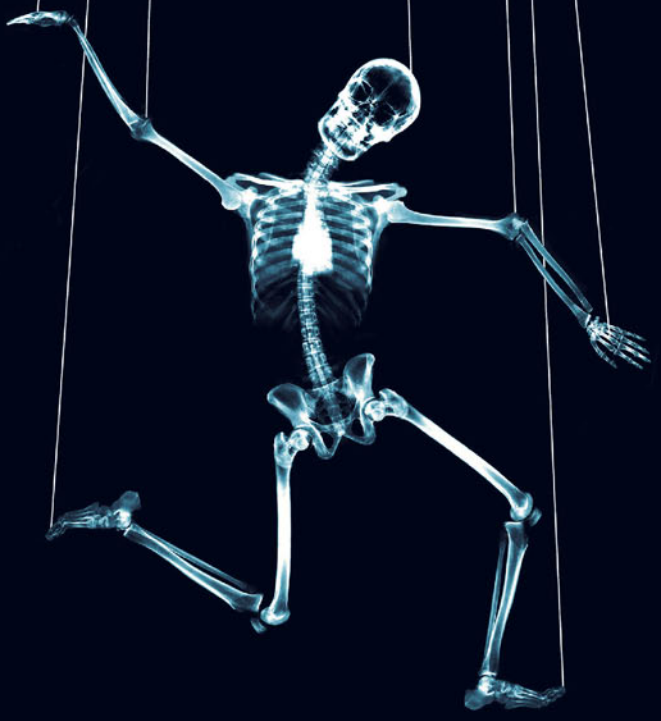
Podczas większości złośliwych ataków wykorzystuje się element socjotechniczny, aby zwieść użytkownika i nakłonić go do zapewnienia atakującym dostępu. Kolejne słabości techniczne można usuwać w miarę ich powstawania, natomiast nic nie da się poradzić na głupotę, a raczej łatwowierność ludzi. Chris wyjaśnia tajemnice tego typu przedsięwzięć, omawiając wykorzystywane współcześnie ścieżki ataku. Ta książka dostarcza cennych informacji, które ułatwiają rozpoznawanie takich ataków.

— **Kevin Mitnick**, **pisarz, prelegent i konsultant**

SOCJOTECHNIKA

Sztuka zdobywania władzy nad umysłami



CHRISTOPHER HADNAGY

PRZEDMOWA PAUL WILSON

Helion

one press EXCLUSIVE!

Tytuł oryginału: Social Engineering: The Art of Human Hacking

Tłumaczenie: Magda Witkowska

ISBN: 978-83-283-3315-4

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://onepress.pl/user/opinie/socjov
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *http://onepress.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

SPIS TREŚCI

4 Wchodzenie w rolę, czyli jak zostać kimkolwiek

Kluczem do budowania relacji jest szczerość. Jeśli potrafisz ją udawać, sukces murowany.

— RICHARD JENI

Pewnie wszystkim nam się zdarza od czasu do czasu zamarzyć o tym, aby być kimś innym. Cóż, sam mógłbym być trochę szczuplejszy i przystojniejszy. Co prawda rozwój medycyny nie pozwolił dotychczas na wynalezienie pigułki, która by to umożliwiała, nie oznacza to jednak, że nie istnieje rozwiązanie tego problemu — nazywa się ono *wchodzeniem w rolę*.

Co to takiego? Niektórzy twierdzą, że to zwykła „bajeczka" lub wręcz kłamstwo wciskane komuś w związku z wykonywanym zadaniem socjotechnicznym. Taką definicję należy jednak uznać za bardzo ograniczoną. Wchodzenie w rolę należałoby raczej zdefiniować jako tworzenie historii oraz dobór stroju, toalety, osobowości oraz postaw, które składają się na charakterystykę postaci odgrywanej przez Ciebie w trakcie wykonywania audytu zabezpieczeń. Wchodzenie w rolę obejmuje wszystko, co tylko możesz sobie wyobrazić na temat odgrywanej osoby. Im lepiej przygotujesz swoją rolę, tym bardziej wiarygodnie wypadniesz. Często sprawdza się tu zasada, że im prostsza rola, tym lepsza.

Wchodzenie w rolę — szczególnie od czasu rozpowszechnienia się internetu — bywa coraz częściej wykorzystywane w złośliwych celach. Miałem kiedyś okazję widzieć koszulkę z napisem: „Internet = miejsce, w którym mężczyźni są mężczyznami, kobiety są mężczyznami, a dzieci to czający się na Ciebie agenci FBI". Jest to oczywiście stwierdzenie żartobliwe, tkwi w nim jednak również sporo prawdy. W internecie możesz być, kim tylko zechcesz. Hakerzy wykorzystują to zjawisko od wielu lat i wcale nie ograniczają się w swoich zakusach do przestrzeni wirtualnej.

Odgrywanie roli lub udawanie kogoś innego stanowi często nieodłączny element pracy socjotechnika. Chris Hadnagy może nie mieć takich możliwości jak pracownik obsługi technicznej czy dyrektor generalny dużej firmy zajmującej się importem. W sytuacji o charakterze socjotechnicznym powinieneś koniecznie dysponować

wszystkimi umiejętnościami niezbędnymi do wejścia w rolę. Chris Nickerson, światowej sławy socjotechnik, powiedział mi kiedyś podczas rozmowy coś, co moim zdaniem doskonale oddaje istotę tego zagadnienia.

Nickerson stwierdził, że wchodzenie w rolę nie polega na tym, aby ją po prostu odgrywać. Nie chodzi o to, aby żyć kłamstwem, lecz o to, żeby faktycznie stać się osobą, za którą się podajemy. Chodzi o to, abyś każdą komórką swojego ciała był tym, kogo udajesz. Powinieneś odpowiednio się poruszać, odpowiednio się wypowiadać i zadbać o odpowiednią mowę ciała — masz stać się osobą, za którą się podajesz. Osobiście w całości zgadzam się z tą koncepcją. Doskonale widać to na przykładzie filmów. Za „najlepszy, jaki kiedykolwiek widzieliśmy" uznajemy zwykle taki film, w którym aktor wczuwa się w odgrywaną rolę do tego stopnia, że mamy trudności z oddzieleniem go od odgrywanej postaci.

Przekonałem się o tym wiele lat temu, gdy razem z żoną obejrzeliśmy znakomity film z Bradem Pittem, zatytułowany *Wichry namiętności*. Brad grał tam samolubnego pacana, zagubionego człowieka, który podjął w życiu wiele złych decyzji. Tak znakomicie odegrał swoją rolę, że moja żona i ja przez kilka kolejnych lat nie cierpieliśmy go również w innych filmach i wcieleniach. Oto przykład człowieka, który potrafi znakomicie wejść w rolę.

Problem z wchodzeniem w rolę polega na tym, że część socjotechników postrzega tę technikę wyłącznie jako przebieranie się w celu odegrania danej postaci. Odpowiedni strój się przydaje, nie przeczę, ale wchodzenie w rolę na tym się nie kończy. Musisz stworzyć dla siebie osobowość zupełnie inną od tej, która cechuje Cię normalnie. W tym celu musisz dokładnie zrozumieć, na czym tak naprawdę polega wchodzenie w rolę. Dopiero wówczas będziesz mógł skutecznie zaplanować i zrealizować to działanie. Potem wystarczy dołożyć jeszcze kilka smaczków, które dopełnią całości. W niniejszym rozdziale zajmiemy się właśnie różnymi aspektami wchodzenia w rolę. Najpierw powiemy sobie, na czym to dokładnie polega, a następnie przejdziemy do socjotechnicznych zastosowań wchodzenia w rolę, aby na koniec zapoznać się z kilkoma historiami, obrazującymi skuteczne przypadki posługiwania się tą techniką.

Na czym polega wchodzenie w rolę?

Wchodzenie w rolę definiuje się jako kreowanie zmyślonego scenariusza w celu przekonania ofiary do ujawnienia określonych informacji lub podjęcia określonych działań. Chodzi o coś więcej niż o tworzenie iluzji — w niektórych sytuacjach będziesz musiał stworzyć zupełnie nową tożsamość i wykorzystać ją w celu zmanipulowania kogoś i wydobycia od niego interesujących Cię informacji. Socjotechnicy mogą stosować tę metodę i podawać się za ludzi na określonych stano-

wiskach lub wykonujących pewną pracę, którą tak naprawdę nigdy się w swoim życiu nie parali. We wchodzeniu w rolę nie ma rozwiązań uniwersalnych. Socjotechnik tworzy i odgrywa podczas swojej kariery wiele różnych ról, wszystkie je łączy jednak pewien wspólny element: przygotowania. O sukcesie lub porażce wchodzenia w rolę zadecyduje rzetelność w gromadzeniu informacji. Możesz idealnie wcielić się w rolę pracownika obsługi technicznej, na nic się to jednak nie zda, jeśli się okaże, że Twoja ofiara nie korzysta z zewnętrznego wsparcia technicznego.

Wchodzenie w rolę to technika, której stosowanie nie ogranicza się do działań o charakterze socjotechnicznym. Sprzedawcy, prelegenci, tak zwani wróżbici, eksperci w dziedzinie programowania neurolingwistycznego (NLP), lekarze, prawnicy, terapeuci i przedstawiciele podobnych zawodów posługują się taką lub inną formą wchodzenia w rolę. Wszyscy oni muszą wymyślać odpowiednie scenariusze, żeby ludzie mogli się poczuć na tyle pewnie, by zechcieli udostępniać informacje, które w normalnych okolicznościach zachowaliby dla siebie. Różnica między posługiwaniem się tą techniką przez socjotechników oraz przez inne osoby ma związek z celem tego działania. Podkreślmy przy okazji raz jeszcze, że socjotechnik musi na pewien czas stać się odgrywaną osobą, a nie tylko odegrać jej rolę.

Dopóki trwa organizowany przez Ciebie audyt lub inne zadanie o charakterze socjotechnicznym, musisz przez cały czas pozostawać w roli. Sam również wcielam się w różne role, podobnie jak wielu moich kolegów po fachu (niektórzy pozostają w tych rolach nawet „po godzinach"). Gdy tylko zachodzi taka potrzeba, powinieneś stawać się tym, kogo w danym momencie chcesz odgrywać. Profesjonalni socjotechnicy zakładają sobie wiele różnych kont internetowych, profili w serwisach społecznościowych i adresów e-mailowych, aby zwiększyć wiarygodność postaci, w które się wcielają.

