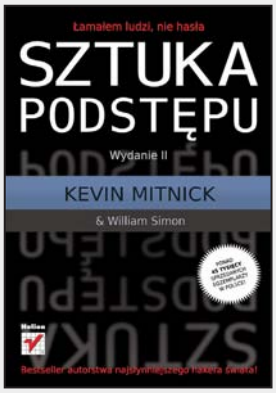
Sztuka podstepu. Łamałem ludzi nie hasła. Wydanie II



Autorzy: Kevin Mitnick, William L. Simon, Steve Wozniak
Tłumaczenie: Jarosław Dobrzański
ISBN: 978-83-246-2795-0
Tytuł oryginału: The Art of Deception: Controlling the Human Element of Security
Format: A5, stron: 400

Łącząc techniczną biegłość ze starą jak świat sztuką oszustwa, Kevin Mitnick staje się programistą nieobliczalnym.

„New York Times", 7 kwietnia 1994

Już jako nastolatek swoimi umiejętnościami zastraszył całą Amerykę. Z czasem stał się najsłynniejszym hakerem świata i wrogiem publicznym numer jeden – okrzyknięty przez media groźnym cyberprzestępcą, gorliwie ścigany przez FBI, w końcu podstępem namierzony, osaczony i spektakularnie ujęty... Uzbrojony w klawiaturę został uznany za groźnego dla społeczeństwa – wyrokiem sądu na wiele lat pozbawiono go dostępu do komputera, internetu i telefonów komórkowych. Życiorys Kevina Mitnicka jest jak scenariusz dobrego filmu sensacyjnego! Nic zatem dziwnego, że doczekał się swojej hollywoodzkiej wersji. Genialny informatyk czy mistrz manipulacji? Jak naprawdę działał człowiek, wokół wyczynów i metod którego narosło tak wiele legend? Jakim sposobem udało mu się włamać do systemów takich firm, jak Nokia, Fujitsu, Novell czy Sun Microsystems?!

Zakup najdroższych technologii zabezpieczeń, karty biometryczne, intensywne szkolenia personelu, restrykcyjna polityka informacyjna czy wreszcie wynajęcie agencji ochrony – Kevin Mitnick udowodnił, że w świecie sieci i systemów poczucie bezpieczeństwa jest tylko iluzją. Ludzka naiwność, łatwowierność i ignorancja – oto najsłabsze ogniwa, wiodące do uzyskania poufnych informacji, tajnych kodów i haseł. Mitnick, obecnie najbardziej rozchwytywany ekspert w dziedzinie bezpieczeństwa komputerów, w swej niezwykłej książce przestrzega i pokazuje, jak łatwo można ominąć bariery systemów wartych miliony dolarów. Przedstawiając i analizując metody hakerów oparte na prawdziwych atakach, demonstruje, że tam, gdzie nie można znaleźć luk technicznych, zawsze skuteczne okazują się ludzkie słabości... A Ty? Jesteś w pełni świadomy narzędzi technologicznych i socjotechnicznych, które hakerzy mogą wykorzystać przeciwko Tobie?

Przekonaj się, że „ściśle tajne" to fikcja.
A bezpieczeństwo systemu to tylko Twoje złudzenie...

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Łamałem ludzi, nie hasła

SZTUKA PODSTĘPU

Wydanie II

KEVIN MITNICK

& William Simon

PONAD **45 TYSIĘCY** SPRZEDANYCH EGZEMPLARZY W POLSCE!

Helion

Bestseller autorstwa najsłynniejszego hakera świata!

Spis treści

2

Kiedy nieszkodliwa informacja szkodzi?

Na czym polega realne zagrożenie ze strony socjotechnika? Czego powinniśmy się strzec?

Jeżeli jego celem jest zdobycie czegoś wartościowego, powiedzmy części kapitału firmy, to być może potrzebny jest solidniejszy skarbiec i większe straże, czyż nie?

Penetracja systemu bezpieczeństwa firmy często zaczyna się od zdobycia informacji lub dokumentu, który wydaje się nie mieć znaczenia, jest powszechnie dostępny i niezbyt ważny. Większość ludzi wewnątrz organizacji nie widzi więc powodów, dla których miałby być chroniony lub zastrzeżony.

Ukryta wartość informacji

Wiele nieszkodliwie wyglądających informacji będących w posiadaniu firmy jest cennych dla socjotechnika, ponieważ mogą one odegrać podstawową rolę podczas wcielania się w kogoś innego.

Ze stron tej książki dowiemy się, jak działają socjotechnicy, stając się „świadkami" ich ataków. Czasami przedstawienie sytuacji, w pierwszej kolejności z punktu widzenia ofiary, umożliwia wcielenie się w jej rolę i próbę analizy, jak my, lub nasi pracownicy, zachowalibyśmy się w takiej sytuacji. W wielu przypadkach te same wydarzenia zostaną przedstawione również z punktu widzenia socjotechnika.

