Social engineering: de kunst van het misleiden

Ir. M.B. Paques CISSP CISA
is als adviseur werkzaam binnen het team 'IT Security en control' van KPMG IT Advisory. Hij houdt zich onder meer bezig met security testing, social engineering, technische security reviews en de beveiliging van nieuwe technologieën.

paques.matthieu@kpmg.nl

Ir. Matthieu Paques CISSP CISA

In een typische penetratietest (hacker test) wordt geprobeerd ongeautoriseerd toegang te krijgen tot systemen of data door misbruik te maken van technische kwetsbaarheden. De 'zwakste schakel' in de informatiebeveiliging blijft in een dergelijke test buiten schot, namelijk *de mens*. In toenemende mate blijkt deze 'schakel' het doelwit van aanvallers te worden. In de media wordt een groot aantal incidenten gerapporteerd waarbij deze aanvallen een rol spelen (security.nl). Reden genoeg om in het kader van een audit of een informatiebeveiligingsonderzoek ook deze 'schakel' aan een test te onderwerpen. Dit artikel beschrijft hoe dit 'hacken van mensen', ook wel 'social engineering' genoemd, in zijn werk gaat, gaat in op enkele praktijkvoorbeelden en behandelt maatregelen die tegen dergelijke aanvallen kunnen worden genomen.

Wat is een social-engineering test?

Door KPMG IT Advisory worden voor een groot aantal klanten social-engineering opdrachten uitgevoerd. Bij een dergelijke test is het doel tweeledig:

- de risico's voor de onderzochte organisatie in kaart te brengen;
- de medewerkers bewust maken van deze risico's (training).

Tijdens de testen wordt geprobeerd medewerkers zo te manipuleren dat toegang wordt verkregen tot vertrouwelijke gegevens. Deze pogingen variëren van een 'eenvoudige beltest' waarbij wachtwoorden moeten worden ontfutseld en zogenaamde phishing-aanvallen (waarin gebruik wordt gemaakt van nep-e-mails of nep-websites), tot fysieke aanvallen waarbij *undercover* al dan niet met nagemaakte toegangspasjes het pand van een klant wordt betreden om vervolgens van binnenuit vertrouwelijke informatie te verzamelen. De bevindingen zijn over het algemeen opmerkelijk; ongeautoriseerde toegang tot kluizen in banken, beveiligde locaties van de overheid en tot in grote datacenters aan toe, om er maar een paar te noemen. In verschillende van deze gevallen wordt de opdracht gecombineerd met een penetratietest. Bij deze gecombineerde testen, ook wel aangeduid met *red teaming* (figuur 1), is over het algemeen de opdracht eerst ongeautoriseerd fysiek in het pand te komen, vervolgens van binnenuit de interne systemen te hacken, en weer ongezien mét vertrouwelijke gegevens het pand te verlaten.

Het grote verschil tussen een penetratietest, waar je aanvallen echt kan 'testen' op systemen, en social-engineering testen is dat je bij de laatste over het algemeen maar één kans hebt. Er is geen 'uitprobeerronde'; het moet in één keer goed. Als je verhaal niet geloofwaardig is, bestaat de kans met handboeien om afgevoerd te worden. De medewerkers van de organisatie waar de test wordt uitgevoerd zijn over het algemeen niet op de hoogte gebracht van de test. Veelal weten alleen enkele directieleden van de test en zelfs zij weten niet in alle gevallen wannéér de test precies zal worden uitgevoerd. Het is niet de bedoeling dat de beveiliging opeens extra gaat opletten bijvoorbeeld. Op deze manier kan een reëel beeld van de risico's worden verkregen. Als gevolg hiervan zal beveiligingspersoneel ook geen halve maatregelen nemen wanneer je als 'indringer' wordt ontmaskerd (zeker niet wanneer je op dat moment een stapel vertrouwelijke interne documenten in bezit hebt).

Ingrediënten van een geslaagde aanval

Om een aanval te laten slagen zijn twee zaken van doorslaggevend belang: *informatie* en *timing*. Een gedegen voorbereiding is essentieel. Voorafgaand aan een onderzoek wordt dan ook zoveel mogelijk *informatie* over het doelwit verzameld. Niet alleen over de organisatie waar het om gaat (corporate homepage, Google maps, search engines, nieuwsgroepen, vacaturesites), maar ook over de medewerkers, hun hobby's, woonplaats en contactgegevens (Facebook, Hyves, LinkedIn en dergelijke zijn erg nuttig). Daarna volgt veelal een aantal telefoontjes naar het algemene nummer en nummers van medewerkers voor zover deze via publiek beschikbare bronnen beschikbaar zijn. Bij grote organisaties zijn vaak reeksen telefoonnummers in gebruik. Op basis van bekende nummers wordt dan een aantal nummers in dezelfde reeks gebeld. Wanneer een medewerker opneemt, wordt aangegeven verkeerd verbonden te zijn en op zoek te zijn naar meneer X. Het goede nummer van meneer X evenals de naam en functie/afdeling van de gebelde persoon worden tevens zijdelings geverifieerd. Informatie die zo wordt verkregen kan weer gebruikt worden om nog meer informatie los te krijgen. Alle te vinden informatie is potentieel interessant. Voor een test op een streng beveiligd datacenter is wel eens twee maanden voor de test met een camera met 500mm lens van alle kanten het gebouw gefotografeerd om vast te stellen waar alle camera's en ingangen waren, hoe de medewerkers gekleed waren, hoe laat ze naar huis gingen, etc. Op basis van deze informatie worden vervolgens de details van een aanvalsscenario bepaald. Als wie gaan we ons voordoen, hoe laat moeten we aankomen (bijvoorbeeld om mee te kunnen lopen met de 'massa'), welke kleding kunnen we het beste aantrekken en welke route nemen we als we eenmaal 'binnen' zijn om zoveel mogelijk risico's (camera's en beveiligingsmensen) te omzeilen.