Prowadziłem kiedyś wywiad z Tomem Mischke, znaną osobowością radiową. Rozmowa ta miała trafić na mój socjotechniczny podcast, który współtworzę (jest on dostępny pod adresem *www.social-engineer.org/episode-002-pretexting-not-just-for-social-engineers/*). Prezenterzy radiowi muszą znakomicie radzić sobie z wchodzeniem w rolę, ponieważ ich praca polega na tym, aby przekazywać opinii publicznej tylko te informacje, które chcą jej przekazać. Tom był w tym tak świetny, że wielu jego słuchaczy miało wrażenie, jakby znali go równie dobrze jak swoich przyjaciół. Otrzymywał zaproszenia na wesela, rocznice, a nawet do towarzyszenia przy porodach. Jak udało mu się tak skutecznie wejść w rolę?

Odpowiedź jest prosta: trening. Tom Mischke zaleca wszystkim, by jak najwięcej ćwiczyli. Powiedział mi, że najpierw planuje swoje „role", a potem je ćwiczy — posługuje się głosem charakterystycznym dla odgrywanej postaci, tak samo jak ona siedzi, czasem nawet ubiera się tak samo. Jeśli chcesz nauczyć się skutecznie wchodzić w różne role, zacznij ćwiczyć.

Powinieneś również koniecznie zapamiętać, że jakość odgrywanej roli jest bezpośrednią pochodną jakości zgromadzonych informacji. Im więcej ich masz, tym lepiej, a im bardziej są one trafne, tym łatwiej Ci będzie przygotować się do roli, a potem skutecznie w nią wejść. Na przykład klasyczna rola pracownika obsługi technicznej okazałaby się całkowitą klapą, gdyby się okazało, że przedsiębiorstwo obrane przez Ciebie na cel nie outsourcuje tego typu usług albo korzysta z bardzo małej firmy zewnętrznej, zatrudniającej zaledwie jedną lub dwie osoby. Wchodzenie w rolę powinno być dla Ciebie tak łatwe, jak naturalne zachowanie podczas rozmowy, podczas której jesteś po prostu sobą.

Chcę, abyś sam się nauczył korzystać z tych umiejętności, dlatego w następnym fragmencie rozdziału wyjaśnię Ci podstawowe zasady wchodzenia w rolę oraz sposób ich wykorzystania w działaniach związanych z planowaniem porządnej roli.

Zasady wchodzenia w rolę oraz etapy planowania roli

Jak to bywa w przypadku wielu różnych kompetencji, także wchodzenie w rolę można podzielić na kilka kroków, następujących po sobie według pewnych zasad. Poniżej przedstawiam listę pomocnych zasad związanych z wchodzeniem w rolę. Oczywiście nie są to wszystkie zasady rządzące tą kwestią, jednak moim zdaniem to właśnie one najlepiej oddają jej istotę:

- Im lepiej się przygotujesz, tym większe będziesz miał szanse na sukces.
- Żeby zmaksymalizować swoje szanse, odwołaj się do własnych zainteresowań.
- Ćwicz różne dialekty i posługiwanie się charakterystycznymi wyrażeniami.
- Nie lekceważ telefonu.
- Im prostsza rola, tym większe szanse na sukces.
- Rola powinna robić wrażenie odgrywanej spontanicznie.
- Przedstaw ofierze logiczny wniosek lub zaproponuj dalsze działanie.

Poniżej znajdziesz szczegółowe omówienie poszczególnych zasad.

Im lepiej się przygotujesz, tym większe będziesz miał szanse na sukces

Tej zasady nie trzeba chyba nikomu wyjaśniać, z pewnością należy ją jednak powtarzać do znudzenia — skuteczność wchodzenia w rolę wykazuje bezpośredni związek ze stopniem przygotowania do jej odgrywania. Jak już wspominałem w rozdziale 2., jest to fundament wszelkich skutecznych działań socjotechnicznych. Im więcej informacji zgromadzisz, tym większe masz szanse na opracowanie roli, która pozwoli Ci z powodzeniem wypełnić zadanie. Przypomnij sobie historię z rozdziału 2. o moim mentorze, Matim Aharonim, który przekonał wysokiego rangą pracownika firmy do wejścia na stronę „kolekcji znaczków". Na pierwszy rzut oka mogłoby się wydawać, że ścieżka dostępu do tamtej firmy wiedzie poprzez zagadnienia finansów, bankowości, zbierania funduszy na cele charytatywne lub coś podobnego — chodziło w końcu o instytucję bankową. Im dłużej Mati gromadził informacje i przygotowywał się do zadania, w tym większym stopniu zdawał sobie sprawę, że powinien stworzyć scenariusz związany z filatelistyką. Wiedza na temat zainteresowań tamtego dyrektora pozwoliła Matiemu znaleźć łatwą ścieżkę dostępu do firmy — ścieżkę, która okazała się skuteczna.

Czasami tajemnica sukcesu tkwi właśnie w tego rodzaju szczegółach. Pamiętaj, że nie ma danych nieistotnych. Gromadząc informacje, skup się także na historiach, przedmiotach lub kwestiach o znaczeniu osobistym dla Twojej ofiary. Odwołanie się do spraw osobistych i emocjonalnych pozwala często zdobyć pierwszy przyczółek. Jeżeli socjotechnik ustali, że dyrektor ds. finansowych pewnej firmy co roku przekazuje spory datek na rzecz ośrodka zajmującego się badaniami nad nowotworami dziecięcymi, niewykluczone, że skutecznym rozwiązaniem będzie stworzenie scenariusza zakładającego zbieranie środków na podobny cel (jakkolwiek bezdusznie by to nie brzmiało).

Problem polega na tym, że złośliwi socjotechnicy bez zastanowienia sięgają po role, w których wykorzystują emocje i uczucia swoich ofiar. Po atakach na WTC z 11 września 2001 roku złośliwi hakerzy i socjotechnicy wykorzystali dramat wielu osób, żeby zbić na tym kapitał dla siebie. Zakładali fałszywe strony internetowe i rozsyłali fałszywe e-maile, wyłudzając w ten sposób pieniądze od ludzi wielkiego serca. To samo zjawisko wystąpiło po trzęsieniach ziemi, do których doszło w 2010 roku w Chile i na Haiti. Pojawiły się wówczas liczne strony internetowe, które rzekomo podawały informacje na temat aktywności sejsmicznej lub informowały o losach zaginionych osób. Na stronach tych zamieszczono również złośliwe oprogramowanie, które włamywało się do komputerów odwiedzających.

Zjawisko to jeszcze wyraźniej uwidacznia się bezpośrednio po śmierci wielkich gwiazd muzyki lub filmu. Eksperci w sprawach optymalizacji w wyszukiwarkach

internetowych (SEO) oraz marketingu potrafią wypromować własne treści poświęcone temu wydarzeniu w ciągu zaledwie kilku godzin. Ze wzrostu natężenia ruchu w wyszukiwarkach skorzystają również złośliwi socjotechnicy, którzy stworzą fałszywe strony internetowe żerujące na tym natężonym ruchu. Ludzie będą trafiać na strony, na których czekają na nich rozmaite wirusy oraz programy zbierające dane.

Ludzie nie cofną się przed wykorzystaniem dramatu lub tragedii innych osób — smutne to, acz prawdziwe. To jeden z tych mrocznych zaułków świata, do których prowadzi ta książka. Jestem audytorem zabezpieczeń i w mojej pracy mogę wykorzystać emocje pracowników, aby dowieść firmom, że nawet ludzie o pozornie dobrych intencjach mogą zmanipulować członków organizacji i wydobyć od nich wartościowe informacje, co dla samej firmy może okazać się katastrofalne w skutkach.

Wszystkie te przykłady powinny utwierdzić Cię w przekonaniu, że im więcej zgromadzisz informacji i im lepiej się przygotujesz, tym większe masz szanse na znalezienie jakiegoś drobiazgu, który zwiększy Twoje szanse na wejście w odpowiednią rolę.

Żeby zmaksymalizować swoje szanse, odwołaj się do własnych zainteresowań

Wykorzystanie własnych zainteresowań w celu zwiększenia skuteczności podejmowanych działań socjotechnicznych to w sumie dość prosty zabieg, a mimo to czasami naprawdę pomaga przekonać ofiarę o Twojej wiarygodności. Kiedy ktoś zdaje się sugerować, że sporo wie na dany temat, a potem okazuje się to nieprawdą, od razu tracisz do takiej osoby zaufanie, tracą też na tym Wasze relacje. Jeśli jesteś socjotechnikiem, ale nigdy wcześniej nie byłeś w serwerowni ani nie rozkładałeś komputera na części, wybierając dla siebie rolę pracownika wsparcia technicznego, fundujesz sobie pewną porażkę. Uwzględnij w swojej roli zagadnienia, które Cię interesują, a będziesz miał wiele do powiedzenia i zrobisz wrażenie osoby inteligentnej i pewnej siebie.

Pewność siebie ma duże znaczenie dla przekonania ofiary, że faktycznie jesteś tym, za kogo się podajesz. Niektóre role wymagają zgromadzenia większej ilości wiedzy. Dotyczy to na przykład ról filatelisty czy fizyka jądrowego — żeby wypaść wiarygodnie, musisz się solidnie przygotować. Niekiedy jednak rola okazuje się na tyle niewymagająca, że wystarczy zapoznać się z kilkoma stronami internetowymi lub przeczytać książkę.

Bez względu na to, w jaki sposób posiądziesz niezbędną wiedzę, bardzo ważne jest to, abyś zgłębiał zagadnienia, które Cię faktycznie interesują. Wybierz historię, zagadnienie, usługę lub dowolny inny przedmiot Twoich zainteresowań, a następnie zastanów się, czy coś Ci to daje.

Dr Tom G. Steves stwierdza: „Należy koniecznie pamiętać, że pewność siebie *zawsze* zależy od danego zadania i sytuacji. W różnych sytuacjach odczuwamy różny stopień pewności siebie". To bardzo ważna obserwacja, ponieważ pewność siebie przekłada się również na to, jak inni postrzegają Cię w roli socjotechnika. Pewność siebie (przynajmniej dopóki nie staniesz się zbyt pewny siebie) stanowi podstawę do budowania zaufania i nawiązywania relacji, dzięki którym inni rozluźniają się w Twoim towarzystwie. Dlatego tak duże znaczenie ma znalezienie takiej ścieżki dostępu do ofiary, która umożliwiłaby prowadzenie rozmowy na bliski Ci temat — dzięki temu zyskasz większą pewność siebie.

