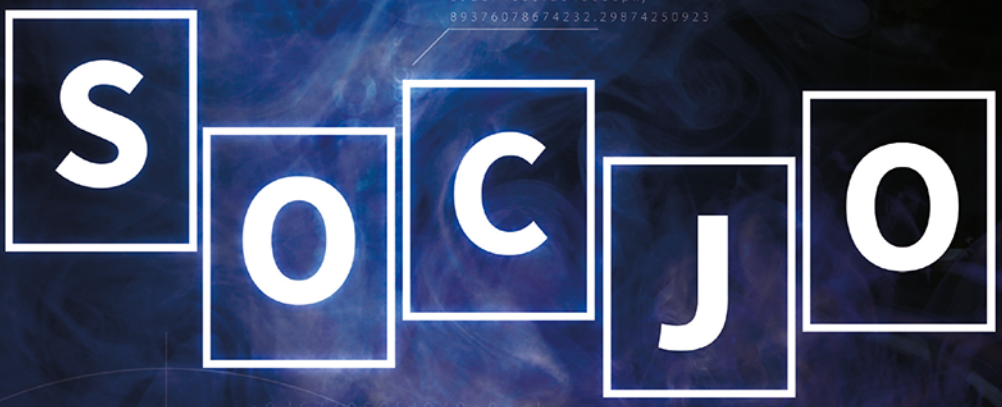
WILEY

Wydanie II



TECHNIKA

Sztuka zdobywania władzy **nad umysłami**

CHRISTOPHER HADNAGY

PRZEDMOWA: STEVE „WOZ" WOZNIAK

onepress

Helion

Tytuł oryginału: Social Engineering: The Science of Human Hacking, 2nd Edition

Tłumaczenie: Cezar Matkowski

ISBN: 978-83-283-9576-3

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW: *https://onepress.pl* (księgarnia internetowa, katalog książek)

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

Printed in Poland.

SPIS TREŚCI

1 Rzut oka na *nowy* świat zawodowej socjotechniki

Sądzę, że twoim sukcesem jest bezpieczeństwo,
a kluczem do sukcesu jest wyrobione podniebienie.

— GORDON RAMSAY

Wciąż doskonale pamiętam, jak siedziałem przed ekranem komputera, rozpoczynając pisanie pierwszego akapitu książki *Socjotechnika. Sztuka zdobywania władzy nad umysłami*. Było to w 2010 roku. Kusi mnie, aby powiedzieć, że w tamtych czasach pisaliśmy teksty na maszynach do pisania, a do redakcji i z powrotem mieliśmy pod górę, ale nie chcę popadać w nadmierny dramatyzm.

Były to jednak czasy, kiedy wpisanie w wyszukiwarkę terminu „socjotechnika" pozwalało znaleźć co najwyżej kilka stron na temat legendarnego Kevina Mitnicka lub wskazówki na temat otrzymania darmowego burgera bądź zwiększenia swoich szans na umówienie się z dziewczyną. Minęło zaledwie osiem lat, a *socjotechnika* — bądź inaczej: *inżynieria społeczna* — stała się powszechnym tematem rozmów. W ciągu ostatnich trzech lub czterech lat widziałem jej rozmaite zastosowania w dziedzinie bezpieczeństwa, administracji, edukacji, psychologii, wojskowości i wielu innych.

Co przyczyniło się do tej zmiany? Jeden z moich kolegów utrzymuje, że to moja wina. Możliwe, że chciał mnie obrazić, choć ja odebrałem to jako komplement, mimo że wcale nie czuję się jedynym twórcą *socjotechniki*. Moim zdaniem jej popularność wynika nie z faktu, że jest to najłatwiejszy sposób ataku (gdyż tak było i siedem lat temu), lecz dlatego, iż tego rodzaju atak zapewnia najwyższe zyski dla osób go podejmujących.

Koszty ataku socjotechnicznego są bardzo niskie, ryzyko jest jeszcze mniejsze, zaś możliwe do osiągnięcia korzyści są *ogromne*. Mój zespół regularnie zbiera informacje o takich atakach i przeszukuje sieć w poszukiwaniu statystyk. Z przekonaniem mogę powiedzieć, że 80% wykrytych w roku 2017 naruszeń bezpieczeństwa zawierało komponent socjotechniki.

Według publikowanych przez IBM raportów dotyczących kosztów naruszenia bezpieczeństwa danych, średni koszt takiego zdarzenia wynosi 3,62 miliona dolarów

amerykańskich. Jeżeli w grę wchodzą tak wielkie zyski, trudno nie zgadnąć, dlaczego wykorzystanie socjotechniki stanowi tak kuszącą opcję.

WSKAZÓWKA **IBM przygotowuje raporty poświęcone kosztom naruszenia bezpieczeństwa danych („Cost of Data Breach Study") od 2005 roku. Można je znaleźć na stronie *https://www-03.ibm.com/security/data-breach/* bądź wpisując angielski tytuł w wyszukiwarkę, aby znaleźć i pobrać pełny raport bieżący.**

Pamiętam jeden z wywiadów udzielonych przeze mnie krótko po opublikowaniu mojej książki *Socjotechnika. Sztuka zdobywania władzy nad umysłami* w roku 2010. Zapytano mnie wtedy, czy nie obawiam się, że publikując ją, udostępniam przestępcom groźną broń. Odpowiedziałem, że socjotechnika nie różni się od innych metod walki.

Aby zilustrować moją opinię, pozwól, że przywołam historię Bruce'a Lee, który przyjechał do USA w latach 60. XX wieku. W tamtych czasach uprzedzenia rasowe były na porządku dziennym, zaś Bruce robił coś, czego nie robił nikt inny: uczył Jeet Kune Do (starożytnej chińskiej sztuki walki) absolutnie każdego chętnego, niezależnie od narodowości, pochodzenia czy koloru skóry. Pewnego razu zorganizował sparing ze studentami, którym wydawało się, że wiedzą coś o sztukach walki, ale Bruce Lee wyszedł zwycięsko ze wszystkich starć. Niedługo później część z jego przeciwników zaprzyjaźniła się z nim lub zaczęła pobierać u niego nauki.