Figuur 1. **Red teaming, testmethode waarbij verschillende aanvalstechnieken gecombineerd worden om een daadwerkelijke aanval te simuleren.**

De *timing* van een aanval is tevens erg belangrijk. Het moment dat een geschikte medewerker zich aandient kan een kwestie van seconden zijn. Veelal is een medewerker nodig om langs een poort/hek/receptie of ander controlepunt te komen. Met kennis van het bovenstaande, een goed verhaal, het kunnen improviseren op onvoorziene situaties, gemakkelijk contacten kunnen leggen en af en toe stalen zenuwen kom je dan al een heel eind.

Op een gegeven moment leer je wat voor mensen je moet benaderen en welke je beter uit de weg kunt gaan. Secretaresses weten bijvoorbeeld vaak bijzonder goed wat er in een bedrijf speelt. Het kan heel waardevol zijn deze te benaderen, maar een goed en degelijk onderbouwd verhaal is wel een voorwaarde. Volledig improviseren is dan een soort Russische roulette. Praktijkvoorbeeld 1 beschrijft een test waarbij de te benaderen personen specifiek werden geselecteerd om de kans van slagen zo groot mogelijk te maken.

Training van medewerkers

Belangrijk bij de test is ook het doel *training van medewerkers* niet uit het oog te verliezen. De aanvalsscenario's dienen zo gekozen te worden dat de impact die medewerkers hiervan kunnen ondervinden tot het minimaal noodzakelijke beperkt wordt. Wij geven de opdrachtgever (voor zover dat mogelijk is) ook géén inzicht in welke medewerkers een rol hebben gespeeld in de testen en bevindingen. Gegevens worden geanonimiseerd en er wordt gerapporteerd over aantallen en de impact van de testresultaten. Het minst verstandige wat een opdrachtgever zou kunnen doen (en natuurlijk ook zeer onwenselijk, maar niet geheel ondenkelijk) is het nemen van disciplinaire maatregelen tegen de betreffende medewerkers. Het effect hiervan is dat

Praktijkvoorbeeld 1

Bij één van onze klanten voerden een collega en ik een geavanceerde phishing-aanval uit. Mijn collega had bij de ingang van het pand van de klant plaatsgenomen en vroeg selectief medewerkers die naar binnen gingen of deze deel wilden nemen aan een enquête over de invulling van een aankomende bedrijfsactiviteit. Bij de 'selectie' van medewerkers richtten we ons tot de jongere, vrouwelijke medewerkers om zoveel mogelijk de kans te beperken per ongeluk een IT-medewerker of managementlid aan te spreken. (Deze zouden het immers weten als er een 'enquêtepagina' bestond en daardoor de aanval mogelijk sneller doorgronden.) Ook hadden we vooraf de LinkedIn- en Facebookprofielen van sleutelpersonen in de organisatie bekeken om zo 'risicopersonen' te herkennen en te kunnen vermijden. Onder de deelnemers zou dezelfde week nog een iPod Touch worden verloot. De medewerkers die wilden deelnemen kregen een gesloten enveloppe met daarin een brief die de actie uitlegde en een link naar een door ons opgezette (nep)internetpagina met daarop de enquête. Na inloggen kreeg de medewerker een tiental vragen te zien en konden aanvullend nog eigen suggesties worden opgegeven. Na versturen werd de medewerker hartelijk bedankt voor de deelname. Uiteraard waren wij in het geheel niet geïnteresseerd in alle 'feestideeën' van medewerkers, maar was het ons alleen om de inloggegevens van de medewerkers te doen. Ikzelf had om de hoek van de ingang positie ingenomen, zodat ik door de ramen aan de zijkant van de ingang in de gaten kon houden of er binnen iets verdachts gebeurde en via de portofoon direct mijn collega kon aangeven zich uit de voeten te maken indien dit nodig was. Tevens kon ik via mijn smartphone 'live' vaststellen dat inmiddels enkele gebruikers hun wachtwoord hadden ingetoetst op onze website en de test dus al succesvol was geweest. Na ongeveer 35 minuten verlieten we beiden in verschillende richtingen de locatie. We hadden bepaald dat dit zo ongeveer de tijdspanne was waarin in geval van detectie een opvolging zou kunnen plaatsvinden. In de nabespreking met de klant bleek later dat hooguit enkele minuten na ons vertrek twee gealarmeerde medewerkers naar buiten waren gekomen om opheldering te vragen.

medewerkers wanneer ze daadwerkelijk 'slachtoffer' worden van een echte social-engineering aanval dit mogelijk niet zullen melden uit angst voor represailles en de organisatie de aanval niet of te laat zal opmerken met alle gevolgen van dien.