W 1957 roku psycholog Leon Festinger stworzył teorię dysonansu poznawczego, zgodnie z którą ludzie wykazują skłonność do dopatrywania się konsekwencji w swoich przekonaniach, poglądach i ogólnie we wszystkim, co stanowi przedmiot ich poznania. Gdy pojawia się rozbieżność lub niespójność między postawą a zachowaniem, musi dojść do jakiejś zmiany, aby ten dysonans został usunięty. Zdaniem dr. Festingera o sile dysonansu poznawczego decydują dwa czynniki:

- liczba przekonań stanowiących źródło dysonansu,
- doniosłość tych przekonań.

Festinger stwierdził również, że istnieją trzy sposoby eliminacji dysonansu poznawczego (socjotechnicy, nadstawiać uszu!):

- zmniejszyć doniosłość przekonań stanowiących źródło dysonansu,
- dodać nowe, zgodne przekonania, które będą górować nad przekonaniami stanowiącymi źródło dysonansu,
- zmienić przekonania stanowiące źródło dysonansu na takie, które tego dysonansu powodować już nie będą.

W jaki sposób socjotechnik może wykorzystać te informacje? Socjotechnikowi wcielającemu się w rolę wymagającą pewności siebie nie może tej pewności zabraknąć, ponieważ w przeciwnym razie automatycznie wykreuje dysonans poznawczy. Taki dysonans natychmiast wyostrza czujność ofiary i utrudnia nawiązywanie relacji, budowanie zaufania i czynienie postępów. Powstają bariery, które wpływają na zmianę zachowań drugiej osoby, która musi w jakiś sposób zrównoważyć postrzegany dysonans — w takiej sytuacji można niemal z całą pewnością stwierdzić, że Twoja rola się nie sprawdzi.

Jednym ze sposobów przeciwdziałania temu zjawisku jest dodawanie kolejnych, zgodnych przekonań, aby w końcu przeważyły one nad tymi stanowiącymi źródło dysonansu. Czego ofiara może się spodziewać po roli, w którą się wcielasz?

Dowiedz się tego, a będziesz w stanie dotrzeć do jej umysłu i emocji, zaszczepiając tam działania, słowa i postawy, które zbudują nowy system przekonań, potężniejszy od dotychczasowego, stanowiącego źródło wątpliwości.

Doświadczony socjotechnik może się również pokusić o próbę zmiany tych przekonań, które stanowią źródło dysonansu, na takie, które jego źródłem już nie będą. Z pewnością jest to trudniejsze, warto jednak opanować tę niezwykle przydatną umiejętność. Niewykluczone na przykład, że Twój wygląd zewnętrzny nie będzie odpowiadać wyobrażeniom ofiary na temat tego, jak powinien wyglądać człowiek, za którego się podajesz. Przypomnij sobie serial *Doogie Howser, lekarz medycyny*. Problem Doogiego polegał na tym, że ze względu na młody wiek „rola" lekarza do niego nie pasowała. To znakomity przykład dysonansu poznawczego, który odczuwały jego „ofiary", a który udawało się zmienić poprzez podejmowanie określonych działań lub posługiwanie się określoną wiedzą. Podobnie jak w poprzednim przykładzie, socjotechnik może uzgodnić swoją rolę z przekonaniami ofiary poprzez oddziaływanie na jej postawy, działania, a w szczególności wyobrażenie o samej roli.

Ostatnio podczas konferencji Defcon 18 miałem okazję zaobserwować inny przykład. Wchodziłem w skład zespołu, który podczas tej konferencji zajmował się organizacją swego rodzaju „socjotechnicznych podchodów". Wielu uczestników zabawy decydowało się wejść w rolę pracownika. Kiedy zadawaliśmy im pytanie na przykład o numer identyfikatora pracowniczego, większość z nich zaczynała okazywać zdenerwowanie lub po prostu się rozłączała. Doświadczonym socjotechnikom udawało się natomiast wyeliminować ten jawny dysonans poznawczy. Podawali numer identyfikatora znaleziony w sieci lub korzystali z innych metod, aby przekonać ofiarę, że nie potrzebuje tej informacji. Dzięki temu udawało się wyrobić w ofierze odpowiednie przekonania.

Zdaję sobie sprawę, że przedstawiam tu niezwykle techniczne rozwiązania bardzo prostego problemu, musisz jednak zrozumieć, że udawać można tylko do pewnego momentu. Dlatego też powinieneś rozważnie wybrać swoją ścieżkę.

Ćwicz różne dialekty i posługiwanie się charakterystycznymi wyrażeniami

Nauka posługiwania się różnymi dialektami to dość istotna kwestia. Przyswojenie sobie innego dialektu lub akcentu innego niż charakterystyczny dla Twojego miejsca zamieszkania musi trochę potrwać. Może się okazać, że nabycie charakterystycznego akcentu z południa Stanów Zjednoczonych albo akcentu azjatyckiego jest bardzo trudne, a czasem wręcz niemożliwe. Uczestniczyłem kiedyś w szkoleniu pewnej międzynarodowej korporacji sprzedażowej, podczas którego podano informację,

że 70% Amerykanów woli słuchać osób mówiących z brytyjskim akcentem. Nie potrafię ocenić wiarygodności tych danych, wiem natomiast, że sam lubię słuchać tego akcentu. Już po zakończeniu zajęć miałem okazję przysłuchiwać się, jak kilku innych uczestników podejmuje próby mówienia z takim właśnie akcentem. Brzmiało to okropnie. Jon, mój przyjaciel z Wielkiej Brytanii, wścieka się za każdym razem, gdy słyszy, jak Amerykanin próbuje cytować Mary Poppins, naśladując przy tym brytyjski akcent. Gdyby słyszał, co wyprawiali uczestnicy tamtego szkolenia, chyba by wyszedł z siebie.

Z tamtego szkolenia najlepiej zapamiętałem to, że dane statystyczne to jedno, a praktyka drugie. Liczby mogą wskazywać, że posługiwanie się konkretnym akcentem pomaga w sprzedaży, jednak sam fakt prowadzenia działań socjotechnicznych na południu USA lub w Europie nie powoduje, że łatwo będzie Ci przyjąć miejscowy akcent i podawać się za osobę „stąd". Aktorzy uczą się mówić z akcentem właściwym odgrywanym przez nich postaciom z pomocą trenerów wokalnych. Weźmy na przykład Christiana Bale'a, aktora wywodzącego się z Walii — słuchając go, niemal nie sposób tego stwierdzić. W większości filmów, w których zagrał, po prostu nie słychać jego brytyjskiego akcentu. Z kolei w filmie *Zakochany Szekspir* Gwyneth Paltrow udało się mówić z bardzo przekonującym brytyjskim akcentem.

Większość aktorów korzysta z pomocy trenerów specjalizujących się w dialektach, którzy pomagają im doskonalić pożądany akcent. Ponieważ większości socjotechników nie stać na korzystanie z usług takiego trenera, warto wiedzieć, że na rynku pojawiły się liczne publikacje poświęcone temu zagadnieniu. Dzięki takiemu opracowaniu możesz szybko opanować podstawy nabywania nowych akcentów — przykładem może być tu książka Evangeline Machlin pt. *Dialects for the Stage*. Jest to co prawda jedna ze starszych pozycji, jednak zamieszczone w niej wskazówki nie tracą na aktualności:

- Znajdź materiały z nagraniami ludzi mówiących z oryginalnym akcentem, którego chciałbyś się nauczyć. Książki takie jak *Dialects for the Stage* często zawierają materiały audio z nagraniami wielu różnych akcentów.
- Spróbuj powtarzać nagrane wypowiedzi i ćwicz tak długo, aż będziesz brzmiał tak samo jak na nagraniu.
- Kiedy nabierzesz już nieco pewności siebie, nagraj własną wypowiedź z danym akcentem, abyś mógł ją potem odsłuchać i skorygować błędy.
- Opracuj scenariusz i ćwicz nowo nabyty akcent w rozmowach z partnerem.
- Mów z nowo nabytym akcentem w miejscach publicznych i uważnie obserwuj reakcje ludzi.

Różnych dialektów i akcentów jest bez liku. Osobiście stosuję fonetyczny zapis stwierdzeń, które mam zamiar wygłosić. To pozwala mi ćwiczyć ich odczytywanie i głęboko zapisywać je w swojej głowie, dzięki czemu potem mój akcent brzmi bardziej naturalnie.

Powyższe wskazówki pomogą socjotechnikowi w opanowaniu obcego dialektu do perfekcji albo przynajmniej w skutecznym posługiwaniu się nim.

Jeśli nie uda Ci się opanować danego dialektu, zawsze możesz osiągnąć pewne efekty, ucząc się wyrażeń często używanych w danym regionie. Udaj się w jakieś miejsce publiczne, gdzie będziesz mógł przysłuchiwać się rozmowom innych ludzi, na przykład do restauracji albo do centrum handlowego. Tak naprawdę może to być dowolne miejsce, w którym spotyka się grupki osób prowadzące rozmowy. Przysłuchuj im się uważnie i wychwytuj charakterystyczne zwroty i słowa. Jeśli jakieś frazy powtórzą się w kilku różnych rozmowach, spróbuj uwzględnić je w swojej roli, w którą chcesz się wcielić — dzięki temu zyskasz na wiarygodności. Przypominam jednak o przygotowaniach i ćwiczeniach.

Nie lekceważ telefonu

W ostatnich latach internet zdominował bardziej „pośrednie" aspekty działań socjotechnicznych, kiedyś jednak nieodłącznym elementem aktywności w tym obszarze był telefon. Zmiana ta spowodowała, że wielu socjotechników nie poświęca wystarczająco dużo uwagi potencjalnym zastosowaniom telefonu, a mogą one okazać się niezwykle skuteczne.

Niniejszym chciałbym jednak podkreślić, że telefon nadal pozostaje jednym z najskuteczniejszych narzędzi dostępnych socjotechnikowi i że nie powinien on ograniczać się w korzystaniu z niego tylko dlatego, że internet daje większe możliwości unikania osobistego kontaktu.