Pierwsza historia uświadamia nam słabe strony firm działających w branży finansowej.

CreditChex

Jak daleko sięgnąć pamięcią, Brytyjczycy musieli zmagać się ze staroświeckim systemem bankowym. Zwykły, uczciwy obywatel nie może po prostu wejść tam do banku i założyć konta. Bank nie będzie traktować go jako klienta, dopóki osoba już będąca klientem nie napisze mu listu referencyjnego.

W naszym, z pozoru egalitarnym świecie bankowości, wygląda to już trochę inaczej. Nowoczesny, łatwy sposób robienia interesów jest najbardziej widoczny w przyjaznej i demokratycznej Ameryce, gdzie każdy może wejść do banku i bez problemu otworzyć rachunek. Chociaż nie do końca. W rzeczywistości banki mają naturalne opory przed otwieraniem rachunku komuś, kto mógł w przeszłości wystawiać czeki bez pokrycia. Klient taki jest tak samo mile widziany jak raport strat z napadu na bank czy defraudacja środków. Dlatego standardową praktyką w wielu bankach jest szybkie sprawdzanie wiarygodności nowego klienta.

Jedną z większych firm, które banki wynajmują do takich kontroli, jest CreditChex. Świadczy ona cenne usługi dla swoich klientów, ale jej pracownicy mogą też nieświadomie pomóc socjotechnikowi.

Pierwsza rozmowa: Kim Andrews

— National Bank, tu mówi Kim. Czy chce pan otworzyć rachunek?

— Dzień dobry, mam pytanie do pani. Czy korzystacie z CreditChex?

— Tak.

— A jak się nazywa ten numer, który trzeba podać, jak się dzwoni do CreditChex? Numer kupca?

Pauza. Kim rozważa pytanie. Czego dotyczyło i czy powinna odpowiedzieć? Rozmówca zaczyna mówić dalej bez chwili zastanowienia:

— Wie pani, pracuję nad książką o prywatnych śledztwach.

— Tak — mówi Kim, odpowiadając na pytanie po zniknięciu wątpliwości, zadowolona, że mogła pomóc pisarzowi.

— A więc to się nazywa numer kupca, tak?

— Mhm.

— Świetnie. Chciałem się po prostu upewnić, czy znam żargon. Na potrzeby książki. Dziękuję za pomoc. Do widzenia.

Druga rozmowa: Chris Walker

— National Bank, nowe rachunki, mówi Chris.

— Dzień dobry, tu Alex — przedstawia się rozmówca. — Jestem z obsługi klientów CreditChex. Przeprowadzamy ankietę, aby polepszyć jakość naszych usług. Czy może pani poświęcić mi parę minut?

Chris zgodziła się. Rozmówca kontynuował:

— Dobrze, a więc jakie są godziny otwarcia waszej filii? — Chris odpowiada na to pytanie i na szereg następnych.

— Ilu pracowników waszej filii korzysta z naszych usług?

— Jak często dzwonicie do nas z zapytaniem?

— Który z numerów 0-800 został wam podany do kontaktów z nami?

— Czy nasi przedstawiciele zawsze byli uprzejmi?

— Jaki jest nasz czas odpowiedzi?

— Jak długo pracuje pani w banku?

— Jakim numerem kupca pani się posługuje?

— Czy kiedykolwiek nasze informacje okazały się niedokładne?

— Co zasugerowałaby nam pani w celu poprawienia jakości naszych usług?

— Czy będzie pani skłonna wypełniać periodycznie kwestionariusze, które prześlemy do filii?

Chris ponownie się zgodziła. Przez chwilę rozmawiali niezobowiązująco. Po zakończeniu rozmowy Chris wróciła do swoich zajęć.

Trzecia rozmowa: Henry Mc Kinsey

— CreditChex, mówi Henry Mc Kinsey. W czym mogę pomóc?

Rozmówca powiedział, że dzwoni z National Bank. Podał prawidłowy numer kupca, a następnie nazwisko i numer ubezpieczenia osoby, o której szukał informacji. Henry zapytał o datę urodzenia. Rozmówca podał ją.

— Wells Fargo, wystąpiło NSF w 1998 na sumę 2066 $ — po paru chwilach Henry odczytuje dane z ekranu komputera (NSF oznacza niewystarczające środki. W żargonie bankowym dotyczy to czeków, które zostały wystawione bez pokrycia).

— Były jakieś zdarzenia od tamtego czasu?

— Nie było.

— Były jakieś inne zapytania?

— Sprawdźmy. Tak — trzy i wszystkie w ostatnim miesiącu. Bank of Chicago...

Przy wymawianiu kolejnej nazwy — Schenectady Mutual Investments — zająknął się i musiał ją przeliterować.

— W stanie Nowy Jork — dodał.

