sturen of gewoon rond te laten slingeren, bereik je veel resultaat. Mensen willen de USB-stick hebben of kunnen hun nieuwsgierigheid niet bedwingen. In april 2017 hebben we een onderzoek gedaan met 25 USB-sticks; een derde daarvan is op zakelijke PC's/laptops aangesloten."

Cialdini versus mystery guest

In dit artikel hebben we met praktijkvoorbeelden laten zien hoe de mystery guest de psychologie van overtuiging inzet. In de afgelopen vijf jaar hebben we als mystery guests meer dan honderd aanvallen uitgevoerd bij verschillende organisaties. Op basis van de verkregen informatie hebben we in kaart gebracht of de toepasbaarheid van de overtuigingsprincipes van Cialdini voor alle organisaties hetzelfde is. Hiervoor hebben we de resultaten van deze principes vergeleken per branche. We maken daarbij een onderscheid tussen overheden, commerciële organisaties en onderwijs.

In figuur 2 is per branche onderzocht in welke mate wij de principes toepasten (hoe wordt een slachtoffer benaderd) en hoe effectief dit was. Hiervoor hebben wij per branche minimaal dertig bevindingenrapportages genalyseerd. De toepasbaarheid van de principes is weergegeven met een score per branche.

Conclusie

We concluderen dat tijdens het uitvoeren van de mystery guest-aanvallen alle principes van Cialdini zijn toegepast. Wij kunnen niet zeggen of andere social engineers deze principes op dezelfde wijze toepassen.

We hebben de overtuigingsprincipes effectiever kunnen gebruiken bij overheden dan bij commerciële organisaties. Dit kan te maken hebben met de dienstbaarheid van medewerkers die bij de overheid werken. De principes 'Wederkerigheid, Commitment, Sociale bewijskracht, Sympathie en Autoriteit' zijn effectiever bij overheden. 'Schaarste' is juist doeltreffender bij commerciële organisaties. Bij commerciële organisaties is het percentage medewerkers dat op een phishing e-mail klikt of een gevonden USB-stick in de computer prikt veel groter dan bij de andere branches.

Gebleken is dat in het onderwijs de principes het minst effectief zijn. Dit komt mogelijk, doordat het onderwijs een open cultuur heeft en erg toegankelijk is. Bij de meeste onderwijsinstellingen loop je direct naar binnen zonder dat men je aanspreekt of tegenhoudt. Dit draagt er, bijvoorbeeld, aan bij dat de principes 'Sociale bewijskracht en Sympathie' minder effectief zijn. Uit de analyse is gebleken, dat als scholen wel bewaking en toegangspoorten hebben, de principes 'Sociale bewijskracht en Sympathie' wel effectief zijn.

Referenties

(1) In dit artikel worden de social engineer en mystery guest aangeduid met hem/hij. Hiermee willen we de vrouwelijke social engineers/mystery guests niet tekort doen, ook zij zijn zeer succesvol.