Jaki z tego morał? Ludzie muszą zaadaptować się do nowych reguł walki, albo będą wiecznie przegrywać. Czy istniało ryzyko, że któryś z uczniów Bruce'a wykorzysta swoje nowe zdolności do czynienia zła? Oczywiście. Mimo to Bruce Lee uważał, że należy uczyć ludzi, aby mogli skutecznie bronić się przed napaścią.

Dziś nie odpowiedziałbym na wspomniane wyżej pytanie w żaden inny sposób. Nie mam kontroli nad tym, w czyje ręce wpadnie moja książka. Jeśli chcesz, możesz wykorzystać zawarte w niej informacje do okradania innych, ale równie dobrze możesz pomóc im się obronić przed potencjalnym atakiem. Wybór należy do ciebie. Aby jednak kogoś obronić, musisz się najpierw skądś nauczyć, jak to robić.

Nauka obrony przez atakiem IS jest trudniejsza niż nauka radzenia sobie w bójce. Podobnie jak w Jeet Kune Do, należy wiedzieć, jak wygląda skuteczny atak, jak wygląda właściwa obrona i kiedy wykorzystywać każdą z tych technik. Dzięki temu w miarę poznawania tajników inżynierii społecznej będziesz w stanie myśleć jak zły człowiek, nie zapominając o tym, że chcesz czynić dobro. Innymi słowy — pozwolę sobie ukraść jeszcze jedną analogię — nauczysz się, jak używać mocy, nie przechodząc przy tym na jej ciemną stronę.

W tym momencie możesz zapytać, dlaczego opublikowałem nowe wydanie tej książki, skoro moja opinia na temat jej zawartości nie uległa zmianie. Pozwól, że wyjaśnię.

Co się zmieniło?

Powyższe pytanie gra w socjotechnice kluczową rolę. Owszem, ogólna odpowiedź brzmi „niewiele". Ludzie wykorzystują IS od zarania dziejów. Już w najstarszej części Starego Testamentu datowanym na okolice XVIII wieku p.n.e. możemy przeczytać o Jakubie, który chciał uzyskać błogosławieństwo przeznaczone dla swojego brata Ezawa. Wiedząc, że ojciec jest niemal ślepy i musi polegać na innych zmysłach, Jakub ubrał się w strój brata i przyrządził ojcu potrawę, którą zwykle przygotowywał Ezaw. Co więcej, wiedząc, że jego brat jest znacznie bardziej kędzierzawy, Jakub założył na ramiona owczą skórę. W ten sposób udało mu się oszukać ojca, który opierając się na swoim dotyku, smaku i powonieniu uznał, że błogosławi Ezawa. Jak wiemy z dalszej lektury Księgi Rodzaju, atak dokonany przez Jakuba okazał się skuteczny!

W najstarszych źródłach historycznych możemy znaleźć przykłady ludzi kłamiących, naciągających i oszukujących się wzajemnie. Stąd też na pierwszy rzut oka można uznać, że inżynieria społeczna nie zmieniła się od dawna, co nie oznacza jednak, iż zmiany takie nie mają miejsca.

Jednym z przykładów jest *vishing*. Pamiętam, że kiedy po raz pierwszy użyłem tego słowa, ludzie patrzyli na mnie, jakbym mówił po klingońsku. Równie dobrze mógłbym powiedzieć *laH yIlo' ghogh HablI' HIv* (miłośnicy Star Treka docenią). W roku 2015 słowo *vishing* zostało zaś dodane do *Oksfordzkiego Słownika Języka Angielskiego*.

WSKAZÓWKA **Klingoński to język fikcyjny, chociaż istnieje instytut zajmujący się nauczaniem, tłumaczeniem i używaniem języka klingońskiego (*www.kli.org*). W sieci można też znaleźć wiele aplikacji tłumaczących z klingońskiego i na klingoński. Do tej pory nie słyszałem jeszcze o żadnym ataku IS przeprowadzonym w tym języku.**

Dodanie słowa *vishing* do oficjalnego słownika jest ważnym wydarzeniem, ponieważ pokazuje, jak inżynieria społeczna wpływa na świat, w którym żyjemy. Słowa, które kiedyś wydawały się wyrażeniami fikcyjnymi, dziś wchodzą do naszego codziennego języka.

Zmiany w języku to nie jedyna powszechna zmiana. Dziś można bowiem skorzystać z wielu usług ułatwiających przestępcom prowadzenie nieetycznego lub nielegalnego procederu. Pracując dla jednego z klientów, zetknąłem się z dostępną 24 godziny na dobę usługą oferującą automatyczne sprawdzanie pisowni w e-mailach phishingowych. Dodajmy do tego fakt, iż w dzisiejszych czasach każdy nosi przy sobie jakieś przenośne urządzenie będące w istocie małym, ale bardzo zaawansowanym komputerem, a duża część ludzi jest wprost uzależniona od mediów społecznościowych

i możemy łatwo zobaczyć, że takie zestawienie okoliczności otwiera nowe pole do manewru dla osoby przeprowadzającej atak IS.

Nie tylko nasze otoczenie ulega zmianom. Sam również zmieniłem się przez ostatnie lata. Kiedy pisałem pierwsze wydanie niniejszej książki, jej tytuł brzmiał *Social Engineering: The Art of Human Hacking*. Wybrałem ten tytuł, gdyż wydawało mi się, że opisywane przeze mnie kwestie mocno przypominały sztukę. Ta zaś jest relatywna i dla różnych ludzi może oznaczać różne rzeczy. Można ją różnie stosować i traktować, można kochać i nienawidzić, zależnie od naszych preferencji.

Niniejsze wydanie nosi tytuł *Social Engineering: The Science of Human Hacking*. Słownik Merriam-Webster definiuje *naukę* jako: „Stan wiedzy: wiedzę stanowiącą przeciwieństwo ignorancji bądź niezrozumienia". Osiem lat temu wszystko, czego uczyłem, było praktycznie nieznane w środowisku specjalistów od bezpieczeństwa, zaś ja sam uczyłem się na bieżąco. Obecnie zaś znajduję się w „stanie wiedzy" dzięki paru latom doświadczenia w branży.