Prywatny detektyw na służbie

Wszystkie trzy rozmowy przeprowadziła ta sama osoba: prywatny detektyw, którego nazwiemy Oscar Grace. Grace zdobył nowego klienta. Jednego z pierwszych. Jako były policjant zauważył, że część jego nowej pracy przychodzi mu naturalnie, a część stanowi wyzwanie dla jego wiedzy i inwencji. Tę robotę mógł zakwalifikować jednoznacznie do kategorii wyzwań.

Twardzi detektywi z powieści, tacy jak Sam Spade i Philip Marlowe, przesiadywali długie nocne godziny w swoich samochodach, czyhając na okazję, by przyłapać niewiernego małżonka. Prawdziwi detektywi robią to samo. Poza tym zajmują się rzadziej opisywanymi, ale nie mniej istotnymi formami węszenia na rzecz wojujących małżonków. Opierają się one w większym stopniu na socjotechnice niż walce z sennością w czasie nocnego czuwania.

Nową klientką Grace'a była kobieta, której wygląd wskazywał, że nie ma problemów z budżetem na ubrania i biżuterię. Któregoś dnia weszła do biura i usiadła na jedynym skórzanym fotelu wolnym od stert papierów. Położyła swoją dużą torebkę od Gucciego na jego biurku, kierując logo w stronę Grace'a, i oznajmiła, iż zamierza powiedzieć mężowi, że chce rozwodu, przyznając jednocześnie, że ma „pewien mały problem".

Wyglądało na to, że mężulek był o krok do przodu. Zdążył pobrać pieniądze z ich rachunku oszczędnościowego i jeszcze większą sumę z rachunku brokerskiego. Interesowało ją, gdzie mogły znajdować się te pieniądze, a jej adwokat nie bardzo chciał w tym pomóc. Grace przypuszczał, że był to jeden z tych wysoko postawionych gości, którzy nie chcą brudzić sobie rąk mętnymi sprawami pod tytułem „Gdzie podziały się pieniądze?".

Zapytała Grace'a, czy jej pomoże.

Zapewnił ją, że to będzie pestka, podał swoją stawkę, określił, że to ona pokryje dodatkowe wydatki, i odebrał czek z pierwszą ratą wynagrodzenia.

Potem uświadomił sobie problem. Co zrobić, kiedy nigdy nie zajmowało się taką robotą i nie ma się pojęcia o tym, jak wyśledzić drogę przebytą przez pieniądze? Trzeba raczkować. Oto znana mi wersja historii Grace'a.

* * *

Wiedziałem o istnieniu CreditChex i o tym, jak banki korzystały z jego usług. Moja była żona pracowała kiedyś w banku. Nie znałem jednak żargonu i procedur, a próba pytania o to mojej byłej byłaby stratą czasu.

Krok pierwszy: ustalić terminologię i zorientować się, jak sformułować pytanie, by brzmiało wiarygodnie. W banku, do którego zadzwoniłem, pierwsza moja rozmówczyni, Kim, była podejrzliwa, kiedy zapytałem, jak identyfikują się, dzwoniąc do CreditChex. Zawahała się. Nie wiedziała, co powiedzieć. Czy zbiło mnie to z tropu? Ani trochę. Tak naprawdę, jej wahanie było dla mnie wskazówką, że muszę umotywować swoją prośbę, aby brzmiała dla niej wiarygodnie. Opowiadając historyjkę o badaniach na potrzeby książki, pozbawiłem Kim podejrzeń. Wystarczy powiedzieć, że jest się pisarzem lub gwiazdą filmową, a wszyscy stają się bardziej otwarci.

Kim miała jeszcze więcej pomocnej mi wiedzy — na przykład, o jakie informacje pyta CreditChex w celu identyfikacji osoby, w sprawie której dzwonimy, o co można ich pytać i najważniejsza rzecz: numer klienta. Byłem gotów zadać te pytania, ale jej wahanie było dla mnie ostrzeżeniem. Kupiła historię o pisarzu, ale przez chwilę trapiły ją podejrzenia. Gdyby odpowiedziała od razu, poprosiłbym ją o wyjawienie dalszych szczegółów dotyczących procedur.

Trzeba kierować się instynktem, uważnie słuchać, co mówią i jak mówią. Ta dziewczyna wydawała się na tyle bystra, że mogła wszcząć alarm, gdybym zaczął zadawać zbyt wiele dziwnych pytań. Co prawda nie wiedziała, kim jestem i skąd dzwonię, ale samo rozejście się wieści, żeby uważać na dzwoniących i wypytujących o informacje nie byłoby wskazane. Lepiej nie *spalić źródła* — być może będziemy chcieli zadzwonić tu jeszcze raz.

Zawsze zwracam uwagę na drobiazgi, z których mogę wywnioskować, na ile dana osoba jest skłonna do współpracy — oceniam to w skali, która zaczyna się od: „Wydajesz się miłą osobą i wierzę we wszystko, co mówisz", a kończy na: „Dzwońcie na policję, ten facet coś knuje!".