Socjotechnik przygotowujący atak z wykorzystaniem telefonu może wykazywać nieco inne podejście, ponieważ będzie wychodził z założenia, że łatwiej byłoby skorzystać z internetu. W przygotowanie ataku socjotechnicznego przez telefon powinieneś włożyć dokładnie tyle samo wysiłku, dokładnie tak samo rzetelnie gromadzić informacje i dokładnie tak samo intensywnie ćwiczyć, jak gdybyś działał z wykorzystaniem internetu. Pracowałem kiedyś z niewielką grupą osób, z którą miałem ćwiczyć prowadzenie rozmów telefonicznych. Wskazaliśmy odpowiednie metody, ton głosu, tempo mówienia, a także konkretne zwroty i słowa, których należało używać. Przygotowaliśmy zarys scenariusza rozmowy (więcej szczegółów na ten temat już za moment), a następnie rozpoczęliśmy sesję. Pierwsza osoba sięgnęła po słuchawkę, połączyła się z kimś i pomyliła kilka pierwszych linijek. Mężczyzna był do tego stopnia zażenowany i wystraszony, że po prostu się rozłączył. Jedna

bardzo ważna uwaga: Twój rozmówca po drugiej stronie nie wie, co masz zamiar powiedzieć, dlatego tak naprawdę nie możesz „pomylić tekstu". Tego rodzaju sesje ćwiczeniowe pomogą Ci nauczyć się radzić sobie z „nieoczekiwanym", czyli z tym, co się wydarzy, kiedy niechcący odbiegniesz od przygotowanego scenariusza.

Jeśli nie dysponujesz grupą partnerów, z którymi mógłbyś ćwiczyć i doskonalić swoje umiejętności w tym zakresie, będziesz musiał wymyślić coś innego. Spróbuj dzwonić do rodziny i znajomych. Przekonaj się, w jakim stopniu uda Ci się ich zmanipulować. Możesz również nagrywać swoje wypowiedzi imitujące rozmowę telefoniczną, a następnie odsłuchiwać je i sprawdzać efekty.

Moim zdaniem zdecydowanie warto posługiwać się przygotowanym wcześniej zarysem scenariusza. Oto przykład: załóżmy, że musisz zadzwonić do swojego dostawcy usług telefonicznych lub dostawcy mediów. Firma pomyliła coś z rachunkami albo napotkałeś pewne problemy z samą usługą i zamierzasz się poskarżyć. Wyjaśniasz sytuację pracownikowi obsługi klienta i mówisz mu, jak bardzo jesteś rozczarowany i zdenerwowany zaistniałymi trudnościami. Pracownik firmy nie robi dla Ciebie absolutnie nic, stwierdza natomiast mniej więcej coś takiego: „Firma X,Y&Z dokłada wszelkich starań, aby świadczyć usługi najwyższej jakości. Czy odpowiedziałem już na wszystkie pana pytania?". Gdyby siedzący po drugiej stronie truteń choć przez chwilę zastanowił się nad tym, co mówi, musiałby zdać sobie sprawę, jakie to głupie. Mam rację? Właśnie do takich sytuacji dochodzi jednak, gdy ktoś posługuje się ścisłym scenariuszem zamiast zarysem scenariusza. Zarys zostawia miejsce na „artystyczną i kreatywną swobodę wyrazu", dzięki której możesz rozmawiać bardziej elastycznie i nie martwić się tym, co *musisz* powiedzieć w następnej kolejności.

Telefon to jedno z najskuteczniejszych narzędzi umożliwiających błyskawiczne uwiarygodnienie roli oraz zapewnienia sobie dostępu do ofiary. Przez telefon możesz udawać praktycznie wszystko. Weź pod uwagę następujący przykład: gdybym chciał do Ciebie zadzwonić i w ramach uwiarygodnienia mojej roli dać Ci do zrozumienia, że przebywam w biurze pełnym ludzi, mógłbym posłużyć się po prostu odpowiednią ścieżką audio ze strony Thriving Office (*www.thrivingoffice.com*). Znajdziesz tam na przykład ścieżki zatytułowane „Busy" (gwar) i „Very Busy" (duży gwar). Oto, co na temat tego rozwiązania mają do powiedzenia jego twórcy: „To niezwykle przydatna płyta CD z mnóstwem dźwięków i odgłosów, które ludzie spodziewają się usłyszeć w dużej, ruchliwej firmie. W ten sposób zapewnisz sobie natychmiastową wiarygodność. Proste i skuteczne! Gwarancja sukcesu!".

Już samo powyższe zdanie sugeruje potencjał socjotechniczny tej metody — „z mnóstwem dźwięków i odgłosów, które *ludzie spodziewają się usłyszeć* w dużej, ruchliwej firmie". Od razu widać, że materiały zostały przygotowane z myślą o zaspokajaniu oczekiwań rozmówców i budowaniu wiarygodności (przynajmniej

w oczach ofiary, na skutek zaspokojenia jej oczekiwań), a także automatycznego zdobywania zaufania.

Warto mieć również świadomość, że oszukanie systemu identyfikacji numerów nie stanowi większego problemu. Możesz skorzystać w tym celu z usług w rodzaju SpoofCard (*www.spoofcard.com*) lub rozwiązań „domowej roboty". Twoja ofiara może myśleć, że dzwonisz do niej z głównej siedziby konkretnej firmy, z Białego Domu albo z lokalnego banku. Dzięki tego rodzaju usługom możesz wywoływać wrażenie, że dzwonisz z dowolnego miejsca na świecie.

W rękach socjotechnika telefon staje się śmiertelnym narzędziem. Naucz się z niego korzystać i traktować go z należytym szacunkiem, a znacząco poszerzysz swój zestaw praktycznych rozwiązań pomocnych we wchodzeniu w rolę. Zadaj sobie trud zdobycia odpowiednich umiejętności w tym zakresie, ponieważ przydadzą się one przy różnych atakach socjotechnicznych.

Im prostsza rola, tym większe szanse na sukces

„Im prościej, tym lepiej" — znaczenia tej zasady nie sposób przecenić. Jeśli przygotowana rola okaże się na tyle złożona, że pominięcie jednego szczegółu zakończy się klęską całego projektu, możesz bezpiecznie założyć, że tak się właśnie stanie. Zadbaj o to, aby Twoja historia, fakty i szczegóły były jak najprostsze, ponieważ korzystnie wpłynie to na Twoją wiarygodność.

Dr Paul Ekman, znany psycholog i badacz ludzkich kłamstw, jest współautorem artykułu z 1993 roku, zatytułowanego *Lies That Fail*. Oto fragment tego tekstu:

> *Nie zawsze dysponuje się wystarczającym czasem, aby z góry przygotować sobie konkretne stwierdzenia, a następnie przećwiczyć je i zapamiętać. Nawet w sytuacji, w której czasu na przygotowania nie brakuje i można szczegółowo sformułować plan kłamstwa, kłamca może nie być na tyle bystry, aby przewidzieć wszystkie możliwe pytania, które mogą zostać mu zadane. W związku z tym nie będzie miał przygotowanych wszystkich niezbędnych odpowiedzi. Nawet największa inteligencja może okazać się niewystarczająca, ponieważ pewne nieprzewidziane zmiany okoliczności mogą obnażyć zaplanowane kłamstwo, które w innych warunkach doskonale by się sprawdziło. Potencjalna zmiana okoliczności to nie jedyny problem. Niektórzy kłamcy mają problemy z przypomnieniem sobie wszystkich kłamstw, które wygłosili wcześniej, w związku z czym napotykają trudności z szybkim i naturalnym udzielaniem odpowiedzi, które pokrywałyby się z ich wcześniejszymi stwierdzeniami.*

Ten krótki fragment najlepiej wyraża przekonanie, że im prościej, tym lepiej. Jeżeli będziesz próbował wejść w rolę tak skomplikowaną, że już jeden błąd może Cię zdemaskować, zapamiętanie całej tej roli okaże się niemal niemożliwe. Twoja rola powinna być naturalna i niczym się nie wyróżniać. Powinna być łatwa do zapamiętania. Jeśli będzie to dla Ciebie coś naturalnego, zdecydowanie łatwiej będzie Ci przypomnieć sobie wszystkie fakty i stwierdzenia wygłoszone podczas wcześniejszego wchodzenia w tę rolę.

Opowiem teraz historię, która potwierdza znaczenie zapamiętywania nawet najdrobniejszych szczegółów. Pewnego razu postanowiłem spróbować swoich sił w sprzedaży. Zostałem przydzielony do menedżera ds. sprzedaży, od którego miałem nauczyć się podstaw wykonywania tej pracy. Pamiętam, jak po raz pierwszy udałem się z nim do klienta. Kiedy zjawiliśmy się na miejscu, przed wyjściem z samochodu powiedział mi: „Pamiętaj: Becky Smith poprosiła o dodatkowe ubezpieczenie. Zaoferujemy jej polisę XYZ. Patrz i ucz się".

Przez pierwsze trzy minuty menedżer zwracał się do kobiety per Beth lub Betty. Za każdym razem, gdy używał złego imienia, zachowanie kobiety zmieniało się. Za każdym razem cichutko go poprawiała: „Becky". Sądzę, że moglibyśmy rozdawać złoto w sztabkach, a ona i tak by powiedziała: „Nie!". Tak bardzo zniechęcało ją to, że mój przełożony nie może zapamiętać jej imienia, iż w ogóle nie chciała go słuchać.

Powyższa historia najlepiej dowodzi tego, że trzeba za wszelką cenę dbać o prostotę faktów, aby ich nie pomylić.

Oprócz zapamiętywania faktów powinieneś skoncentrować się również na tym, aby wszelkie szczegóły miały jak najmniejsze znaczenie. Wejdź w prostą rolę, a scenariusz sam zacznie się rozwijać, ponieważ ofiara wykorzysta własną wyobraźnię w celu wypełnienia wszelkich luk. Nie próbuj ponad miarę rozbudowywać roli, za to koniecznie pamiętaj o istotnych szczegółach, ponieważ to od nich zależy, jak ofiara odbierze Twoją rolę.

Z drugiej strony warto zwrócić uwagę na pewną ciekawostkę: sławni przestępcy i oszuści stosują często metodę, w ramach której celowo popełniają kilka błędów. Wychodzą z założenia, że „nikt nie jest doskonały", a więc pojedyncze pomyłki powodują, że ofiara czuje się bezpieczniej. Jeśli postanowisz spróbować tego rozwiązania, uważaj, jakie błędy popełniasz — choć dzięki temu rozmowa wydaje się bardziej naturalna, zwiększasz w ten sposób stopień skomplikowania roli. Nie szafuj tą metodą, a kiedy już się na nią zdecydujesz, pamiętaj o prostocie.

Pozwól, że podsumuję ten fragment kilkoma przykładami sytuacji z moich własnych audytów lub audytów, którym miałem okazję się przyglądać. Na skutek niezwykle udanej telefonicznej próby wywoływania pewien anonimowy socjotechnik uzyskał nazwę firmy zajmującej się wywozem odpadów i nieczystości. Po kilku

chwilach spędzonych w sieci mężczyzna ten dysponował zupełnie dobrym logo, nadającym się do wydruku. W internecie znajdziesz dziesiątki firm, które wydrukują Ci takie logo na koszulkach lub czapkach z daszkiem.