Mam nadzieję, że doświadczenie to sprawi, iż niniejsza książka będzie dla Ciebie bardziej użyteczna, niezależnie od tego, czy zawodowo zajmujesz się bezpieczeństwem, jesteś chcącym poszerzyć swoje horyzonty amatorem, czy też pracujesz jako nauczyciel i starasz się zrozumieć problemy poruszane w czasie lekcji. Powód, dla którego sięgasz po tę książkę, jest jednak nieistotny — mam nadzieję, że myśląc o przedstawionych w niej zagadnieniach w sposób bardziej naukowy, będę w stanie przedstawić je w bardziej przekrojowy i użyteczny sposób.

Dlaczego warto przeczytać tę książkę?

Uważam, że pierwszy rozdział powinien wyglądać tak jak w poprzednim wydaniu, dlatego też chciałbym poświęcić nieco czasu na wytłumaczenie, dlaczego ktoś miałby zapoznać się z niniejszą książką. Tak, wiem, że mam w tym swój interes, ale pozwól mi na drobne wyjaśnienie.

Czy jesteś człowiekiem? Nie pomylę się chyba, jeśli założę, że jeżeli masz przed sobą tę książkę i czytasz niniejszy akapit, jesteś albo niezwykle zaawansowaną sztuczną inteligencją, albo człowiekiem. Pozwolę sobie na stwierdzenie, że 99,9999999% czytelników to ludzie. Inżynieria społeczna zajmuje się zaś ludzkimi mechanizmami podejmowania decyzji i wykorzystywaniem wrażliwych elementów tych procesów.

Celem każdego socjotechnika jest sprawienie, aby jego cel podjął decyzję, nie myśląc, gdyż im dłużej myślisz, tym więcej masz szans na zauważenie próby manipulacji, co, rzecz jasna, jest bardzo niekorzystne dla atakującego. W rozdziałach 7. i 70. podcastu *The Social-Engineer Podcast* miałem okazję gościć dr Ellen Langer, która wyjaśnia różnice pomiędzy trybem alfa a trybem beta.

Tryb alfa oznacza pracę mózgu z częstotliwością 8 – 13 cyklów/s. Jest on zwykle nazywany „marzeniem na jawie" bądź, jak ujęła to dr Langer, „odprężeniem połączonym z uważną koncentracją".

Cykl beta oznacza częstotliwość w zakresie 14 – 100 cyklów/s. W trybie tym nasze mózgi są czujne, spostrzegawcze i świadome tego, co się dzieje w naszym otoczeniu.

WSKAZÓWKA

Poniżej możesz znaleźć odnośniki do odcinków podcasta, w których rozmawiam z dr Ellen Langer:

- **Odcinek 7. zawiera mój pierwszy wywiad z dr Ellen Langer, w którym omawiamy jej badania i książki: *www.social-engineer.org/podcast/episode-007-using-persuasion-on-the-mindless-masses/***
- **Odcinek 70. został nagrany pięć lat po pierwszej wizycie dr Langer. Tym razem omawia ona to, czego dowiedziała się w międzyczasie, a także jak zmienił się świat i w jaki sposób wpłynęło to na nas: *www.social-engineer.org/podcast/ep-070-thinking-with-out-a-box/***

Który stan jest korzystniejszy dla osoby korzystającej z socjotechniki? Rzecz jasna stan alfa, ponieważ uwaga i czujność są w nim osłabione. Nie dotyczy to jednak wyłącznie działania w złej wierze, gdyż wszystkie formy manipulacji oraz niektóre rodzaje wpływu mają na celu nakłonienie nas do działania bez zastanowienia.

Weźmy za przykład popularny model reklamy. Na ekranie pojawia się znana piosenkarka, zaś w tle słychać wolny, smutny utwór. Następuje zmiana sceny. Teraz widzimy kociaki i szczeniaki, które są wyraźnie ranne, brudne i niedożywione, część z nich wygląda, jakby zostało im niewiele życia. Następnie wspomniana piosenkarka wraca, tym razem otoczona zdrowymi, pięknymi zwierzętami. Co taka reklama chce przekazać? Na ogół to, że wydając niewielką kwotę, możemy przekształcić te zaniedbane, chore zwierzęta w zdrowe i szczęśliwe. Obrazy w takiej reklamie zwykle przypominają zdjęcie, które można zobaczyć na ilustracji 1.1.

Czy producenci reklamy manipulują Tobą wyłącznie dla własnej korzyści? Niezupełnie. Ich działanie wynika z tego, że ludzie ci zdają sobie sprawę z tego, iż odwołanie się do Twoich emocji zwiększa prawdopodobieństwo uzyskania wpłaty na ustalony cel czy też podjęcia przez Ciebie innego pożądanego działania. Szansa ta jest przy tym wyższa, niż gdyby twórcy reklamy stosowali wyłącznie racjonalne argumenty. Gdy nasze emocje zostaną wzbudzone, zaczynamy myśleć mniej racjonalnie, a im mniej racjonalnie myślimy, tym szybciej podejmujemy decyzje w oparciu o same emocje.

Zdjęcie uzyskane za zgodą Amazon Community Animal Rescue, *www.flickr.com/photos/amazon-cares/2345707195*

Rysunek 1.1. Jak się czujesz, gdy widzisz coś takiego?

Wróćmy jednak do meritum. Jeżeli jesteś człowiekiem, niniejsza książka pomoże Ci poznać różne rodzaje takich ataków. Dowiesz się, jak źli ludzie wykorzystują Twoje człowieczeństwo przeciwko Tobie, a także poznasz metody obrony przed takimi atakami, aby skutecznie bronić siebie i bliskich.

Zacznijmy od ogólnego omówienia zjawiska, jakim jest socjotechnika.

Przedstawienie socjotechniki

Kiedy przedstawiam zagadnienia związane z socjotechniką, zwykle zaczynam od definicji, której z niewielkimi zmianami używam od dziesięciu lat.