Żargon ➤

Spalenie źródła — mówi się o napastniku, że spalił źródło, kiedy dopuści do tego, że ofiara zorientuje się, iż została zaatakowana. Wówczas najprawdopodobniej powiadomi ona innych pracowników i kierownictwo o tym, że miał miejsce atak. W tej sytuacji kolejny atak na to samo źródło staje się niezwykle trudny.

Kim była gdzieś w środku skali, dlatego zadzwoniłem jeszcze do innej filii. W czasie mojej drugiej rozmowy z Chris trik z ankietą udał się doskonale. Taktyka polegała tu na przemyceniu ważnych pytań wśród innych, błahych, które nadają całości wiarygodne wrażenie. Zanim zadałem pytanie o numer klienta CreditChex, przeprowadziłem ostatni test, zadając osobiste pytanie o to, jak długo pracuje w banku.

Osobiste pytanie jest jak mina — niektórzy ludzie przechodzą obok niej i nawet jej nie zauważają, a przy innych wybucha, wysyłając sygnał ostrzegawczy. Jeżeli więc zadam pytanie osobiste, a ona na nie odpowie i ton jej głosu się nie zmieni, oznacza to, że prawdopodobnie nie zdziwiła jej natura pytania. Mogę teraz zadać następne pytanie bez wzbudzania podejrzeń i raczej otrzymam odpowiedź, jakiej oczekuję.

Jeszcze jedno. Dobry detektyw nigdy nie kończy rozmowy zaraz po uzyskaniu kluczowej informacji. Dwa, trzy dodatkowe pytania, trochę niezobowiązującej pogawędki i można się pożegnać. Jeżeli rozmówca zapamięta coś z rozmowy, najprawdopodobniej będą to ostatnie pytania. Reszta pozostanie zwykle w pamięci zamglona.

Tak więc Chris podała mi swój numer klienta i numer telefonu, którego używają do zapytań. Byłbym szczęśliwszy, gdyby udało mi się jeszcze zadać parę pytań dotyczących tego, jakie informacje można wyciągnąć od CreditChex. Lepiej jednak nie nadużywać dobrej passy.

To było tak, jakby CreditCheck wystawił mi czek in blanco — mogłem teraz dzwonić i otrzymywać informacje, kiedy tylko chciałem. Nie musiałem nawet płacić za usługę. Jak się okazało, pracownik CreditChex z przyjemnością udzielił mi dokładnie tych informacji, których potrzebowałem: podał dwa miejsca, w których mąż mojej klientki ubiegał się o otwarcie rachunku. Gdzie w takim razie znajdowały się pieniądze, których szukała jego „już wkrótce była żona"? Gdzieżby indziej, jak nie w ujawnionych przez CreditChex instytucjach?

Analiza oszustwa

Cały podstęp opierał się na jednej z podstawowych zasad socjotechniki: uzyskania dostępu do informacji, która mylnie jest postrzegana przez pracownika jako nieszkodliwa.

Pierwsza urzędniczka bankowa potwierdziła termin, jakim określa się numer identyfikacyjny, używany do kontaktów z CreditChex — „numer kupca". Druga podała numer linii telefonicznej używanej do połączeń z CreditChex i najistotniejszą informację — numer kupca przydzielony bankowi — uznała to za nieszkodliwe. W końcu myślała, że rozmawia z kimś z CreditChex, więc co może być szkodliwego w podaniu im tego numeru?

Wszystko to stworzyło grunt do trzeciej rozmowy. Grace miał wszystko, czego potrzebował, aby zadzwonić do CreditChex, podając się za pracownika National Bank — jednego z ich klientów i po prostu poprosić o informacje, których potrzebował.

Grace potrafił kraść informacje tak jak dobry oszust pieniądze, a do tego miał rozwinięty talent wyczuwania charakterów ludzi i tego, o czym w danej chwili myślą. Znał powszechną taktykę ukrywania kluczowych pytań wśród zupełnie niewinnych. Wiedział, że osobiste pytanie pozwoli sprawdzić chęć współpracy drugiej urzędniczki przed niewinnym zadaniem pytania o numer kupca.

Błąd pierwszej urzędniczki, polegający na potwierdzeniu nazewnictwa dla numeru identyfikacyjnego CreditChex był w zasadzie nie do uniknięcia. Informacja ta jest tak szeroko znana w branży bankowej, że wydaje się nie mieć wartości. Typowy przykład nieszkodliwej informacji. Jednak druga urzędniczka, Chris, nie powinna odpowiadać na pytania bez pozytywnej weryfikacji, że dzwoniący jest tym, za kogo się podaje. W najgorszym przypadku powinna zapytać o jego nazwisko i numer telefonu, po czym oddzwonić. W ten sposób, jeżeli później narodziłyby się jakiekolwiek wątpliwości, miałaby przynajmniej numer telefonu, spod którego dzwoniła dana osoba. W tym przypadku wykonanie telefonu zwrotnego znacznie utrudniłoby intruzowi udawanie przedstawiciela CreditChex.