Kilka minut zabawy z szablonami i koszulka oraz czapka zostały zamówione. Kilka dni później, ubrany w opatrzony logotypami strój i podkładką do notowania w ręce, nasz socjotechnik stanął przed budką strażników firmy obranej za cel.

„Witam, jestem Joe z ABC Waste. Dzwonił ktoś z waszego działu zakupów i prosił, abyśmy przysłali kogoś do sprawdzenia uszkodzonego śmietnika na tyłach. Odbiór śmieci wypada jutro, więc jeśli nie uda mi się naprawić kontenera, jutro śmieciarka przywiezie nowy. Muszę jednak najpierw przyjrzeć się temu uszkodzonemu pojemnikowi".

Strażnik bez chwili wahania stwierdził: „W porządku. Aby wjechać na teren, będziesz potrzebował tego identyfikatora. Przejedź tędy i zajedź od tyłu, bo tam stoją kontenery na śmieci".

Socjotechnik zapewnił sobie właśnie możliwość przeprowadzenia długiego i szczegółowego przeszukania śmieci, ponieważ jednak chciał maksymalnie wykorzystać swoje szanse, postanowił zadać decydujący cios. Spojrzał w swoje dokumenty i stwierdził: „Z mojej notatki wynika, że chodzi o jeden z kontenerów na dokumenty i stary sprzęt elektroniczny. Gdzie je znajdę?".

„Jedź tą samą drogą, znajdziesz je w trzeciej alejce", odparł strażnik.

„Dzięki".

Prosta rola, uwiarygodniona odpowiednim strojem i „rekwizytami" (jak podkładka pod dokumenty), a przede wszystkim prosty i łatwy do zapamiętania scenariusz — wszystko to zadecydowało o tym, że socjotechnik wypadł w swojej roli niezwykle wiarygodnie i odniósł sukces.

Do często stosowanych ról należy również rola pracownika obsługi technicznej. W tym wypadku wystarczy koszulka polo, spodnie koloru khaki oraz niewielka torba na laptopa. Wielu socjotechników stosuje to wcielenie, żeby dostać się na teren firmy, ponieważ „technikom" na ogół udostępnia się wszystko, przy czym nie nadzoruje się ich pracy szczególnie uważnie. Obowiązuje tutaj ta sama zasada: pamiętaj o prostocie, a Twoja rola będzie bardziej rzeczywista i wiarygodna.

Rola powinna robić wrażenie odgrywanej spontanicznie

Rozważania na temat spontaniczności roli, w którą zamierzasz wejść, odwołują się w zasadzie do moich uwag na temat posługiwania się raczej zarysem scenariusza zamiast sztywnym skryptem. Zarys pozostawia socjotechnikowi więcej swobody, a skrypt czyni z niego niemal robota. Źródłem spontaniczności jest również posługiwanie się rzeczami i historiami, które stanowią przedmiot Twoich faktycznych

zainteresowań. Szkodzisz swojej wiarygodności za każdym razem, gdy ktoś zadaje Ci pytanie, a Ty odpowiadasz przydługim „Hmmm", zaczynasz się intensywnie zastanawiać lub nie znajdujesz inteligentnej odpowiedzi. Oczywiście nie brakuje ludzi, którzy najpierw mówią, a dopiero potem myślą — nie chodzi zatem o to, abyś odpowiadał w ciągu jednej sekundy, lecz o to, abyś zawsze miał wiarygodną odpowiedź albo dobry powód, dla którego nie potrafisz jej udzielić. Podczas pewnej rozmowy telefonicznej zostałem zapytany o informację, którą nie dysponowałem. Odpowiedziałem wówczas: „Chwileczkę", po czym odchyliłem się do tyłu i zacząłem udawać, że krzyczę do mojej współpracowniczki: „Jill, czy możesz poprosić Billa, żeby podrzucił mi zamówienie naszego klienta XYZ? Dzięki!".

W tym samym czasie, w którym „Jill" zdobywała dla mnie ten dokument, mnie udało się uzyskać niezbędne dane i problem dokumentu już nigdy nie powrócił.

Opracowałem krótką listę sposobów, które pozwalają zachowywać się bardziej spontanicznie:

- **Nie myśl o tym, jak się czujesz**. To bardzo ważna wskazówka. Kiedy wchodzisz w rolę i zaczynasz za dużo myśleć, pojawiają się emocje, a od nich już prosta droga do strachu, podenerwowania lub niepokoju. Wszystkie te czynniki mogą stać się przyczyną Twojej porażki. Zamiast podenerwowania i lęku możesz doświadczyć także nadmiernej ekscytacji, przez którą również możesz popełnić wiele błędów.

- **Nie traktuj samego siebie zbyt poważnie**. To świetna wskazówka natury ogólnej, znajduje jednak zastosowanie także w kontekście socjotechnicznym. Jesteś profesjonalistą, specjalistą w dziedzinie bezpieczeństwa, masz poważną pracę i zajmujesz się poważną problematyką. Jeśli jednak nie nauczysz się śmiać z własnych błędów, możesz zamknąć się w sobie lub stać się zbyt nerwowy, a przez to stracić zdolność radzenia sobie nawet z najmniejszymi wybojami na drodze. Nie chcę przez to sugerować, że powinieneś traktować kwestie bezpieczeństwa jak żarty. Nie możesz jednak wychodzić z założenia, że ewentualna porażka będzie dla Ciebie jednoznaczna z porażką życiową — w ten sposób bowiem nakładasz na siebie presję, która sprowadzi na Ciebie właśnie to, czego się najbardziej obawiasz. Drobne porażki mogą stać się punktem wyjścia do wielkich sukcesów — musisz się tylko nauczyć je wykorzystywać.

- **Naucz się rozpoznawać to, co ma znaczenie**. Osobiście wolę formułować tę radę następująco: „Uwolnij się od własnych myśli i w końcu idź do ludzi" — to moim zdaniem jeszcze lepsza sugestia. Socjotechnik może planować trzy ruchy naprzód, a w międzyczasie pominąć jakiś istotny szczegół, przez co cała rola może się rozpaść. Staraj się jak najszybciej identyfikować

istotne materiały i informacje znajdujące się wokół Ciebie, bez względu na to, czy chodzi o mowę ciała Twojej ofiary, wypowiadane przez nią słowa, mikroekspresje (więcej szczegółów na ten temat znajdziesz w rozdziale 5.). Wszystkie te informacje powinieneś uwzględnić przy planowaniu ataku wybraną metodą.

Pamiętaj również, że ludzie potrafią stwierdzić, iż ktoś tylko udaje, że ich słucha. Poczucie, że nawet te mniej istotne słowa nie spotykają się z aktywnym odbiorem, w przypadku wielu osób okazuje się bardzo poważnym czynnikiem zniechęcającym. Każdy z nas z pewnością ma doświadczenia w interakcjach z osobami, których najwyraźniej w ogóle nie interesuje to, co mamy do powiedzenia. Druga osoba może mieć zupełnie dobry powód, dla którego jej myśli biegną innym torem, nie zmienia to jednak faktu, że tracimy ochotę na rozmowę z nią.

Koniecznie słuchaj, co ma do powiedzenia Twoja ofiara — słuchaj jej bardzo uważnie, a wychwycisz pewne niezwykle istotne dla niej szczegóły. Być może przy okazji usłyszysz coś, co pomoże Ci odnieść sukces.

- **Staraj się zdobywać nowe doświadczenia**. Koncepcja ta odnosi się do porady, którą znajdziesz w tej książce ze cztery miliony razy: ćwicz. Zdobywanie doświadczenia w drodze ćwiczeń i prób może zadecydować o sukcesie lub porażce roli, w którą chcesz wejść. Trenuj spontaniczność na rodzinie, przyjaciołach i zupełnie obcych osobach, kierując się wyłącznie jednym celem: zachowywać się spontanicznie. Nawiązuj rozmowy z ludźmi — uważaj tylko, żeby nie wypaść na nagabywacza. Proste, codzienne rozmowy mogą pomóc Ci poczuć się pewniej w okazywaniu spontaniczności.

Powyższe wskazówki mogą bez wątpienia zapewnić socjotechnikowi przewagę w kwestii wchodzenia w rolę. Umiejętność zachowywania się w sposób spontaniczny to prawdziwy dar. We wcześniejszych fragmentach tego rozdziału wspominałem o swojej rozmowie z Tomem Mischke, który ma bardzo ciekawe podejście do tego tematu. Powiedział on, że stara się zawsze kreować złudzenie spontaniczności opakowanej przygotowaniem i próbami. Ćwiczy i próbuje tak długo, aż kreowana rola sprawia wrażenie spontanicznego zlepku talentu i poczucia humoru.

Przedstaw ofierze logiczny wniosek lub zaproponuj dalsze działanie

Możesz w to wierzyć lub nie, ale fakt pozostaje faktem: ludzie lubią, gdy im się mówi, co mają robić. Wyobraź sobie, że idziesz do lekarza. Ten Cię bada, nanosi trochę informacji na wykres, po czym stwierdza: „W porządku. Do zobaczenia za

miesiąc". To nie do pomyślenia. Nawet gdyby miały to być złe wieści, ludzie chcą usłyszeć, co powinni robić dalej.

Socjotechnikowi może zależeć na tym, żeby po zakończeniu rozmowy jego ofiara podjęła konkretne działania albo czegoś zaniechała. Może się również zdarzyć, że socjotechnik uzyska wszystko, na czym mu zależało, i teraz chce się już tylko ewakuować. Bez względu na to, w jakich okolicznościach się znalazłeś, przedstaw ofierze jakiś logiczny wniosek lub zaproponuj działania, które pozwolą jej wypełnić ewentualne luki.

Podobnie jak lekarz nie może zbadać pacjenta i odesłać go do domu bez żadnych dalszych wskazówek, tak samo osoba podająca się za pracownika obsługi technicznej nie może wejść na teren firmy, a potem go opuścić, nic nikomu nie mówiąc, ale uprzednio sklonowawszy bazę danych — ludzie zaczęliby się zastanawiać, co się właściwie wydarzyło. Ktoś może zechcieć zadzwonić do „firmy zapewniającej wsparcie techniczne" i zapytać, czy przysłany właśnie pracownik miał jakieś konkretne zadanie. W najlepszym razie taka sytuacja wywołuje zdziwienie. Tak naprawdę wystarczy, że powiesz mniej więcej coś takiego: „Sprawdziłem serwery i naprawiłem system plików. W ciągu następnych kilku dni powinniście zauważyć wzrost szybkości rzędu około 22%". Dzięki temu ofiara będzie miała poczucie, że „dostała coś w zamian za swoje pieniądze".