Zanim jednak przejdę do definicji, muszę wyjaśnić jedną istotną rzecz. Socjotechnika, inaczej inżynieria społeczna (IS), nie jest politycznie poprawna. Może być to dla niektórych trudne dla zaakceptowania, ale taka jest prawda. Istnienie socjotechniki jest możliwe między innymi dlatego, że uprzedzenia związane z płcią, pochodzeniem, wiekiem i statusem społecznym (oraz ich połączenia) są faktem.

Przykładowo: wyobraź sobie, że chcesz przeniknąć do budynku klienta w USA. Aby to zrobić, musisz wymyślić stosowny pretekst. Zakładając, że do dyspozycji masz zespół złożony z kliku różnych osób i decydujesz się wprowadzić jedną z nich pod przykrywką sprzątacza, która z poniższych osób Twoim zdaniem będzie najbardziej wiarygodna w tej roli?

- 40-letni biały blondyn
- 33-letnia Azjatka
- 27-letnia Latynoska

A teraz przyjmijmy, że chcesz wprowadzić kogoś pod przykrywką pracownika kuchni. Kto będzie najlepiej pasować do takiej roli?

- 40-letni biały blondyn
- 33-letnia Azjatka
- 27-letnia Latynoska

Rzecz jasna doświadczony socjotechnik może poradzić sobie w każdej sytuacji niezależnie od tego, kim jest. Niektóre z wymienionych wyżej osób będą jednak w swojej roli budzić mniej podejrzeń, a co za tym idzie, będą w mniejszym stopniu prowokować innych do myślenia. Pamiętaj, że logiczne myślenie jest wrogiem każdego socjotechnika.

Mając to na uwadze, wróćmy do mojej definicji socjotechniki.

Socjotechnika, inaczej inżynieria społeczna (IS), to każde działanie wpływające na inną osobę w celu nakłonienia jej do podjęcia działania, które może być niezgodne z osobistym interesem tej osoby.

Dlaczego stosuję taką ogólną definicję? Głównie dlatego, że moim zdaniem, socjotechnika *nie zawsze* jest rzeczą szkodliwą.

Był taki czas, kiedy na stwierdzenie „Jestem hakerem" ludzie nie odłączali w panice wszystkich okolicznych urządzeń. Kiedyś bowiem termin „haker" oznaczał osobę *chcącą* wiedzieć, jak coś działa. Ktoś taki nie zadowalał się znajomością obsługi urządzenia, lecz chciał dokładnie poznać mechanizmy rządzące działaniem sprzętu, aby zrozumiawszy je, móc ominąć, rozbudować, wykorzystać bądź zmienić jego pierwotne zachowanie.

Kiedy zaczynałem pracę nad swoją pierwszą książką, chciałem przede wszystkim wyjaśnić, że socjotechnika nie jest wyłącznie dziedziną oszustów, naciągaczy i złodziei. Mechanizmy, których pozbawieni skrupułów ludzie używają do nieetycznych celów, mogą bowiem posłużyć do osiągnięcia celów jak najbardziej pożądanych.

Oto przykład. Jeżeli powiesz do mnie: „Słuchaj, Chris. Chciałbym się z Tobą pobawić w księżniczki. Usiądziemy przy stole, założysz różową szarfę, a ja będę malować ci paznokcie przy rozmowie o księżniczkach z filmów Disneya", to nie tylko zacznę się śmiać, ale najprawdopodobniej zacznę się też wycofywać w stronę

najbliższego wyjścia. Choć muszę przyznać, nie zdziwiłbym się, gdyby jacyś dorośli ludzie tak się właśnie bawili.

Kiedyś jednak moja córka poprosiła mnie, abym pobawił się z nią dokładnie w ten sposób. Zanim jednak powiesz: „To niesprawiedliwe porównanie — swoją córkę kochasz!", zaznaczam, że był to właśnie jeden z powodów, dla których się zgodziłem, ale nie o tym chcę teraz mówić. Moim celem jest bowiem przedstawienie psychologicznych mechanizmów stojących za podjęciem takiej decyzji. Aby zgodzić się na coś, co odrzuciłbym po nanosekundzie namysłu, gdyby poprosił mnie o to ktoś inny, musiałem bowiem przełamać moje standardowe schematy podejmowania decyzji.

CIEKAWOSTKA

Jedna nanosekunda to miliardowa część sekundy. Zakładając, że przeciętna osoba mówi z prędkością 145 słów na sekundę, nie byłaby w stanie powiedzieć: „Nie" w czasie jednej nanosekundy. Nawet światło poruszające się z gigantyczną prędkością 300 000 km/s byłoby w stanie przebyć w tym czasie około 30 cm.

Kiedy już zrozumiesz, jak podejmowane są decyzje, możesz zacząć orientować się, w jaki sposób nieetyczne osoby mogą wykorzystywać bodźce emocjonalne, mechanizmy psychologiczne oraz sztukę i naukę socjotechniki do tego, aby nakłonić cię do „podjęcia działania, które może być niezgodne z Twoim osobistym interesem".

Wystepujący w 44. odcinku *The Social-Engineer Podcast* dr Paul Zak jest autorem książki *The Moral Molecule* (Dutton 2012), w której przedstawił swoje badania nad hormonem zwanym oksytocyną. Ich wyniki rzuciły nowe światło na kwestię zaufania, gdyż zdaniem dr. Zaka oksytocyna jest uwalniana do naszego krwiobiegu w chwili, gdy wydaje nam się, że ktoś nam ufa. Zauważ, że odnosi się to do sytuacji, w której nie tylko komuś ufamy, ale także gdy *czujemy*, że ktoś obdarzył nas zaufaniem. Wspomniane badania wykazały, że zjawisko to występuje podczas spotkania w cztery oczy, rozmowy telefonicznej, kontaktu przez internet, a nawet kiedy nie widzimy osoby, która w teorii nam ufa.

SE-PODCAST

Odcinek 44. *The Social-Engineer Podcast* zawiera fascynującą rozmowę z dr. Paulem Zakiem o jego pracy zawodowej. Można go znaleźć pod adresem: *www.social-engineer.org/podcast/ep-044-do-you-trust-me/*

Kolejną substancją produkowaną przez nasz mózg jest neurotransmiter zwany dopaminą, która jest uwalniana w chwilach przyjemności, szczęścia i stymulacji. Połączenie oksytocyny z dopaminą daje niezwykle mocny koktajl, który pozwala zręcznemu człowiekowi na otwarcie każdych drzwi.