Een goede opvolging van een social-engineering test is om de resultaten terug te koppelen naar (alle) medewerkers zodat deze de test daadwerkelijk als een leermoment kunnen ervaren en daarmee (beter) voorbereid zijn tegen een 'echte' aanval. In de praktijk blijkt overigens het merendeel van niet-getrainde medewerkers gevoelig voor een social-engineering aanval en laten medewerkers van hoog tot laag in de organisatie zich misleiden.

Psychologische trucs

Hoewel het aanvalsscenario voor een test volledig wordt afgestemd op de situatie bij de klant en daarmee iedere keer verschillend is, is er een aantal psychologische principes of 'trucs' die hier de basis van zijn en iedere keer terugkomen:

- *Een band opbouwen*, bijvoorbeeld door het benoemen van een gemeenschappelijk probleem of interesse. Sociale media kunnen hierbij een waardevolle bron van informatie over iemand zijn. Aangeven bij hetzelfde bedrijf te hebben gewerkt, of dezelfde sport te beoefenen kan vertrouwen wekken. Ook kan gerefereerd worden aan een (zogenaamde) gemeenschappelijke vriend of kennis. Verzoeken die vervolgens gedaan worden, zijn daardoor voor het 'slachtoffer' lastiger te weigeren.
- *Tijdsdruk*, het 'slachtoffer' geen tijd geven goed over de beslissing na te denken door het schetsen van omstandigheden die een snelle beslissing vereisen. Windows onthoudt vaak de naam van de laatst ingelogde gebruiker (maar niet het wachtwoord). Door achter een (vergrendelde) pc van een gebruiker plaats te nemen kan over het algemeen de account van deze gebruiker worden geblokkeerd door meer dan vijf maal het onjuiste wachtwoord in te voeren. Wanneer een aanvaller bijvoorbeeld op deze wijze een account blokkeert en vervolgens de helpdesk belt en zeg dat hij *binnen vijf minuten* een belangrijke presentatie moet geven, maar zijn account heeft geblokkeerd, zal deze tijdsdruk er mogelijk toe leiden dat de helpdeskmedewerker (na te hebben vastgesteld dat de account inderdaad zojuist is geblokkeerd) een nieuw tijdelijk wachtwoord instelt en dit via de telefoon doorgeeft, waarna op het systeem kan worden ingelogd.
- Het verwijzen naar een *hooggeplaatste persoon in de organisatie* (autoriteit/gezag). Deze truc werkt vaak bijzonder effectief met het element 'tijdsdruk'. Door aan te geven dat het 'slachtoffer' de werkzaamheden van een hooggeplaatst persoon in de organisatie belemmert en daarom direct op het verzoek dient in te gaan. Een variatie hierop is het zelf door middel van kleding en accessoires 'afdwingen' van gezag (zie ook figuur 2). Met een pak en stropdas is het in sommige gevallen veel eenvoudiger om zonder vragen een pand in te komen als met een spijkerbroek en shirtje. Ik ben ooit met een kletsnatte bouwvakkersjas een bank ingelopen met de mededeling dat er in het bovengelegen pand lekkage was. Of ik 'even achter mocht kijken of het niet door het plafond heen kwam zetten'. De medewerkers

waren blij dat ze tijdig gewaarschuwd werden en zonder verdere vragen werd toegang verleend tot de achtergelegen ruimten die alleen voor bankpersoneel toegankelijk waren.