Z punktu widzenia socjotechnika najtrudniej jest nakłonić ofiarę do podjęcia jakiegoś działania już po tym, gdy on opuści dane miejsce. Jeżeli działanie to ma kluczowe znaczenie dla zakończenia audytu zabezpieczeń, być może powinieneś zastanowić się nad możliwością samodzielnego podjęcia danej czynności. Wróćmy do historii opowiadającej o spotkaniu w izbie handlowej, którą przytoczyłem w rozdziale 3. Gdybym chciał, aby ofiara skontaktowała się ze mną później za pomocą poczty elektronicznej, mógłbym powiedzieć: „Oto moja wizytówka. Czy mógłbyś w poniedziałek wysłać mi e-mailem dodatkowe szczegóły na temat firmy XYZ?". Ofiara albo by spełniła moją prośbę, albo poszła do biura i zapomniała o całej sprawie, a wtedy cały mój plan spaliłby na panewce. Dlatego lepiej powiedzieć coś takiego: „Chętnie uzyskałbym od Ciebie pewne dodatkowe informacje. Czy mógłbym w poniedziałek do ciebie zadzwonić albo wysłać ci maila z prośbą o te dane?".

Formułowane prośby powinny pasować do roli, w którą wchodzisz. Jeżeli wcielasz się w pracownika obsługi technicznej, nie możesz rozstawiać ludzi po kątach, mówiąc im, co mają robić, a czego im nie wolno — w końcu to Ty pracujesz dla nich. Jeśli podajesz się za kuriera UPS, nie możesz żądać dostępu do serwerowni.

Jak już wspominałem wcześniej, na doskonalenie roli mogą składać się również inne działania, jednak te wymienione w tym rozdziale powinny zapewnić każdemu socjotechnikowi solidny fundament pod opracowanie w pełni wiarygodnej roli.

Być może zastanawiasz się teraz, co z tego wszystkiego wynika. W jaki sposób socjotechnik może stworzyć odpowiednio przygotowaną, wiarygodną, pozornie spontaniczną i prostą rolę — rolę, która będzie równie skuteczna w działaniu osobistym, jak i przez telefon, oraz która pozwoli osiągnąć zamierzone efekty? Zapoznaj się z dalszą częścią rozdziału.

Przykłady skutecznego wchodzenia w rolę

Jeżeli chcesz nauczyć się kreować udane role, przyjrzyj się dwóm historiom udanych ról, które zostały z powodzeniem opracowane i zastosowane przez socjotechników. Ostatecznie obaj zostali przyłapani i właśnie dzięki temu możemy dziś te historie opowiedzieć.

Przykład nr 1 — Stanley Mark Rifkin

Stanleyowi Markowi Rifkinowi przypisuje się największy skok na bank w historii Stanów Zjednoczonych (świetny artykuł na jego temat znajdziesz na stronie *www.social-engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer-furtherInfo.htm*). Rifkin był komputerowym maniakiem, który prowadził we własnym mieszkaniu niewielką firmę konsultingową specjalizującą się w dziedzinie IT. W gronie jego klientów znalazła się firma, która serwisowała komputery Security Pacific Bank. Pięćdziesięciopięciopiętrowa siedziba główna banku Security Pacific National Bank w Los Angeles sprawiała wrażenie prawdziwej fortecy ze szkła i granitu. Lobby strzegli ubrani na ciemno strażnicy, a klienci wpłacający i wypłacający pieniądze przez cały czas znajdowali się pod czujnym okiem ukrytych kamer.

Budynek wydawał się nie do zdobycia, więc jakim cudem Rifkin ukradł stamtąd 10,2 miliona dolarów, nigdy nie dotykając broni, nie trzymając w ręku nawet dolara i nie biorąc nikogo na muszkę?

Bankowe procedury związane z wykonywaniem przelewów wydawały się odpowiednio zabezpieczone. Transakcje były autoryzowane zmienianym codziennie kodem numerycznym, który znali wyłącznie upoważnieni pracownicy. Kody te zamieszczano na tablicy ogłoszeń w bezpiecznym pomieszczeniu, do którego dostęp miały wyłącznie „osoby upoważnione".

Oto fragment artykułu, o którym wspominałem powyżej:

> *W październiku 1978 roku Rifkin zjawił się w Security Pacific, a pracownicy banku bez problemu rozpoznali w nim specjalistę ds. komputerów. Następnie Rifkin wjechał windą na poziom D, gdzie znajdowało się pomieszczenie związane z obsługą przelewów. Sprawiał wrażenie uprzejmego młodego*

człowieka, więc udało mu się przekonać pracowników, aby wpuścili go do pomieszczenia, w którym znajdował się tajny kod autoryzacji przelewów na dany dzień. Rifkin zapamiętał kod i wyszedł, nie wzbudzając żadnych podejrzeń.

Niedługo potem pracownicy banku z pomieszczenia związanego z wykonywaniem przelewów odebrali telefon od mężczyzny, który przedstawił się jako Mike Hansen, pracownik międzynarodowego oddziału tego samego banku. Zlecił on wykonanie rutynowego przelewu środków na rachunek w nowojorskim banku Irving Trust Company, podając oczywiście tajny kod autoryzacyjny. Wszystko wydawało się być w zupełnym porządku, więc Security Pacific dokonał przelewu środków do banku w Nowym Jorku. Przedstawiciele banku nie wiedzieli jednak, że mężczyzna podający się za Mike'a Hansena to w rzeczywistości Stanley Rifkin, który za pomocą wewnętrznego kodu autoryzacyjnego obrabował właśnie bank na kwotę 10,2 miliona dolarów.

Niniejszy scenariusz stanowi niezwykle wdzięczny temat do rozważań, na razie skoncentrujmy się jednak na samej roli. Przyjrzyjmy się szczegółowo temu, co musiał zrobić Rifkin:

- Musiał być pewny siebie i zachowywać się na tyle swobodnie, żeby nikt nie zakwestionował jego prawa do przebywania w pomieszczeniu, w którym dokonywano przelewów.
- Gdy zadzwonił w celu zlecenia przelewu, musiał przedstawić wiarygodną historię i dysponować szczegółami na jej poparcie.
- Musiał zachowywać się na tyle spontanicznie, aby odpowiednio reagować na wszelkie pytania, które mogły się pojawić.
- Musiał radzić sobie na tyle sprawnie, żeby nie wzbudzić żadnych podejrzeń.

Rola ta wymagała szczegółowego planowania i przemyślenia najmniejszych detali. Rifkin został schwytany dopiero wtedy, gdy odwiedził swojego byłego wspólnika — dopiero wtedy jego rola zawiodła. Po fakcie ludzie, którzy go znali, nie kryli zdumienia: „To niemożliwe, żeby Mark był złodziejem. Wszyscy go uwielbiają".

Nie ulega wątpliwości, że Rifkin dobrze przygotował swoją rolę. Dysponował znakomicie przemyślanym i prawdopodobnie wielokrotnie przećwiczonym planem. Wiedział, co zamierza osiągnąć, a potem znakomicie wszedł w swoją rolę. W kontaktach z obcymi ludźmi radził sobie świetnie. Noga powinęła mu się dopiero, kiedy spotkał się z dawnym współpracownikiem. Mężczyzna usłyszał o napadzie w wiadomościach, zestawił fakty i zawiadomił policję.

Co ciekawe, po wyjściu z aresztu za kaucją Rifkin obrał sobie na cel kolejny bank, posługując się tym samym planem. Tym razem okazało się, że został wystawiony przez tajniaka. Został ujęty i spędził osiem lat w więzieniu federalnym. Rifkin jest bez wątpienia „czarnym charakterem", jednak na podstawie jego historii możesz się bardzo wiele nauczyć na temat wchodzenia w rolę — choćby tego, że rola powinna być jak najprostsza i że warto wykorzystać w niej to, na czym się znasz.

Rifkin miał zamiar zainwestować skradzione środki w dobra nie do wytropienia, a mianowicie w diamenty. Najpierw musiał jednak zostać pracownikiem banku, aby ukraść pieniądze, następnie wcielić się w rolę poważnego nabywcy diamentów, aby pozbyć się gotówki, a w końcu sprzedać diamenty, aby pozyskać niepodejrzaną gotówkę na bieżące potrzeby.

Jego rola nie zakładała posługiwania się wyjątkowymi strojami ani sposobami mowy. Rifkin musiał jednak odegrać najpierw pracownika banku, potem poważnego nabywcę diamentów, a na koniec poważnego ich sprzedawcę. W ramach tego przekrętu Rifkin zmieniał role trzy-, cztero-, a może nawet pięciokrotnie. Był w tym na tyle dobry, że udało mu się oszukać niemal wszystkich.

Rifkin doskonale znał swój cel i przystąpił do realizacji swoich planów z zachowaniem wszystkich opisanych powyżej zasad. Oczywiście nie można zapominać, że Rifkin prowadził działalność przestępczą, jednak jego umiejętność wchodzenia w rolę bez wątpienia może budzić podziw. Gdyby wykorzystał swoje uzdolnienia w bardziej szczytnym celu, prawdopodobnie mógłby być świetnym sprzedawcą czy aktorem albo z powodzeniem zaangażować się w życie publiczne.

Przykład nr 2 — Hewlett-Packard

W 2006 roku „Newsweek" opublikował niezwykle ciekawy artykuł (*www.social-engineer.org/resources/book/HP_pretext.htm*). W dużym skrócie chodziło o to, że Patricia Dunn, wiceprezes firmy HP, zatrudniła zespół specjalistów ds. bezpieczeństwa, którzy pozyskali do współpracy zespół detektywów, a ci z kolei posłużyli się metodą wchodzenia w rolę w celu uzyskania billingów telefonicznych. Zatrudnieni profesjonaliści odegrali role członków zarządu HP oraz role dziennikarzy, a wszystko po to, aby wykryć rzekomy przeciek w szeregach HP.