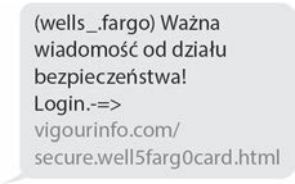
Dopamina i oksytocyna uwalniane są w sytuacjach mocno intymnych, ale mogą pojawiać się w krwiobiegu także podczas zwykłych konwersacji. Rozmowy takie stanowią podstawę socjotechniki.

Moim zdaniem pewne reguły kontaktów są przez nas stosowane (często nieświadomie) w rozmowach z naszymi małżonkami, szefami, współpracownikami, duchownymi, terapeutami, pracownikami i innymi ludźmi, których spotykamy na co dzień. Oznacza to, że zrozumienie inżynierii społecznej i zasad komunikacji z innymi ludźmi jest dla nas niezwykle istotną kwestią.

W świecie, w którym dzięki technologii możemy komunikować się za pomocą emotikon lub wiadomości liczących poniżej 280 znaków, umiejętność konwersacji staje się coraz rzadsza, co jedynie utrudnia nam obronę przed osobami, które taką zdolność posiadły. Co więcej, media społecznościowe stworzyły społeczeństwo, w którym mówienie wszystkiego o sobie losowo napotkanym osobom jest nie tylko akceptowane, ale wręcz promowane.

Kiedy mówię o inżynierii społecznej w jej szkodliwym wcieleniu, zwykle dzielę ją na cztery podstawowe typy:

- **SMiShing:** Tak, taka nazwa istnieje. Jest to skrót od SMS phishing, co oznacza korzystanie z metod phishingowych przy użyciu wiadomości tekstowych. Kiedy bank Wells Fargo padł ofiarą takiego ataku, otrzymałem SMS pokazany na Rysunku 1.2.



Rysunek 1.2. Ofiarą tego ataku SMiShingowego padło wiele osób

Zabawne jest to, otrzymałem tego SMS-a, chociaż nigdy nie korzystałem z usług tego banku. I nie, nie powiem, w jakim banku trzymam pieniądze. Nie ma tak łatwo!

Kliknięcie w załączony odnośnik powodowało wykradzenie danych logowania, wgranie szkodliwego oprogramowania (malware) na urządzenie mobilne bądź obie te rzeczy.

- **Vishing:** Jak wspomniałem wcześniej, słowo to oznacza phishing głosowy (ang. *voice phishing*) i metoda ta znacznie zyskała na popularności po roku 2016. Jest ona tania, prosta i niezwykle korzystna dla atakującego. Co więcej, wykorzystanie fikcyjnego numeru i połączenia międzynarodowego sprawia, że wykrycie i schwytanie osoby stosującej tę metodę jest prawie niemożliwe.

- **Phishing:** Jest to najpowszechniejsza metoda ataku znana w środowisku znawców socjotechniki. Kilka lat temu wraz z redaktorką niniejszej pozycji, Michele, napisałem książkę *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* (Wiley, 2016). Wiem, nie wypada się chwalić, ale nie mogłem sobie odmówić odrobiny autoprezentacji. Z doświadczenia wiemy, że phishing pozwala na zatrzymywanie pracy fabryk, hakowanie komisji wyborczych, włamanie się do Białego Domu i dziesiątek wielkich korporacji oraz wykradanie milionów dolarów. Jak dotychczas phishing jest najgroźniejszą z czterech głównych metod IS.

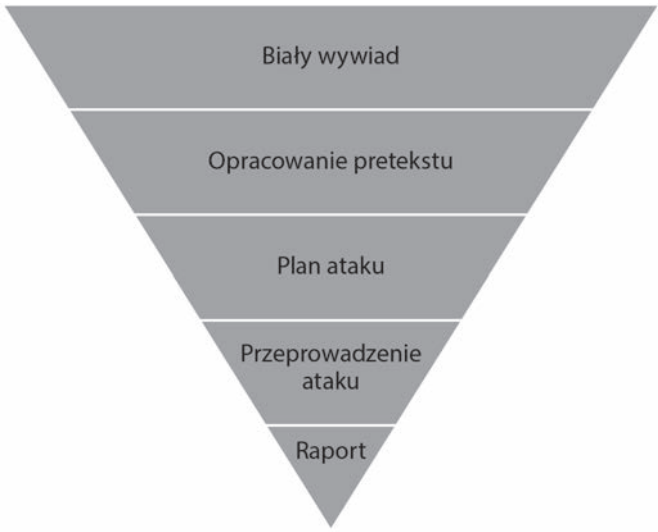
- **Podszywanie się:** Chociaż kusiło mnie, aby wymyślić jakiś techniczny termin podobny do trzech poprzednich, zrezygnowałem z tego zamiaru, gdyż ta metoda jednak różni się od innych, co w żadnym razie nie oznacza, że jest mniej groźna. W ciągu ostatnich 12 miesięcy zebraliśmy ogromną ilość zgłoszeń opisujących przypadki nierzadko strasznych zbrodni popełnionych przez ludzi podszywających się pod policjantów, agentów federalnych bądź pracowników firm. W kwietniu 2017 usłyszałem o człowieku, który wykorzystywał przebranie policjanta, aby handlować dziecięcą pornografią. Na szczęście został schwytany.

  Każdy atak IS można zaliczyć do jednej z powyższych kategorii, chociaż ostatnio coraz częściej pojawiają się osoby łączące kilka metod podczas dokonywania ataku.

  Analiza takich przypadków pozwoliła mi dostrzec pewne prawidłowości, które nie tylko pozwalają ustalić, jakie narzędzia i procesy zostały użyte do osiągnięcia celu, ale także umożliwiają zrozumienie mechanizmu ataków i wykorzystanie tej wiedzy do edukowania innych, aby mogli się skutecznie bronić. Wspomniane prawidłowości nazwałem *Piramidą IS*.