- *Verzoek om hulp*: bijvoorbeeld een verzoek om een bestandje van een USB-stick te printen, die zonder dat het 'slachtoffer' het weet, is geïnfecteerd met malware, of bijvoorbeeld het lenen van een elektronische toegangsbadge omdat de eigen badge 'nog op het bureau ligt'. Een verzoek van een man (de tester) aan een vrouw (het 'slachtoffer') of andersom zal in het algemeen eerder worden ingewilligd als bij gelijke sekse.
- Gebruik van *'herkenbare' zaken* voor de organisatie waar het onderzoek wordt uitgevoerd. Personen die een collega denken te herkennen door het dragen van een (al dan niet gekopieerde) toegangsbadge, vergelijkbare stijl van kleding, visitekaartjes, jargon, kennis van werkwijze of namen van informatiesystemen of collega's (namedropping) zullen minder snel kritische vragen stellen. Wanneer van de naam op de (valse) toegangsbadge ook nog een LinkedIn- of Hyvesprofiel bestaat dat refereert aan het onderzochte bedrijf, zijn de meeste kritische medewerkers ook overtuigd dat ze met een collega te maken hebben.
- Een andere methode kan zijn het *via de ene medewerker opvragen van gegevens bij een andere medewerker* (bijvoorbeeld het laten doorzetten van gegevens naar een bestaande interne afdeling die vervolgens benaderd wordt om de 'verkeerd gestuurde e-mail' door te zetten). Door gebruik te maken van deze interne referenties wordt de geloofwaardigheid vergroot. Een ander voorbeeld is het opnemen van de wachtmuziek, die bedrijven gebruiken als bellers in de wacht worden gezet. Wanneer je vervolgens belt met een medewerker zeg je na een paar minuten: 'Wacht even, ik krijg een andere lijn binnen', en zet het 'slachtoffer' in de wacht. Vervolgens speel je het wachtmuziekje af dat je eerder hebt opgenomen, waardoor het 'slachtoffer' onbewust denkt: 'Hé, dat is ons melodietje, hij werkt dus bij ons'.
- Aangeven dat *'alle collega's' van het 'slachtoffer' op dezelfde wijze hebben gehandeld*, dus dat het verzoek 'héél normaal' is. Mensen zijn geneigd iets als juist te beschouwen wanneer anderen dezelfde keuze hebben gemaakt. Een variatie hierop is het opbouwen van (informatie)verzoeken. Wanneer iemand al op een aantal verzoeken is ingegaan (bijvoorbeeld het opzoeken van compleet niet relevante informatie) zal het moeilijker zijn vervolgens een verzoek om vertrouwelijke informatie af te slaan.
- Noodzaak om iets '*terug te moeten doen/compenseren*' creëren. Door mensen iets te geven kan de gevoelsmatige verplichting gecreëerd worden jou iets verschuldigd te zijn. Hierdoor wordt het makkelijker iemand aan een verzoek te laten voldoen als zijnde normaal. Wanneer je iets voor iemand hebt gedaan (ook al heeft degene hier helemaal niet om gevraagd) wordt het voor deze persoon veel lastiger om een verzoek tot een wederdaad te weigeren.

Figuur 2. **Beveiligingsbadges waarmee een social engineer autoriteit kan afdwingen zijn voor enkele euro's te verkrijgen.**

Figuur 3. **De 'Sinterklaas en Zwarte Piet' die het datacenter wisten binnen te dringen.**

- De indruk geven dat het eigenlijke verzoek al een *concessie* is. Wanneer het genoeg is om ergens vijf minuten binnen te zijn, kan het zinvol zijn in te zetten op een rondleiding door het pand, maar als dit niet kan dan erop aan te dringen dat er in ieder geval even vijf minuten rondgekeken mag worden.
- Het aanbieden van iets wat leidt tot een *persoonlijk voordeel*. Bijvoorbeeld een phishing-e-mail met de code voor het bestellen van het persoonlijk kerstpakket.
- Het *veroorzaken van 'onvoorziene situaties'*, waardoor medewerkers (en in het bijzonder beveiligingsmedewerkers) niet meer in staat zijn hun gebruikelijke routine te volgen. Zo zijn we wel eens verkleed als Sinterklaas en Zwarte Piet een zwaarbeveiligd datacentrum binnengedrongen (figuur 3). Het datacentrum lag op een afgezonderde locatie en was omgeven door metershoge hekken met prikkeldraad, tientallen camera's en een aarden wal die het zicht op het gebouw ontnam. Een week van tevoren hadden we de beveiliging al aan de telefoon gehad en ons voorgedaan als HR-medewerkers die belden in verband met de aankomende Sinterklaasactiviteiten op de verschillende locaties. De beveiliging had dus al 'iets' van de activiteiten gehoord, maar werd toch overrompeld door de situatie. Om op het terrein te komen moest eerst een soort 'checkpoint Charlie' worden gepasseerd waar een beveiligingsmedewerker achter kogelvastglas met de beveiliging binnen overlegde over de te nemen stappen. Min of meer tot onze eigen verbazing werden we doorgelaten het terrein op, terwijl de deur achter ons weer vergrendeld werd. Bij het datacentrum zelf aangekomen liepen we ook weer direct

tegen een glazen beveiligingsruimte aan waar zich een vijftal beveiligingsmedewerkers bevond. Eén blik in onze zware zak met kilo's pepernoten was voldoende geweest om de opnameapparatuur van de spionagecamera (figuur 4) te ontdekken en ons te ontmaskeren. 'Hallo! Hier zijn we dan!!', riepen we, en vulden het bakje waar normaliter de paspoorten onder het glas worden doorgeschoven met pepernoten. Nadat we één van de beveiligers nog hadden omgekocht met een chocoladeletter hebben we een rondje door het pand gemaakt en zijn we zonder problemen weer vertrokken.

- Gebruik van een *afleidingsmanoeuvre*, bijvoorbeeld het meenemen van die leuke vrouwelijke collega met hoge hakken en een kort rokje.