Patricia Dunn chciała uzyskać dostęp do billingów telefonicznych członków zarządu oraz reporterów (nie chodziło o billingi połączeń wykonanych z wewnętrznych telefonów HP, lecz o spisy połączeń z prywatnych linii domowych oraz telefonów komórkowych). Chciała ustalić, gdzie ma miejsce rzekomy przeciek. Oto fragment artykułu opublikowanego w „Newsweeku":

18 maja w siedzibie głównej HP w Palo Alto w Kalifornii Dunn przedstawiła zarządowi swoje rewolucyjne wieści: znalazła osobę odpowiedzialną za przeciek. Według relacji Toma Perkinsa, członka zarządu HP i naocznego świadka tamtych wydarzeń, Dunn ujawniła swoją siatkę szpiegowską i wskazała na jednego z członków zarządu, który przyznał, że rzeczywiście przekazywał informacje dziennikarzom portalu CNET. Członek zarządu, którego tożsamości na razie nie ujawniono, przeprosił za swoje zachowanie, a następnie stwierdził: „Przecież sam bym wam o tym wszystkim powiedział. Wystarczyło po prostu zapytać". Jak relacjonuje Perkins, osoba ta została poproszona o rezygnację z pełnionej funkcji i tak też zrobiła.

Szczególnie ciekawym aspektem tej historii wydaje się kontekst, w jakim wykorzystano metodę wchodzenia w rolę:

Przykład firmy HP rzuca nieco światła na wątpliwe praktyki stosowane przez konsultantów ds. bezpieczeństwa w celu pozyskiwania danych o charakterze osobistym. Firma HP poświadczyła w wewnętrznym e-mailu, wysłanym Perkinsowi przez niezależnego konsultanta, że dowody obwiniające członka zarządu przekazującego informacje portalowi CNET udało się uzyskać dzięki zastosowaniu kontrowersyjnej metody, zwanej „wchodzeniem w rolę". „Newsweekowi" udało się dotrzeć do kopii tej wiadomości. Federal Trade Commission definiuje tę praktykę jako posługiwanie się „fałszywymi przesłankami" w celu uzyskania osobistych i prywatnych danych na temat danej osoby, takich jak billingi telefoniczne, numery rachunków bankowych i kart kredytowych, numer ubezpieczenia społecznego itp.

Zazwyczaj odbywa się to w ten sposób, że osoba wcielająca się w rolę dzwoni na przykład do firmy telefonicznej i podszywa się pod jej klienta. Tego rodzaju firmy rzadko oczekują od swoich klientów posługiwania się hasłami, osoba stosująca metodę wchodzenia w rolę nie musi dysponować żadnymi wyszukanymi danymi — wystarczą adres domowy, numer konta oraz uprzejma prośba o udostępnienie szczegółowych danych o tym koncie. Według informacji opublikowanych na stronie internetowej Federal Trade Commission osoby stosujące tę praktykę sprzedają pozyskane dane wielu różnym osobom, od legalnie działających prywatnych detektywów, pożyczkodawców, stron potencjalnych procesów sądowych i podejrzliwych małżonków, aż po ludzi, którzy mogą próbować kogoś okraść lub dopuścić się oszustwa kredytowego. FTC stwierdza, że posługiwanie się metodą wchodzenia w rolę „jest niezgodne z prawem". Przedstawiciele FTC oraz kilku prokuratorów stanowych wydało walkę osobom

> *stosującym te praktyki w związku z podejrzeniem o naruszenie federalnych i stanowych przepisów dotyczących oszustw, podszywania się pod inne osoby oraz nieuczciwej konkurencji. W gronie członków zarządu HP znajduje się Larry Babbio, prezes firmy Verizon, która podejmuje liczne kroki prawne przeciwko osobom zaangażowanym w ten proceder.*

(Jeżeli masz ochotę zgłębiać szczegółowo prawne aspekty tego zagadnienia, tekst ustawy Telephone Records and Privacy Protection Act z 2006 roku znajdziesz pod adresem *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4709enr.txt.pdf*).

Końcowy efekt był taki, że zarzuty postawiono nie tylko pani Dunn, lecz również zatrudnionym przez nią konsultantom. Ktoś może się zastanawiać, jak to możliwe, skoro zostali oni zatrudnieni do wykonania tych testów.

Jeśli podobna wątpliwość zrodziła się również w Twojej głowie, przyjrzyj się temu, z jakich metod ci konsultanci korzystali i jakie pozyskali informacje. Były to nazwiska, adresy, numery ubezpieczenia społecznego, billingi telefoniczne oraz inne dane na temat członków zarządu HP oraz dziennikarzy. Posunęli się nawet do wykorzystania numeru ubezpieczenia społecznego w celu założenia konta internetowego jednemu z dziennikarzy, aby uzyskać w ten sposób informacje o jego prywatnych rozmowach telefonicznych.

Na 32. stronie poufnego dokumentu wewnętrznego HP wystosowanego do prawnika firmy oraz jej działu prawnego (*www.social-engineer.org/resources/book/20061004hewlett6.pdf*) znajduje się wiadomość skierowana przez Toma Perkinsa do członków zarządu HP. Można się z niej dowiedzieć nieco więcej o tym, jakie role zostały wykorzystane. Oto przykłady kilku wybranych metod:

- Konsultanci podawali się za przedstawicieli operatora telefonicznego, aby w sposób niezgodny z prawem uzyskać dostęp do danych na temat połączeń.
- Wykorzystali tożsamość obserwowanych osób, podszywając się pod nie w celu uzyskania informacji o prywatnych rozmowach telefonicznych.
- Na stronach operatorów telefonicznych zakładali konta internetowe, dzięki którym niezgodnie z prawem pozyskiwali nazwiska, numery ubezpieczenia społecznego oraz inne dane niezbędne do uzyskania dostępu do billingów.

11 września 2006 roku pani Dunn otrzymała list z United States House of Representatives Committee on Energy and Commerce (kopię tego listu znajdziesz pod adresem *www.social-engineer.org/resources/book/20061004hewlett6.pdf*) z prośbą

o przekazanie informacji, które udało jej się zdobyć. W dokumencie tym wymieniono następujące rodzaje danych, które miały zostać przekazane:

- wszystkie publiczne i zastrzeżone numery telefonów,
- wyciągi z kart kredytowych,
- dane osobowe i adresowe klientów,
- rachunki za media,
- numery pagerów,
- numery telefonów komórkowych,
- numery ubezpieczenia społecznego,
- zestawienia bilansowe,
- informacje o numerach skrzynek pocztowych,
- informacje o rachunkach bankowych,
- informacje majątkowe,
- inne informacje o charakterze konsumenckim.

Wszystkie te dane pozyskano w sposób, który w najlepszym wypadku można by zakwalifikować do bardzo szarej strefy socjotechniki. Czy zważywszy na to, że konsultanci wykonywali pracę na zlecenie, ich postępowanie można uznać za moralnie i etycznie uzasadnione? Wielu profesjonalnych socjotechników nie zdecydowałoby się na tak daleko idące działania. Wniosek z tego taki, że w zawodzie socjotechnika można kopiować i naśladować sposób myślenia złośliwych socjotechników, nigdy nie można się jednak zniżać do ich poziomu. Problemy tych konsultantów wynikły z tego, że byli oni upoważnieni do wcielania się w różne role w celu wykonania audytu w HP, nie powinni natomiast podejmować tych samych działań w stosunku do firm AT&T, Verizon, dostawców mediów itd. Przystępując do wcielania się w rolę, musisz uprzednio wszystko dokładnie zaplanować i wiedzieć, do jakich granic prawnych możesz się zbliżyć i których z nich nie wolno Ci przekroczyć.

Historia firmy HP prowokuje do rozważań na temat polityki, warunków umownych oraz Twojej oferty jako audytora zabezpieczeń, jednak zagadnienia te wykraczają poza zakres tematyczny tego rozdziału. Przestrzegaj zasad w nim opisanych, a łatwiej Ci będzie podejmować decyzje, które nie ściągną na Ciebie kłopotów.

Ze stosowaniem metody złośliwego wchodzenia w rolę wiąże się ryzyko dokonania kradzieży tożsamości, w związku z czym mamy tu do czynienia z ważnym

elementem socjotechnicznego testu penetracyjnego. Testowanie, sprawdzanie i weryfikacja tego, czy pracownicy firmy będącej Twoim klientem dadzą się złapać na metody stosowane przez złośliwych socjotechników, mogą zdecydowanie pomóc w skutecznym zabezpieczeniu organizacji przed tego rodzaju atakami.

Jak nie łamać prawa?

W 2005 roku „Private Investigator Magazine" przeprowadził wywiad z Joelem Winstonem, dyrektorem Division of Financial Practices wchodzącej w skład Federal Trade Commission (FTC). Jego biuro odpowiada za regulowanie i monitorowanie posługiwania się metodą wchodzenia w rolę (z tym niezwykle ciekawym artykułem możesz się zapoznać na stronie *www.social-engineer.org/resources/book/ftc_article.htm*).

Oto kilka najciekawszych kwestii poruszonych w tym tekście:

- Zgodnie ze stanowiskiem FTC metoda wchodzenia w rolę polega na pozyskiwaniu *wszelkiego rodzaju informacji* od banków lub konsumentów, a więc również informacji o charakterze niefinansowym, z wykorzystaniem oszustwa, fałszu lub mylących pytań.
- Posługiwanie się pozyskanymi już informacjami w celu dokonania weryfikacji tożsamości ofiary, nawet z wykorzystaniem fałszywych przesłanek, jest zgodne z definicją legalnego posługiwania się metodą wchodzenia w rolę. Wyjątek stanowi podejmowanie tego rodzaju działań w stosunku do instytucji finansowych, ponieważ w tej sytuacji będziemy mieć do czynienia z naruszeniem prawa.
- Pozyskiwanie billingów z budek telefonicznych oraz telefonów komórkowych z wykorzystaniem zwodniczych praktyk biznesowych jest uznawane za nielegalny przejaw stosowania metody wchodzenia w rolę.

Dodatkowe wyjaśnienia oraz nowe informacje znaleźć można na stronie internetowej FTC:

- Niezgodne z prawem jest posługiwanie się przez kogokolwiek informacjami i dokumentami fałszywymi, fikcyjnymi lub podawanymi z myślą o dokonaniu oszustwa w celu pozyskania danych o klientach od instytucji finansowych lub bezpośrednio od klientów tych instytucji.
- Niezgodne z prawem jest posługiwanie się przez kogokolwiek podrobionymi, fałszywymi, utraconymi lub skradzionymi dokumentami w celu pozyskania informacji o klientach od instytucji finansowych lub bezpośrednio od klientów tych instytucji.

» Niezgodne z prawem jest kierowanie pod adresem drugiej osoby próśb o pozyskanie należących do kogoś innego danych o klientach z wykorzystaniem informacji i dokumentów fałszywych, fikcyjnych lub podawanych z myślą o dokonaniu oszustwa lub z wykorzystaniem podrobionych, fałszywych, utraconych lub skradzionych dokumentów.