Piramida IS

Zanim przejdę do szczegółowego opisu piramidy i jej poszczególnych sekcji, pozwól, że dokonam jej ogólnego omówienia. Schemat piramidy znajdziesz na rysunku 1.3.



Rysunek 1.3. Piramida socjotechniki

Jak widać, piramida została podzielona na kilka elementów i stanowi ilustrację inżynierii społecznej z perspektywy specjalisty od IS, czyli człowieka, który korzysta ze swoich umiejętności nie po to, by krzywdzić innych, ale aby pomagać swoim klientom.

Poniżej opiszę poszczególne sekcje piramidy, zaś ich warstwy przedstawię w dalszych rozdziałach.

Biały wywiad

Biały wywiad nazywany równie OSINT (*Open Source Intelligence*) stanowi podstawę każdej kwestii związanej z socjotechniką i między innymi dlatego jest elementem najlepiej zbadanym. Z tego też powodu stanowi pierwszą i największą część piramidy. W tym miejscu chciałbym zwrócić uwagę na jeden z elementów takiego wywiadu, który bywa dość rzadko wspominany, a mianowicie dokumentację. W jaki sposób można dokumentować, zapisywać i katalogować wszystkie uzyskane informacje? Szczegółowo opowiem o tym w następnym rozdziale.

Opracowanie pretekstu

Uzyskawszy informacje poprzez OSINT, można przystąpić do wymyślenia odpowiedniego pretekstu. W oparciu o dostępne dane należy ustalić optymalne podejście, a także wybrać ewentualne narzędzia i rekwizyty, które mogą być przydatne w realizacji planu.

Plan ataku

Sam pretekst to za mało. Aby plan zadziałał, konieczne jest udzielenie odpowiedzi na trzy pytania: „co?", „kiedy?" i „kto?".

- Co jest celem? Co chcesz osiągnąć? Co chce uzyskać klient? Odpowiedź na te pytania ułatwia odpowiedź na kolejne.
- Kiedy będzie najlepiej dokonać ataku?
- Kto musi być dostępny w czasie ataku, aby posłużyć jako wsparcie, gdy zajdzie taka potrzeba?

Przeprowadzenie ataku

Teraz najciekawsze, czyli atak właściwy. Mając gotowy plan, możesz przystąpić do działania. Ważne jest, aby plan nie był zbyt sztywny i szczegółowy, gdyż utrudnia to dynamiczne wprowadzanie niezbędnych zmian. Sam jestem zwolennikiem zapisywania planu, gdyż znacząco ułatwia to jego wykonanie. Pamiętaj tylko, aby nie zapisywać każdego słowa i działania, gdyż może być to przyczyną kłopotów, jeśli natkniesz się na niespodziewane przeszkody. Kiedy wykonujesz wyłącznie poszczególne punkty scenariusza, konieczność zrobienia czegoś, czego w nim nie ma, sprawia, że mózg traci punkt odniesienia. W takiej sytuacji możesz zacząć się denerwować, tracić wątek, jąkać się i przejawiać inne oznaki lęku, co może zaprzepaścić cały misterny plan. Dlatego też zawsze proponuję zapisywanie wyłącznie ogólnego schematu działań, aby pozostawić nieco miejsca na improwizację.

Raport

Nie pomijaj tego punktu! Wiem, że raportowanie czegokolwiek nie jest przyjemne, ale musisz pamiętać, iż klient zapłacił Ci za wykonanie usługi i najprawdopodobniej udało Ci się odnieść sukces. Klient zapłacił Ci jednak nie tylko dlatego, że chce dobrze wypaść w oczach innych, ale również dlatego, że chce wiedzieć, jak może uchronić się przed podobnymi problemami w przyszłości. Raportowanie umieściłem zatem na samym czubku piramidy, gdyż stanowi ono ukoronowanie całego procesu.

Sprawne wykorzystanie opisanych pięciu poziomów piramidy zapewni Ci sukces w roli nie tylko socjotechnika, ale także specjalisty oferującego usługi inżynierii społecznej. Warto też pamiętać, że osoby wykorzystujące opisywane umiejętności do nieetycznych i nielegalnych celów także korzystają z piramidy, na ogół pomijając etap raportowania.

W roku 2015 serwis Dark Reading zgłosił atak, który dokładnie wpisuje się w schemat ilustrowany piramidą socjotechniki (artykuł *CareerBuilder Attack Sends Malware-Rigged Resumes to Businesses* można przeczytać pod adresem *www.darkreading.com/vulnerabilities---threats/careerbuilderattack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236?*).

1. Atakujący przeprowadzili wstępne rozpoznanie, atakując kilka celów i podczas fazy wywiadu zorientowali się, że ich cele korzystają z popularnego serwisu CareerBuilder.
2. Po zakończeniu fazy wywiadu atakujący zaczęli opracowywać pretekst. Stworzyli w tym celu na wspomnianym serwisie profil użytkownika szukającego dowolnej pracy oferowanej przez wybrane cele. Narzędziem ataku miały być odpowiednio zakodowane pliki oraz realistycznie wyglądające CV.
3. Planując atak, sprawcy uzyskali odpowiedzi na trzy kluczowe pytania.
4. Następnie przeprowadzili oni atak, umieszczając swoje pliki *nie* na serwerach celu, lecz w serwisie CareerBuilder, który automatycznie powiadamiał pracodawców o nowych aplikacjach na zgłoszone wakaty i właśnie te automatyczne e-maile miały zawierać spreparowane pliki.
5. Atakujący nie opisali nikomu swoich działań, ale analiza ataku dokonana przez badaczy z firmy Proofpoint może posłużyć nam za swego rodzaju raport.

Opisany wyżej atak okazał się skuteczny, ponieważ cele otrzymały e-maile z zaufanego źródła, jakim jest serwis CareerBuilder, przez co pracujący tam ludzie otworzyli je bez większego zastanowienia. A jak już wiesz z lektury niniejszego rozdziału, sprawienie, by ludzie podejmowali działania, które *nie* są w ich interesie, nie zastanawiając się przy tym nad potencjalnymi skutkami takiego zachowania, jest celem każdego socjotechnika.