Lepszym rozwiązaniem byłby telefon do CreditChex, przy użyciu numeru, z którego wcześniej korzystał bank, a nie tego, który poda dzwoniący. Telefon taki miałby na celu sprawdzenie, czy dana osoba rzeczywiście tam pracuje i czy firma przeprowadza właśnie jakieś badania klientów. Biorąc pod uwagę praktyczne aspekty pracy i fakt, że większość ludzi pracuje pod presją terminów, wymaganie takiej weryfikacji to dużo, chyba że pracownik ma podejrzenie, iż jest to próba inwigilacji.

Uwaga Mitnicka ➤

W tej sytuacji numer klienta spełniał taką samą rolę jak hasło. Jeżeli personel banku traktowałby ten numer w taki sam sposób jak numery PIN swoich kart kredytowych, uświadomiłby sobie poufną naturę tej informacji.

Pułapka na inżyniera

Wiadomo, że socjotechnika jest często stosowana przez „łowców głów" w celu rekrutacji utalentowanych pracowników. Oto przykład.

Pod koniec lat 90. pewna niezbyt uczciwa agencja rekrutacyjna podpisała umowę z nowym klientem, który szukał inżynierów elektryków z doświadczeniem w branży telekomunikacyjnej. Sprawę prowadziła kobieta znana ze swojego głębokiego głosu i seksownej maniery, której nauczyła się, by zdobywać zaufanie i bliski kontakt ze swoimi rozmówcami telefonicznymi.

Zdecydowała się zaatakować firmę będącą dostawcą usług telefonii komórkowej i spróbować zlokalizować jakichś inżynierów, którzy mogą mieć ochotę na przejście do konkurencji. Nie mogła oczywiście zadzwonić na centralę firmy i powiedzieć: „Chciałam rozmawiać z jakąś osobą z pięcioletnim doświadczeniem na stanowisku inżyniera". Zamiast tego, z powodów, które za chwilę staną się jasne, rozpoczęła polowanie na pracowników od poszukiwania pozornie bezwartościowej informacji, takiej, którą firma jest skłonna podać prawie każdemu, kto o nią poprosi.

Pierwsza rozmowa: recepcjonistka

Kobieta, podając się za Didi Sands, wykonała telefon do głównej siedziby dostawcy usług telefonii komórkowej. Oto fragment rozmowy:

RECEPCJONISTKA: Dzień dobry. Mówi Marie. W czym mogę pomóc?

DIDI: Może pani mnie połączyć z wydziałem transportu?

R: Nie jestem pewna, czy taki wydział istnieje. Spojrzę na spis. A kto mówi?

D: Didi.

R: Dzwoni pani z budynku czy... ?

D: Nie, dzwonię z zewnątrz.

R: Didi jak?

D: Didi Sands. Miałam gdzieś wewnętrzny do transportowego, ale go nie pamiętam.

R: Chwileczkę.

Aby załagodzić podejrzenia, Didi zadała w tym miejscu luźne, podtrzymujące rozmowę pytanie, mające pokazać, że jest z „wewnątrz" i jest obeznana z rozkładem budynków firmy.

D: W jakim budynku pani jest, w Lakeview czy w głównym?

R: W głównym (pauza). Podaję ten numer: 805 555 6469.

Aby mieć coś na zapas, gdyby telefon do wydziału transportowego w niczym jej nie pomógł, Didi poprosiła jeszcze o numer do wydziału nieruchomości. Recepcjonistka podała również i ten numer. Kiedy Didi poprosiła o połączenie z transportowym, recepcjonistka spróbowała, ale numer był zajęty.

W tym momencie Didi zapytała o *trzeci* numer telefonu do działu rachunkowości, który znajdował się w głównej siedzibie firmy w Austin w Teksasie. Recepcjonistka poprosiła ją, aby poczekała i wyłączyła na chwilę linię. Czy zadzwoniła do ochrony, że ma podejrzany telefon i coś się jej tu nie podoba? Otóż nie i Didi nawet nie brała tej możliwości pod uwagę. Była co prawda trochę natrętna, ale dla recepcjonistki to raczej nic dziwnego w jej pracy. Po około minucie recepcjonistka powróciła do rozmowy, sprawdziła numer do rachunkowości i połączyła Didi z tym wydziałem.

Druga rozmowa: Peggy

Następna rozmowa przebiegła następująco:

PEGGY: Rachunkowość, Peggy.

DIDI: Dzień dobry, Peggy, tu Didi z Thousand Oaks.

PEGGY: Dzień dobry, Didi.

DIDI: Jak się masz?

PEGGY: Dobrze.

W tym momencie Didi użyła częstego w firmie zwrotu, który opisuje kod opłaty, przypisujący wydatek z budżetu określonej organizacji lub grupie roboczej.