Afhankelijk van de specifieke situatie bij de klant worden aanvalsscenario's uitgewerkt waarin veelal één of meer van bovenstaande technieken worden toegepast. In praktijkvoorbeeld 2 wordt bijvoorbeeld *een band opgebouwd met het 'slachtoffer', herkenning gecreëerd* door te refereren aan interne afdelingen, gerefereerd aan een *persoonlijk voordeel* (het niet verliezen van data) en een *compromis gesloten* (laatste alinea). Doordat er sprake is geweest van eerdere 'hulp' wordt tevens de noodzaak tot *'compensatie'* gecreëerd.

Methoden

Hieronder enkele veelgebruikte methoden die ingezet worden tijdens een social-engineering aanval. Bij deze methoden wordt deels gesteund op de eerder beschreven psychologische 'trucs'. De combinatie van methoden vormt samen het aanvalsscenario.

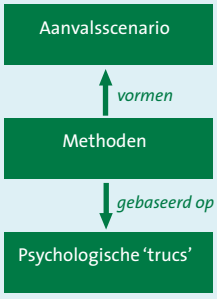
- *Phishing*: vorm van aanval waarbij gebruik wordt gemaakt van e-mails of internetpagina's die van een legitieme partij lijken te zijn, bijvoorbeeld van de eigen werkgever, maar in werkelijkheid worden beheerd door de aanvaller. Deze mails of pagina's hebben veelal tot doel gegevens van medewerkers (bijvoorbeeld wachtwoorden) te verzamelen.
- *Dumpster diving*: het doorzoeken van prullenbakken, bakken bij kopieermachines of buiten geplaatste containers van een organisatie op zoek naar waardevolle informatie. 'Waardevolle informatie' kan in dit geval bijvoorbeeld ook briefpapier of visitekaartjes zijn omdat deze weer kunnen worden gebruikt in een volgende aanval.
- *Pretexting*: het onder valse voorwendselen (de pretext) verkrijgen van informatie. Bijvoorbeeld het bellen van een medewerker en je voordoen als een interne collega.
- *Tailgating*: het 'meeliften' met een medewerker om door een beveiligd toegangspoortje te komen om zo fysieke toegang tot een beveiligde locatie te krijgen.
- *Reverse Social Engineering*: een methode waarbij het 'slachtoffer' zodanig gemanipuleerd wordt dat deze de social engineer om hulp zal vragen. De social engineer creëert voor het 'slachtoffer' een probleem en zal zich vervolgens kenbaar maken als 'expert' die het probleem kan oplossen. Vervolgens zal de social engineer het verzoek van het 'slachtoffer' afwachten. Omdat het initiatief bij het 'slachtoffer' ligt is er sneller een vertrouwensband.

Figuur 4. **Een 'knoopcamera' waarmee ongemerkt bijvoorbeeld toetsaanslagen gefilmd kunnen worden.**

Praktijkvoorbeeld 2

Bij een test waarbij het doel was systeemtoegang te verkrijgen heb ik een medewerkster gebeld met de melding dat er waarschijnlijk een probleem was met haar systeem en dat dit een enorme hoeveelheid netwerkverkeer op het netwerk veroorzaakte. Ik gaf aan dat het systeem hier uiteindelijk door kon vastlopen en in het ergste geval de aanwezige data niet meer benaderbaar zouden zijn. Op mijn vraag of de laptop niet erg traag was de laatste tijd kreeg ik uiteraard een bevestigend antwoord. Na wat willekeurig getik op mijn toetsenbord zei ik dat ik het probleem had gevonden, benadrukte dat het erg lastig was dit op te lossen, maar dat ik ermee bezig ging. Ik hing op en belde na een half uurtje opnieuw om te vertellen dat het probleem was opgelost. Nadat ze mij nadrukkelijk had bedankt hing ik op.

Twee dagen later belde ik opnieuw en zei dat het probleem helaas toch niet opgelost bleek te zijn en ook op de laptop zelf aanpassingen moesten worden doorgevoerd. Ik vroeg of ze de laptop even bij local IT kon langsbrengen (die ik al in een eerder gesprek had gebeld om vast te stellen hoe de procedure werkte en om te controleren dat deze daadwerkelijk een lokaal servicepunt had) om daarmee de indruk te wekken dat ik daadwerkelijk een interne medewerker was. De medewerkster was echter erg druk en dit kwam erg slecht uit. Bij wijze van uitzondering wilde ik dan ook wel op afstand kijken of ik het probleem kon oplossen, zei ik. Omdat we, zo liet ik weten, vanuit veiligheidsoogpunt nooit aan gebruikers vragen hun wachtwoord over de telefoon af te geven, vroeg ik haar om het wachtwoord tijdelijk te veranderen in 'welkom123', zodat ik dan op afstand het probleem kon oplossen. Twee minuten later kon ik op de laptop inloggen en had ik toegang tot de (vertrouwelijke) data die ik nodig had.