FTC koncentruje swoją uwagę na instytucjach finansowych, jednak powyższe regulacje pozwalają zorientować się co do tego, jakie praktyki ogólnie uważa się w Stanach Zjednoczonych za niezgodne z prawem. Profesjonalny socjotechnik zawsze powinien zapoznać się z przepisami obowiązującymi w danym miejscu i podejmować działania wyłącznie w granicach prawa. W 2006 roku Federal Trade Commission wniosła o rozszerzenie rozdziału 5. ustawy FTC Act o konkretne przepisy zakazujące stosowania metody wchodzenia w rolę w celu pozyskiwania billingów telefonicznych.

Historia z udziałem HP zakończyła się postawieniem jednemu z zatrudnionych socjotechników zarzutów spisku oraz kradzieży tożsamości (przestępstwo federalne) — to naprawdę poważne zarzuty.

Profesjonalny socjotechnik, który chce działać zawsze w granicach prawa, będzie musiał trochę poszperać, a następnie opracować precyzyjny i *zatwierdzony* plan zastosowania metody wchodzenia w rolę, jeśli takie działania zostały w ogóle przewidziane.

Abstrahując od wspomnianych tu problemów natury prawnej, posługiwanie się odpowiednio przygotowaną rolą stanowi jeden z najszybszych sposobów na uzyskanie dostępu do interesującej nas firmy. Umiejętność posługiwania się tą metodą sama w sobie jest sztuką — nie polega wyłącznie na założeniu peruki i okularów oraz udawaniu kogoś innego.

Dodatkowe narzędzia przydatne przy wchodzeniu w rolę

Istnieją również inne narzędzia pomocne przy stosowaniu tej metody.

W celu dodania sobie wiarygodności w nowej roli możesz posługiwać się rekwizytami, takimi jak magnetyczne napisy na samochód, odpowiednie stroje i mundury, narzędzia i inne rzeczy, które nosisz ze sobą, czy wreszcie najważniejszym — wizytówką.

Z potencjału tego kartonika zdałem sobie sprawę dopiero niedawno, kiedy leciałem w interesach do Las Vegas. Na lotniskach moja torba na laptopa zwykle zostaje zeskanowana, potem zeskanowana ponownie, skontrolowana pod kątem materiałów wybuchowych i nie wiadomo czego jeszcze. Należę do ludzi, którym te dodatkowe środki bezpieczeństwa nie przeszkadzają — dzięki nim udaje mi się nie wylecieć w powietrze wraz z samolotem, z czego jestem dość zadowolony.

Wiem jednak, że w 90% przypadków mogę być pewien, że pracownicy kontroli bezpieczeństwa wykażą mną szczególne zainteresowanie. Przy okazji tamtej podróży miałem przy sobie skaner RFID, cztery dodatkowe twarde dyski, klucze uderzeniowe (więcej szczegółów na ich temat w rozdziale 7.) oraz mnóstwo różnego sprzętu do hakingu bezprzewodowego. Wszystko to miałem w torbie na laptopa, zgłoszonej jako bagaż podręczny. Jestem więc na lotnisku, a moja torba przejeżdża przez skaner i wtedy słyszę, jak kobieta oglądająca jej wnętrze mówi: „Co to do diabła jest?".

Kobieta wzywa następnego mężczyznę, który wpatruje się w ekran i stwierdza: „Nie mam zielonego pojęcia, co to wszystko jest". Mężczyzna rozgląda się, dostrzega moją uśmiechniętą twarz i pyta: „To pana?".

Podchodzę z nim do stołu. Pracownik ochrony wyjmuje skaner RFID oraz imponującą kolekcję wytrychów, po czym pyta: „Dlaczego ma pan to wszystko przy sobie i co to w ogóle jest?".

Nie przygotowałem wcześniej żadnej konkretnej odpowiedzi, więc w ostatniej chwili decyduję się na takie oto posunięcie — wyciągam wizytówkę i mówię: „Jestem konsultantem ds. bezpieczeństwa, specjalizującym się w testowaniu sieci, budynków i ludzi pod kątem luk w zabezpieczeniach. To wszystko narzędzia potrzebne mi w pracy". Wręczam mężczyźnie wizytówkę, ten patrzy na nią przez jakieś pięć sekund, po czym odpowiada: „W porządku. Dziękuję za wyjaśnienia".

Potem odkłada wszystko ostrożnie do torby, zapina ją i puszcza mnie dalej. Zazwyczaj przechodzę jeszcze kontrolę bombową, test urządzeniem wykrywającym ślady prochu i innych substancji, a na koniec jestem jeszcze obszukiwany ręcznie — tym razem jednak usłyszałem szybkie „dziękuję" i mogłem iść dalej. Zacząłem się zastanawiać, co takiego zrobiłem inaczej niż zwykle. Jedyna różnica polegała na tym, że posłużyłem się wizytówką. Nie jest to oczywiście najtańszy promocyjny wariant wizytówki, zaskoczyło mnie jednak, że ten mały kartonik tak znacząco uwiarygodnił moje słowa.

Przed czterema kolejnymi lotami celowo spakowałem wszystkie możliwe przyrządy hakerskie, nie zapominając włożyć do kieszeni wizytówki. Za każdym razem, gdy badano mój bagaż, szybko wyciągałem wizytówkę. Za każdym razem otrzymywałem przeprosiny, mój bagaż zostawał ponownie elegancko spakowany i mogłem iść dalej.

Wyobraź sobie teraz, że we wszystkich tych sytuacjach wcielałbym się w rolę. Kilka szczegółów do tego stopnia uwiarygodnia moje słowa, że nagle staję się dla kontrolerów porządnym, godnym zaufania człowiekiem. Jedna wizytówka powoduje, że wszystkie moje słowa zostają uznane za prawdziwe. Stąd też dobra rada: nie ignoruj potencjału wizytówki, a jednocześnie słowo przestrogi: wyrabiając sobie kiepsko wyglądającą wizytówkę, możesz osiągnąć efekt dokładnie odwrotny od

zamierzonego. Wizytówka, którą wyrobiłeś „za darmo", a która ma na odwrocie reklamę, raczej nie zwiększy Twojej wiarygodności jako profesjonalisty. Nie ma jednak żadnego powodu, dla którego powinieneś wydawać majątek na wizytówki jednorazowego zastosowania. Poszukaj firmy internetowej, która zaoferuje Ci niewielką ilość wizytówek w przystępnej cenie.

Kolejny powód, dla którego warto poważnie podchodzić do zagadnień omówionych w tym rozdziale, ma związek z faktem, że metodą wchodzenia w rolę często posługują się profesjonalni złodzieje tożsamości. Ostatnio tego rodzaju przestępstwa wyraźnie pną się w rankingach, więc konsumenci, firmy i profesjonaliści zajmujący się bezpieczeństwem powinni tym bardziej poszerzać swoją wiedzę w tym zakresie. Jeżeli zajmujesz się audytowaniem systemów bezpieczeństwa, Twoje zadanie polega na wspieraniu klientów w poszerzaniu wiedzy na temat tego rodzaju zagrożeń oraz w identyfikacji potencjalnych luk w ich zabezpieczeniach.

Podsumowanie

W tym rozdziale skupiłem się na metodzie wchodzenia w rolę oraz przedstawianiu z życia wziętych przykładów jej stosowania, nieustannie nawiązywałem jednak także do psychologicznych aspektów korzystania z tego rozwiązania. Stąd też kolejny element naszego modelu socjotechniki dotyczy mentalnych kompetencji, jakie musi posiadać profesjonalny socjotechnik, aby stać się mistrzem kontrolowania umysłów i znacząco zwiększyć skuteczność podejmowanych przez siebie działań.

Skorowidz

G

H

I

K

L

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ź

POKRĘTNY LABIRYNT SOCJOTECHNIKI

Ludzki umysł to najmocniejszy element każdego systemu.
Ludzki umysł to najsłabszy element każdego systemu.

Brzmi paradoksalnie? A jednak bez względu na to, jak skomplikowane zabezpieczenia ustanowisz, Twoje przedsięwzięcie może się nie powieść właśnie z winy infrastruktury ludzkiej. Człowiek funkcjonuje według pewnych schematów, które można z powodzeniem rozgryźć. A złośliwy socjotechnik, dysponujący odpowiednimi umiejętnościami, to przeciwnik, przed którym niemal nie sposób się obronić.

Poznaj pierwszy na świecie model socjotechniki. Autor tej książki definiuje, wyjaśnia i rozkłada go na cząstki elementarne, a następnie ilustruje zagadnienie, przytaczając analizy i prawdziwe historie. Zabierze Cię na wycieczkę po ciemnych zaułkach społeczeństwa, gdzie żyją szemrane typy. Przedstawi Ci mroczne arkana socjotechniki stosowanej przez szpiegów i oszustów. Będziesz podglądać nawet takich mistrzów jak Kevin Mitnick, autor książki *Sztuka podstępu*. Przyjrzysz się także powszechnym, codziennym sytuacjom pod kątem scenariuszy socjotechnicznych. W ostatniej części znajdziesz „tajemne" porady i wskazówki profesjonalnych socjotechników, a czasem również prawdziwych przestępców.

SEKRETY OSZUSTÓW I SOCJOTECHNIKÓW

- Model komunikacji i jego geneza
- Wykorzystywanie wpływu alkoholu
- Wchodzenie w rolę, czyli jak zostać tym, kim chcesz
- Sztuczki socjotechniczne — psychologiczne zasady stosowane w socjotechnice
- Programowanie neurolingwistyczne (NLP)
- Pięć podstaw wywierania wpływu
- Tworzenie programu podnoszenia świadomości osobistych zagrożeń
- Wyczulenie na złośliwe taktyki
- Dalajlama i socjotechnika

Christopher Hadnagy jest głównym twórcą Social-Engineer.org, pierwszego modelu socjotechniki. Ma wieloletnie doświadczenie w branży systemów zabezpieczeń oraz IT. Współpracował z zespołem www.backtrack-linux.org i brał udział w licznych projektach związanych z bezpieczeństwem. Pracuje również jako szkoleniowiec i główny socjotechnik w grupie penetracyjnej Offensive Security.

książkiklasybusiness

one press

Księgarnia internetowa:
http://onepress.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

Sprawdź najnowsze promocje:
http://onepress.pl/promocje
Książki najchętniej czytane:
http://onepress.pl/bestsellery
Zamów informacje o nowościach:
http://onepress.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: onepress@onepress.pl
http://onepress.pl

ISBN 978-83-283-3315-4

cena 59,00 zł