DIDI: To świetnie. Mam pytanie. Jak mam znaleźć centrum kosztów dla danego wydziału?

PEGGY: Musisz się skontaktować z analitykiem budżetowym danego wydziału.

DIDI: Nie wiesz, kto jest analitykiem dla dyrekcji w Thousand Oaks? Właśnie wypełniam formularz i nie znam prawidłowego centrum kosztów.

PEGGY: Ja tylko wiem, że jeśli ktokolwiek potrzebuje centrum kosztów, dzwoni do analityka budżetowego.

DIDI: A macie centrum kosztów dla waszego wydziału w Teksasie?

PEGGY: Mamy własne centrum kosztów. Widocznie góra stwierdziła, że więcej nie musimy wiedzieć.

DIDI: A z ilu cyfr składa się centrum kosztów? Jakie jest na przykład wasze centrum?

PEGGY: A wy jesteście w 9WC czy w SAT?

Didi nie miała pojęcia, jakich wydziałów lub grup dotyczyły te oznaczenia, ale nie miało to znaczenia.

DIDI: 9WC.

PEGGY: No to zwykle ma 4 cyfry. Jeszcze raz: skąd dzwonisz?

DIDI: Z dyrekcji w Thousand Oaks.

PEGGY: Podaję numer dla Thousand Oaks. To 1A5N. N jak Natalia.

Rozmawiając wystarczająco długo z osobą skłonną do pomocy, Didi uzyskała numer centrum kosztów, którego potrzebowała. Była to jedna z tych informacji, której nikt nie stara się chronić, ponieważ wydaje się ona bezwartościowa dla kogokolwiek spoza organizacji.

Trzecia rozmowa: pomocna pomyłka

W następnym kroku Didi wymieni numer centrum kosztów na coś, co przedstawia rzeczywistą wartość, wykorzystując go jak wygrany żeton w następnej rundzie gry.

Na początku zadzwoniła do wydziału nieruchomości, udając, że dodzwoniła się pod zły numer. Rozpoczynając od: „Nie chciałabym panu przeszkadzać...", powiedziała, że jest pracownikiem firmy i zgubiła gdzieś spis telefonów, a teraz nie wie, do kogo powinna zadzwonić, żeby dostać nowy. Mężczyzna powiedział, że wydrukowany spis jest już nieważny, bo bieżący jest dostępny na firmowej stronie intranetowej.

Didi powiedziała, że wolałaby korzystać z wydruku. Mężczyzna poradził jej, by zadzwoniła do działu publikacji, a następnie z własnej woli — być może chciał podtrzymać trochę dłużej rozmowę z kobietą o seksownym głosie — poszukał i podał jej numer telefonu.

Czwarta rozmowa: Bart z publikacji

W dziale publikacji rozmawiała z człowiekiem o imieniu Bart. Didi powiedziała, że dzwoni z Thousand Oaks i że mają nowego konsultanta, który potrzebuje kopii wewnętrznego spisu telefonów firmy.

Dodała, że wydrukowana kopia będzie lepsza dla konsultanta, nawet jeżeli nie jest najświeższa. Bart powiedział, że musi wypełnić odpowiedni formularz i przesłać mu go.

Didi stwierdziła, że skończyły jej się formularze, a sprawa była dla niej pilna i czy Bart mógłby być taki kochany i wypełnić formularz za nią. Zgodził się, okazując nadmierny entuzjazm, a Didi podała mu dane. Zamiast adresu fikcyjnego oddziału podała numer czegoś, co socjotechnicy określają mianem *punktu zrzutu* — w tym przypadku chodziło o jedną ze skrzynek pocztowych, jakie jej firma wynajmowała specjalnie na takie okazje.

Żargon ➤

Punkt zrzutu — w języku socjotechników miejsce, gdzie ofiara oszustwa przesyła dokumenty lub inne przesyłki (może to być np. skrzynka pocztowa, którą socjotechnik wynajmuje, zwykle posługując się fałszywym nazwiskiem).

W tym momencie przydaje się wcześniejsza zdobycz. Za przesłanie spisu będzie opłata. Nie ma sprawy — Didi podaje w tym momencie numer centrum kosztów dla Thousand Oaks: „1A5N. N jak Nancy".

Po paru dniach, kiedy dotarł spis telefonów, Didi stwierdziła, że otrzymała nawet więcej, niż się spodziewała. Spis wymieniał nie tylko nazwiska i numery telefonów, ale pokazywał też, kto dla kogo pracuje, czyli strukturę organizacyjną firmy.

Didi ze swoim ochrypłym głosem mogła w tym momencie rozpocząć telefonowanie w celu upolowania pracowników. Informacje konieczne do rozpoczęcia poszukiwań uzyskała dzięki darowi wymowy polerowanemu przez każdego zaawansowanego socjotechnika. Teraz mogła przejść do rekrutacji.