Figuur 5. **De samenhang tussen methoden, trucs en een aanvalsscenario.**

- *Shoulder Surfing*: meekijken bij het intoetsen van een wachtwoord of pincode. Hier hoeft niet daadwerkelijk te worden meegekeken. Bij verschillende tests wordt gebruikgemaakt van miniatuur-spionagecamera's, bijvoorbeeld een knoopcamera (figuur 4), waarbij je één van de knopen in je jasje vervangt door een knoop met camera. Wanneer hiermee het intoetsen van een wachtwoord wordt opgenomen, kan dit later vanuit de opnamen worden teruggekeken.
- *Het plaatsen van afluisterapparatuur (bugs), draadloos access point of keylogger.* Wanneer toegang is verkregen tot een pand kan vaak eenvoudig afluisterapparatuur worden geplaatst. Moderne afluisterapparatuur is voor een beperkt budget te verkrijgen en kan bijvoorbeeld een van tevoren ingesteld GSM-nummer bellen zodat via de telefoon live kan worden meegeluisterd (figuur 6). Alternatief wordt een keylogger geïnstalleerd (figuur 7). Deze kan in enkele seconden tussen het toetsenbord en de systeemkast van een gebruiker worden ingeklikt en slaat vervolgens alle toetsaanslagen op. Huidige versies van keyloggers kunnen deze vervolgens automatisch via een draadloos netwerk via mail doorsturen naar de aanvaller. Het verborgen intern plaatsen van een access point (bijvoorbeeld door deze achter een radiator te verstoppen) kan ook zinvol zijn. Wanneer deze op het netwerk is aangesloten kan de aanvaller vervolgens weer het pand verlaten en van buitenaf (bijvoorbeeld vanuit de auto) het interne netwerk aanvallen door een verbinding te maken met het zojuist geïnstalleerde access point met een kleine kans te worden opgespoord en opgepakt.
- *Malware*: kwaadaardige software die bijvoorbeeld wachtwoorden verzamelt en doorstuurt naar een e-mailadres van de aanvaller. Malware kan op het systeem geplaatst worden door middel van bijvoorbeeld een geïnfecteerde pdf-file ([Paquo1]). De pdf-file kan worden verspreid door bijvoorbeeld het achterlaten van een USB-stick met daarop bestanden als 'loonlijst 2011' of 'fraudeonderzoeken 2011'. Ideale plaatsen om dergelijke sticks achter te laten is bij de toiletten of het koffieapparaat. Wanneer het 'slachtoffer' de pdf-file opent wordt daarmee ongemerkt tevens de malware opgestart.

In praktijkvoorbeeld 3 wordt een aantal van de hierboven genoemde methoden toegepast. Dit voorbeeld laat onder andere zien hoe informatie die wordt verkregen vanuit de ene aanval, kan worden gebruikt in een volgende aanval om daarmee meer informatie te verkrijgen.

Praktijkvoorbeeld 3

Het is even over achten als ik mijn auto op een kleine honderd meter afstand van het pand van één van onze klanten neerzet. Ik heb eerder vastgesteld dat de meeste medewerkers met de auto komen en deze achter het hoofdkantoor neerzetten op de besloten parkeerplaats, dus het lijkt me het beste om dit patroon te volgen omdat het lopend de parkeerplaats opgaan al mogelijk de aandacht trekt. In mijn spiegel houd ik in de gaten of er medewerkers aan komen rijden. Na een minuut of tien verschijnt er een grijze personenauto. Zodra de wagen mij passeert, voeg ik in en volg op korte afstand. Helaas rijdt de auto het pand van het doelwit van vandaag voorbij en word ik gedwongen via een rondje weer terug te gaan naar mijn beginpositie. De tweede keer heb ik meer geluk en kan ik, nadat de medewerker met zijn personeelspas de slagboom heeft geopend, op korte afstand volgen tot op het besloten parkeerterrein achter het pand. Ik wacht even tot de medewerker uit de auto voor mij via de personeelsingang aan de achterzijde het pand is ingegaan en loop naar de rookplek vlak voor de ingang. Ik pak het nieuwe pakje sigaretten uit mijn zak, steek er één aan. Gelukkig zijn er geen camera's aan deze zijde van het pand, dus kan ik hier rustig even blijven hangen tot er een nietsvermoedende medewerker aanhaakt om te komen roken met deze niet-roker, die voor de gelegenheid maar even met een sigaret staat te zwaaien. Op gegeven moment verschijnt er een dame die zich bij mij voegt om ook te roken, we maken een praatje en lopen gezamenlijk – door met haar personeelspas de deur te openen – het pand in. Binnen! Ik besluit gelijk maar in volgmodus het trappenhuis in te lopen, want deze klant heeft zo te zien ook paslezers bij de deuren naar de verschillende verdiepingen aangebracht. Ik volg haar naar de vierde etage en betreed, opnieuw doordat zij netjes de deur voor ons opent, de verdieping. Gelukkig staat er een koffieapparaat dus kan ik daar de verdieping observeren zonder mezelf klem te lopen in één of ander doodlopend deel van het pand. Even verderop blijken wat vergaderruimteachtige werkplekken te zitten. Ik neem mijn koffie mee, trek in de vergaderzaal de kabel uit de VoIP-telefoon en prik deze in mijn laptop. Terwijl mijn laptop opstart, werp ik een blik op de stapel papier