Co zawiera ta książka?

Planując niniejszą książkę, starałem się zachować ogólny schemat wykorzystany w pierwszym wydaniu książki *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, aby ułatwić lekturę czytelnikom, którzy mieli okazję ją przeczytać. Z drugiej strony chciałem też zmienić i rozwinąć przedstawione wcześniej informacje, aby przedstawić nowe rodzaje ataków i kwestie, których nie poruszałem w pierwszym wydaniu książki.

Chcąc sprawić, by niniejsza pozycja była lepsza od poprzedniej, korzystałem z niezliczonych rad fanów, czytelników, badaczy i recenzentów. Pozwól zatem, że zacznę od przedstawienia treści kolejnych rozdziałów.

Rozdział 2. „Czy widzisz to, co ja?" omawia szerzej zagadnienia białego wywiadu i niektóre z najpowszechniejszych technik wykorzystywanych do uzyskiwania informacji. Nie poświęciłem przy tym zbyt wiele uwagi samym narzędziom, chociaż przybliżyłem kilka najczęściej wykorzystywanych przeze mnie metod.

W rozdziale 3. „Profilowanie przez komunikację" — omawiam kwestię, której prawie nie poruszyłem w pierwszym wydaniu, a mianowicie dokładne przedstawienie modelowania w komunikacji oraz narzędzi do profilowania.

W rozdziale 4. „Bądź, kim tylko chcesz być" — zaczynam poruszać kwestię pretekstu. Jest to temat, który rzadko pojawia się poza środowiskiem socjotechników. W samym rozdziale znajdziesz wiele porad, uwag i historii z mojego życia (opisujących zarówno zwycięstwa, jak i porażki).

Rozdział 5. „Wiem, jak sprawić, byście mnie lubili" — zamieściłem informacje, które znalazłem w różnych podcastach i biuletynach lub usłyszałem od wielu znanych ludzi i które odnoszą się do kwestii budowania relacji w inżynierii społecznej. Jedną z osób, której słowa przytaczam w tym rozdziale, jest Robin Dreeke, szef Zespołu Analiz Behawioralnych w FBI, z którym miałem okazję się zaprzyjaźnić.

Rozdział 6. „Pod wpływem" odnosi się do prac jednego z głównych badaczy kwestii wpływu psychologicznego, Roberta Cialdiniego, i wyjaśnia, w jaki sposób zasady takiego wpływu mogą być wykorzystane przez socjotechników.

Rozdział 7. „Tworzenie dzieła sztuki" opisuje zjawiska ramowania i wzbudzania, a także wykorzystywania ich do własnych celów.

W rozdziale 8. „Widzę, czego mi nie mówisz" — wracam do jednego z moich ulubionych tematów, a mianowicie zachowań niewerbalnych. Bardzo szczegółowo opisuję to zagadnienie w swojej książce *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014), ale ten rozdział może posłużyć jako solidne wprowadzenie w świat sygnałów niewerbalnych.

W rozdziale 9. „Hakowanie ludzi" — wykorzystuję informacje przedstawione w poprzednich ośmiu rozdziałach, odnosząc je do pięciu różnych rodzajów ataków socjotechnicznych i podkreślając, jak ważne dla każdego specjalisty w zakresie inżynierii społecznej są zjawiska i mechanizmy przedstawione w niniejszej książce.

Znajdujący się przy końcu rozdział 10. „Czy wiesz, co to M.A.P.A.?" obejmuje kwestie zapobiegania i zmniejszania szkód. Jako że moim celem jest wspieranie osób chcących wykorzystywać inżynierię społeczną w dobrych celach, opisałem tam cztery etapy działań pomagających w odpieraniu ataków.

Jak wszystko, co dobre, także i ta książka kiedyś się kończy. Rozdział 11. „Co teraz?" stanowi podsumowanie wszystkich zawartych w niej treści.

Oto kilka obietnic z mojej strony:

- Obiecuję, że nie będę powoływał się na Wikipedię, zwłaszcza przytaczając wyniki badań (wystarczy, że już wcześniej popełniłem ten błąd).
- Obiecuję, że przedstawię rozmaite historie z ostatnich siedmiu lat mojej pracy. Czasami opiszę jedno wydarzenie z kilku możliwych perspektyw, aby ułatwić jego zrozumienie. Postaram się jednak, aby historie te były urozmaicone.
- Powołując się na najlepszych specjalistów w danej dziedzinie, będę przytaczał stosowne źródła, ułatwiając Ci tym samym zapoznanie się z nimi bezpośrednio.
- Jak w przypadku mojej pierwszej książki zachęcam Cię do dzielenia się uwagami, wnioskami, sugestiami i krytyką.

W zamian proszę o potraktowanie tej książki zgodnie z celem, dla którego została napisana. Jeżeli omawiana tematyka jest dla Ciebie czymś nowym, niniejsza pozycja pomoże Ci nauczyć się wszystkich umiejętności niezbędnych zawodowemu socjotechnikowi. Jeżeli masz już doświadczenie w tej dziedzinie, mam nadzieję, że zawarte tu informacje, porady i opowieści rozszerzą Twój repertuar metod i narzędzi. Jeśli po prostu interesujesz się taką tematyką, to mam nadzieję, że lektura tej książki będzie dla Ciebie co najmniej tak pasjonująca, jak dla mnie było jej pisanie. A jeśli jesteś sceptykiem, to podczas lektury staraj się pamiętać, że w żadnym razie nie uważam się za guru IS i nie głoszę „jedynego słusznego podejścia". Jestem wyłącznie miłośnikiem socjotechniki z wieloletnią praktyką, który chce podzielić się swoją wiedzą i uczynić świat choć trochę bezpieczniejszym.

Podsumowanie

Żadna z napisanych przeze mnie książek nie może obejść się bez analogii kucharskich, więc nie inaczej będzie i tym razem. Wspaniały posiłek wymaga długiego planowania, dobrego przepisu, świeżych składników oraz podejścia łączącego kulinarną sztukę i naukę. Socjotechnika, chociaż w gruncie rzeczy prosta, wymaga pewnej wiedzy na temat tego, jak ludzie podejmują decyzje, co ich motywuje i w jaki sposób kontrolować własne uczucia, wykorzystując przy tym emocje innych ludzi.