Analiza oszustwa

W tym ataku socjotechnicznym Didi rozpoczęła od uzyskania numerów telefonów do trzech oddziałów interesującej ją firmy. Było to łatwe, ponieważ numery te nie były zastrzeżone, szczególnie dla pracowników. Socjotechnik uczy się rozmawiać tak, jakby był pracownikiem firmy — Didi potrafiła to robić świetnie. Jeden z numerów telefonów doprowadził ją do tego, że otrzymała numer centrum kosztów, którego z kolei użyła, aby otrzymać kopię spisu telefonów firmy.

Główne narzędzia, jakich używała, to przyjazny ton, używanie żargonu firmowego i, przy ostatniej ofierze, trochę werbalnego trzepotania rzęsami.

Jeszcze jednym, jakże ważnym, narzędziem są zdolności socjotechnika do manipulacji, doskonalone przez długą praktykę i korzystanie z doświadczeń innych oszustów.

Uwaga Mitnicka ➤

Tak jak w układance, osobny fragment informacji może być sam w sobie nieznaczący, ale po połączeniu wielu takich klocków w całość otrzymujemy jasny obraz. W tym przypadku obrazem tym była cała wewnętrzna struktura przedsiębiorstwa.

Kolejne bezwartościowe informacje

Jakie inne, pozornie mało istotne, informacje, oprócz numeru centrum kosztów lub listy telefonów firmy, mogą być cennym łupem dla intruza?

Telefon do Petera Abelsa

— Dzień dobry — słyszy w słuchawce. — Tu mówi Tom z Parkhurst Travel. Pana bilety do San Francisco są do odbioru. Mamy je panu dostarczyć, czy sam pan je odbierze?

— San Francisco? — mówi Peter. — Nie wybieram się do San Francisco.

— A czy to pan Peter Abels?

— Tak, i nie planuję żadnych podróży.

— No tak — śmieje się rozmówca — a może jednak chciałby pan wybrać się do San Francisco?

— Jeżeli pan jest w stanie namówić na to mojego szefa... — mówi Peter, podtrzymując żartobliwą konwersację.

— To pewnie pomyłka — wyjaśnia głos w słuchawce. — W naszym systemie rezerwujemy podróże pod numerem pracownika. Pewnie ktoś użył złego numeru. Jaki jest pana numer?

Peter posłusznie recytuje swój numer. Czemu miałby tego nie robić? Przecież numer ten widnieje na każdym formularzu, który wypełnia, wiele osób w firmie ma do niego dostęp: kadry, płace, a nawet zewnętrzne biuro podróży. Nikt nie traktuje tego numeru jak tajemnicy. Co za różnica, czy go poda czy nie?

Odpowiedź jest prosta. Dwie lub trzy informacje mogą wystarczyć do tego, by wcielić się w pracownika firmy. Socjotechnik ukrywa się za czyjąś tożsamością. Zdobycie nazwiska pracownika, jego telefonu, numeru identyfikacyjnego i może jeszcze nazwiska oraz telefonu jego szefa wystarczy nawet mało doświadczonemu socjotechnikowi, aby być przekonującym dla swojej następnej ofiary.

Gdyby ktoś, kto mówi, że jest z innego oddziału firmy, zadzwonił wczoraj i, podając wiarygodny powód, poprosił o Twój numer identyfikacyjny, czy miałbyś jakieś opory przed jego podaniem?

A przy okazji, jaki jest Twój numer ubezpieczenia społecznego?

Uwaga Mitnicka ➤

Morał z historii jest taki: nie podawaj nikomu żadnych osobistych i wewnętrznych informacji lub numerów, chyba że rozpoznajesz głos rozmówcy, a ten tych informacji naprawdę potrzebuje.

Zapobieganie oszustwu

Firma jest odpowiedzialna za uświadomienie pracownikom, jakie mogą być skutki niewłaściwego obchodzenia się z niepublicznymi informacjami. Dobrze przemyślana polityka bezpieczeństwa informacji, połączona z odpowiednią edukacją i treningiem, poważnie zwiększy u pracowników świadomość znaczenia informacji firmowych i umiejętność ich chronienia. Polityka klasyfikacji danych wprowadza odpowiednie środki sterujące wypływem informacji. Jeżeli polityka taka nie istnieje, wszystkie informacje wewnętrzne muszą być traktowane jako poufne, chyba że wyraźnie wskazano inaczej.

W celu uniknięcia wypływu pozornie nieszkodliwych informacji z firmy należy podjąć następujące kroki:

- Wydział Bezpieczeństwa Informacji musi przeprowadzić szkolenie uświadamiające na temat metod stosowanych przez socjotechników. Jedną z opisanych powyżej metod jest uzyskiwanie pozornie błahych informacji i używanie ich w celu zbudowania chwilowego zaufania. Każdy z zatrudnionych musi być świadomy, że wiedza rozmówcy dotycząca procedur firmowych, żargonu i identyfikatorów w żaden sposób nie uwierzytelnia jego prośby o informację. Rozmówca może być byłym pracownikiem albo zewnętrznym wykonawcą usług,

który posiada informacje umożliwiające „poruszanie się" po firmie. Zgodnie z tym, każda firma jest odpowiedzialna za ustalenie odpowiednich metod uwierzytelniania do stosowania podczas kontaktów pracowników z osobami, których ci osobiście nie rozpoznają przez telefon.