Uit praktijkvoorbeeld 3 blijkt dat het niet altijd van belang is hoeveel medewerkers daadwerkelijk in de trucs van een social engineer trappen. In deze specifieke situatie was het voor een buitenstaander al voldoende om slechts twee medewerkers te misleiden om vervolgens de volledige IT-omgeving te kunnen overnemen.

die ik zojuist in het langslopen uit de verzamelbak naast de printer heb meegegrist. Onder andere e-mails, met een hoop mailadressen van medewerkers in de 'To'- en 'CC'-velden. Mooi zo! Dit worden mijn 'slachtoffers' in de volgende aanval.
Mijn laptop is inmiddels opgestart en ik start een poortscan op poort 80 op de nabijgelegen IP-adressen op zoek naar wat interne webpagina's. Tevens probeer ik via mijn webbrowser een aantal voor de hand liggende url's. 'intranet.klantnaam.nl',' intraweb.klantnaam.nl', 'search.klantnaam.nl', 'telefoongids.klantnaam.nl'. Na niet al te lang zoeken heb ik een interne webpagina gevonden. Ik kopieer de pagina en pas wat teksten aan en na een kwartiertje heb ik een 'medewerker van de maand'-verkiezingspagina in elkaar gezet die er precies zo uitziet als de pagina's van het bedrijf zelf inclusief bijbehorende logo's en kleuren. Vervolgens start ik de webserver op mijn eigen laptop zodat de zojuist gemaakte pagina vanaf het interne netwerk kan worden benaderd.
Door een tweede beperkte poortscan weet ik een interne mailserver te identificeren waarop mail relaying aanstaat (waardoor anoniem e-mail verstuurd kan worden). Ik ben inmiddels zeker twintig minuten in het pand en nog niemand heeft me tot nu toe vragen gesteld over wat ik hier doe. Nu richt ik me weer op de 'slachtoffers'. Via de mailserver stuur ik allereerst een mail met een vals extern e-mailadres dat ik vanuit mijn spamfolder heb gekopieerd naar een deel van de adressen in de uitgeprinte e-mails. Ik hoop op deze test-e-mails een out-of-office bericht terug te krijgen van één van de medewerkers. Wanneer ik deze inderdaad retour krijg, kopieer ik de ondertekening en pas naam en functie aan naar een fictieve naam. Ik heb nu een webpagina én een e-mailbericht die er precies zo uitzien alsof ze van de eigen organisatie zijn. Vervolgens zet ik in de e-mail een *Reminder* van de uitnodiging voor de 'medewerker van de maand'-verkiezing. De mail geeft aan dat een willekeurig gekozen selectie van medewerkers één van hun collega's kan nomineren voor deze prijs. Dit kan via een interne webpagina waarvan de link onderaan de e-mail is opgenomen. Uiteraard moet wel worden ingelogd om te voorkomen dat mensen dubbele stemmen uitbrengen. De reminder geeft aan dat degenen die de eerste mail hebben gemist nog tot 12:00 uur dezelfde dag de kans hebben om hun stem uit te brengen. Ik switch naar een tweede venster waar ingetoetste wachtwoorden zullen verschijnen en wacht rustig af tot de eerste enthousiastelingen hun wachtwoord inkloppen. Dit duurt op de kop af twee minuten na het versturen van de e-mail.
Met het inloggen op de site hebben de medewerkers automatisch naast hun wachtwoord ook hun gebruikersnaam en IP-adres achtergelaten. Dit is voor mij alle informatie die ik nodig heb en ik start Metasploit (een hackers toolkit) en log hiermee op afstand in op de pc van de eerste enquêtedeelnemer. Inmiddels heb ik de gebruiker ook teruggevonden in de interne online telefoongids. Helaas blijkt de eerste medewerker op de financiële afdeling te werken. In deze fase ben ik meer op zoek naar een IT-beheerder omdat deze vaak hoge gebruikersrechten hebben en daarmee toegang tot een groot aantal of alle systemen. Ik besluit een dump te maken van de lokale wachtwoord-hashes. Met de hash van de lokale administrator account probeer ik vervolgens te authenticeren tegen het systeem van een willekeurige andere gebruiker op het netwerk. Deze 'truc' heeft al bij verschillende klanten gewerkt en blijkt ook nu succesvol. Inmiddels ben ik zo'n drie kwartier binnen zonder dat dit iemand is opgevallen en heb ik reeds twee systemen volledig overgenomen. Helaas werkt de hash niet op de domain controller, dus besluit ik net zo lang op systemen in te loggen tot ik een systeem tref waar een gebruiker (of proces) aanwezig is met hoge rechten (bijvoorbeeld de IT-beheerder). Na twintig minuten vind ik een systeem waarop een IT-beheerder is ingelogd. De tool Metasploit, die overigens gratis te downloaden is, heeft een ingebouwde functie om de identiteit, en daarmee alle rechten van een gebruiker over te nemen. Nadat ik de identiteit van IT-beheerder heb overgenomen, heb ik domain administrator rechten en volledige toegang tot alle Windows-systemen en daarop aanwezige data op het netwerk, inclusief alle servers met financiële administratie en de mailboxen van de directie. Ik maak wat screenshots en vind dat het tijd is voor een tweede kop koffie.