Treść niniejszej książki jest tak samo aktualna, jak osiem lat temu, jeżeli nie bardziej. Przez ten czas widziałem, jak ludzie rozpoczynają karierę zawodowych inżynierów społecznych, ale miałem też okazję obserwować wzloty i upadki ludzi, którzy swoje umiejętności wykorzystywali, aby szkodzić innym.

Jako że opisywane tu formy ataku wykorzystują czynnik ludzki, każdy, kto chce zajmować się zawodowo inżynierią społeczną, musi dobrze poznać przedstawione tu zasady, mimo że w żadnym razie nie wyczerpują one tematu. Kiedy zaczynałem pracę w charakterze kucharza (dawno i nieprawda), mój mentor poprosił, abym spróbował każdego składnika, którego miałem użyć.

Ćwiczenie to miało mi uzmysłowić, że nie będę w stanie „smakować" potrawy, jeśli nie będę znać smaku każdego z jej składników. Jeśli wiem, jak smakuje chrzan, to będę wiedzieć, ile muszę go dodać, aby potrawa była ostrzejsza. Świadomość tego, że któryś ze składników jest słony, pozwoli mi odpowiednio dobrać ilość dodawanej soli, aby cała potrawa miała właściwy smak. I tak dalej…

Nawet jeżeli nie pracujesz w branży bezpieczeństwa, musisz wiedzieć, jak każda z opisywanych tu metod „smakuje", aby skutecznie wykorzystać ją do obrony przed atakami. Co oznacza „budowanie relacji" i jak może zostać to wykorzystanie do przywłaszczania cudzych pieniędzy? Piszę o tym w rozdziale 5. W jaki sposób wpływ wzbogacony szczyptą konwersacji wzbudzającej może skłonić kogoś do ujawnienia hasła do telefonu? Tego dowiesz się z lektury rozdziałów 6. i 7.

Każdy z powyższych „składników" pomaga nauczyć się „smakowania". Kiedy dobrze znasz mechanizmy socjotechniki, dużo łatwiej będzie Ci się zorientować, kiedy ktoś zdecyduje się wykorzystać je przeciwko Tobie. A jeśli wiesz, że coś jest nie tak, znacznie łatwiej będzie Ci podjąć działania zapobiegawcze.

Czy zdarzyło Ci się kiedyś oglądać programy kulinarne z udziałem Gordona Ramsaya? Kiedy próbuje on czegoś, co mu nie smakuje, zawsze określa on przyczynę problemu, mówiąc np.: „Tutaj dodano za dużo pieprzu i użyto za dużo oliwy przy smażeniu". Początkujący kucharz mógłby ograniczyć się w takiej sytuacji do stwierdzenia: „To jest za ostre i za tłuste". Niby to samo, ale jednak pierwsza ocena jest lepsza. Mam nadzieję, że lektura niniejszej książki pomoże Ci stać się Gordonem Ramsayem socjotechniki. No, może poza jego kwiecistym, acz nie zawsze cenzuralnym językiem.

Wyjaśniwszy to sobie, możemy przejść do konkretów. Kolejny rozdział wprowadzi Cię w tematykę białego wywiadu.

Socjotechnika: najważniejsze narzędzie hakerów, polityków i… aktywistów!

Socjotechnika określa sposoby wpływania na drugiego człowieka w celu nakłonienia go do działania, które może być niezgodne z jego osobistym interesem. Koszt użycia socjotechnik jest bardzo niski, ryzyko — akceptowalne, a korzyści bywają ogromne. Uważa się, że socjotechniki są nieodzownym narzędziem hakerów, przestępców czy służb specjalnych. Oczywiście nie zawsze intencje towarzyszące stosowaniu inżynierii społecznej zasługują na potępienie: tego rodzaju działanie przy kampaniach edukacyjnych, akcjach charytatywnych czy w marketingu trudno jednoznacznie nazywać nieetycznym. Niemniej wiedza o socjotechnikach jest obecnie bardzo ważna i potrzebna, choćby po to, aby skutecznie bronić się przed atakami tego typu.

To drugie, przejrzane i gruntownie zaktualizowane wydanie znakomitego przewodnika po różnych technikach inżynierii społecznej, od klasycznych po najnowocześniejsze. Przedstawiono tu naukowe podwaliny socjotechnik, a poszczególne metody, takie jak tworzenie pretekstu, modelowanie komunikacji, tailgating czy phishing, opisano z przywołaniem rzeczywistych zdarzeń. Książka pozwala zrozumieć, jak łatwo jest skłonić ludzi do podjęcia szkodliwych decyzji, a równocześnie podpowiada, jak można skutecznie bronić się przed socjotechnikami. Są one coraz powszechniejsze: w ciągu ostatnich kilku lat ich zastosowanie bardzo się rozpowszechniło — i dotyczy to zarówno przestępców, jak i najzupełniej legalnie działających profesjonalistów.

W tej książce między innymi:

- najnowsze osiągnięcia zawodowej socjotechniki
- stosowanie białego wywiadu, manipulacja relacjami, praca na emocjach
- testy penetracyjne, phishing, vishing, podszywanie się
- budowanie systemu obrony przed atakami socjotechnicznymi
- wykorzystanie umiejętności miękkich w inżynierii społecznej

Christopher Hadnagy — prezes firmy Social Engineer LLC. Brał udział w tworzeniu pierwszego serwisu poświęconego inżynierii społecznej (*www.social-engineer.org*). Jest cenionym mówcą i trenerem, często występuje na różnego rodzaju konferencjach, takich jak RSA, Black Hat i DEF CON. Na specjalne zaproszenie przedstawił kluczowym pracownikom Pentagonu zasady inżynierii społecznej i jej wpływ na Stany Zjednoczone.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-9576-3
9 788328 395763
Cena: 59,00 zł
INFORMATYKA W NAJLEPSZYM WYDANIU
onepress
WILEY