Figuur 6. **'Audiobug' waarmee via GSM gesprekken kunnen worden afgeluisterd.**

Maatregelen

Bewustzijn

Het sleutelwoord tegen social-engineering aanvallen is bewustzijn, of specifieker gezegd, kennis van de mogelijke doelwitten en van de technieken van een aanvaller, maar ook kennis van de eigen zwakheden. Bij één van mijn opdrachten had de klant op alle verdiepingen naast de gebruikelijke papierbakken bij de printers grote afgesloten bakken voor vertrouwelijk papier

geplaatst. Een greep in de bak voor gewoon afvalpapier leverde echter een grote stapel met vertrouwelijke documenten op (rapporten van security-incidenten, HR-informatie, wachtwoorden, enz.) Waarom? Vermoedelijk was het te veel moeite geweest om de stapels papier door de kleine sleuf van de bak voor vertrouwelijk papier te proppen en was in één keer weggooien makkelijker.

Wanneer klanten in een presentatie of training horen hoe een truc werkt, zegt men over het algemeen iets als 'dan moet je wel echt naïef zijn om daar in te trappen, dat zou bij mij niet lukken'. De praktijk is echter vaak anders. Om echt bewustzijn te creëren is het daarom naast het verschaffen van informatie zinvol om een test/oefening uit te voeren. Hierdoor zien mensen vaak in dat ze helemaal niet zo bestand zijn tegen een dergelijke aanval als ze vaak zelf denken en wordt daadwerkelijk bewustzijn gecreëerd. Naast het creëren van bewustzijn is een test een prima middel om de risico's in kaart te brengen.

Richtlijnen

Naast bewustzijn is het opstellen van richtlijnen en het controleren van de naleving daarvan essentieel. Hierbij kan bijvoorbeeld gedacht worden aan 'tien regels voor informatiebeveiliging'. Deze zouden er bijvoorbeeld als volgt uit kunnen zien:

1. Maak je wachtwoorden in geen enkel geval bekend aan anderen (ook niet aan IT-medewerkers).
2. Deel geen interne informatie met buitenstaanders.
3. Houd je aan de clean desk en whiteboard policy.
4. Vergrendel je computer als je je werkplek verlaat.
5. Laat geen informatie bij de printer achter.
6. Maak gebruik van beveiligde afvalbakken voor vertrouwelijke gegevens.
7. Verifieer de identiteit van de gesprekspartner wanneer gevraagd wordt om vertrouwelijke gegevens. (In geval van een telefonisch verzoek kan dit bijvoorbeeld door de beller terug te bellen op een vast nummer.)
8. Sla vertrouwelijke informatie nooit lokaal of op een privé-pc op.
9. Alarmeer bij verdachte zaken direct de security officer.
10. Draag de toegangsbadge zichtbaar en wijs collega's op het dragen van deze badge. Onbekenden zonder badge dienen naar de uitgang van het pand te worden geëscorteerd en daar worden overgedragen aan de receptie/beveiliging.

Figuur 7. **Keylogger die alle toetsaanslagen verzamelt.**

Om een effectieve naleving van dergelijke regels te bewerkstelligen dient te worden gecontroleerd of medewerkers deze daadwerkelijk naleven. Bevindingen hieruit (zowel positief als negatief) dienen naar de betreffende medewerkers te worden teruggekoppeld.

Conclusie

Wellicht denkt na het lezen van dit artikel dat de genoemde voorbeelden onmogelijk gebeurd kunnen zijn en dat dergelijke voorvallen in de praktijk niet zullen slagen. De werkelijkheid is echter dat deze en vergelijkbare aanvallen elke dag plaatsvinden en dat ondanks allerlei beveiligingsmaatregelen als beveiligingspersoneel, hekken met prikkeldraad, toegangspasjes, camerabewaking, alarminstallaties en dergelijke social engineers weten door te dringen tot het hart van de organisatie. Het uitvoeren van een social-engineering test kan een goede methode zijn om de risico's in een organisatie in kaart te brengen en het bewustzijn van medewerkers te verhogen.

Referenties

[Hadg01] Christopher Hadgany, *Social engineering – the art of human hacking*, 2010.

[Mitn01] Kevin D. Mitnick en William L. Simon, *The Art of Deception*, 2002.

[Paqu01] Matthieu Paques, *Hacken met PDF-files*, http://www.compact.nl/artikelen/C-2009-4-Paques.htm.

[security.nl] : artikelen inzake social-engineering aanvallen http://www.security.nl/tag/social%20engineering.