- Osoby, które mają za zadanie stworzenie polityki klasyfikacji danych, powinny przeanalizować typowe rodzaje informacji, które mogą pomóc w uzyskaniu dostępu komuś podającemu się za pracownika. Wydają się one niegroźne, ale mogą prowadzić do zdobycia informacji poufnych. Mimo że nie podalibyśmy nikomu kodu PIN naszej karty kredytowej, czy powiedzielibyśmy komuś, jaki typ serwera wykorzystywany jest w naszej firmie? Czy ktoś mógłby użyć tej informacji, aby podać się za pracownika, który posiada dostęp do sieci komputerowej firmy?
- Czasami zwykła znajomość wewnętrznej terminologii może uczynić socjotechnika wiarygodnym. Napastnik często opiera się na tym założeniu, wyprowadzając w pole swoją ofiarę. Na przykład numer klienta to identyfikator, którego pracownicy działu nowych rachunków używają swobodnie na co dzień. Jednak numer ten nie różni się niczym od hasła. Jeżeli każdy pracownik uświadomi sobie naturę tego identyfikatora i spostrzeże, że służy on do pozytywnej identyfikacji dzwoniącego, być może zacznie traktować go z większym respektem.
- Żadna firma — powiedzmy, prawie żadna — nie podaje bezpośredniego numeru telefonu do członków zarządu lub rady nadzorczej. Większość firm nie ma jednak oporów przed podawaniem numerów telefonów większości wydziałów i innych jednostek organizacyjnych, w szczególności osobom, które wydają się być pracownikami firmy. Jednym z rozwiązań jest wprowadzenie zakazu podawania numerów wewnętrznych pracowników, konsultantów wykonujących usługi i przejściowo zatrudnionych w firmie jakimkolwiek osobom z zewnątrz. Co więcej, należy stworzyć procedurę opisującą krok po kroku identyfikację osoby proszącej o numer pracownika firmy.
- Kody księgowe grup i wydziałów oraz kopie spisów telefonów wewnętrznych (w formie wydruku, lub pliku w intranecie) to często obiekty pożądania socjotechników. Każda firma

potrzebuje pisemnej, rozdanej wszystkim procedury opisującej ujawnianie takich informacji. W środkach zapobiegawczych należy uwzględnić odnotowywanie przypadków udostępnienia informacji osobom spoza firmy.

- Informacje takie jak numer pracownika nie powinny być jedynym źródłem identyfikacji. Każdy pracownik musi nauczyć się weryfikować nie tylko tożsamość, ale również powód zapytania.
- W ramach poprawy bezpieczeństwa można rozważyć nauczenie pracowników następującego podejścia: uczymy się grzecznie odmawiać odpowiedzi na pytania i robienia przysług nieznajomym, dopóki prośba nie zostanie zweryfikowana. Następnie, zanim ulegniemy naturalnej chęci pomagania innym, postępujemy zgodnie z procedurami firmy, opisującymi weryfikację i udostępnianie niepublicznych informacji. Taki styl może nie iść w parze z naturalną tendencją do pomocy drugiemu człowiekowi, ale odrobina paranoi wydaje się konieczna, aby nie stać się kolejną ofiarą socjotechnika.

Historie przedstawione w tym rozdziale pokazują, w jaki sposób pozornie mało ważne informacje mogą stać się kluczem do najpilniej strzeżonych sekretów firmy.

Uwaga Mitnicka ➤

Jak głosi stare powiedzenie, nawet paranoicy miewają realnych wrogów. Musimy założyć, że każda firma ma swoich wrogów, których celem jest dostęp do infrastruktury sieci, a w rezultacie do tajemnic firmy. Czy naprawdę chcemy wspomóc statystykę przestępstw komputerowych? Najwyższy czas umocnić obronę, stosując odpowiednie metody postępowania przy wykorzystaniu polityki i procedur bezpieczeństwa.

3

Bezpośredni atak — wystarczy poprosić

Ataki socjotechników bywają zawiłe, składają się z wielu kroków i gruntownego planowania, często łącząc elementy manipulacji z wiedzą technologiczną.

Zawsze jednak uderza mnie to, że dobry socjotechnik potrafi osiągnąć swój cel prostym, bezpośrednim atakiem. Jak się przekonamy — czasami wystarczy poprosić o informację.

MLAC — szybka piłka

Interesuje nas czyjś zastrzeżony numer telefonu? Socjotechnik może odszukać go na pół tuzina sposobów (część z nich można poznać, czytając inne historie w tej książce), ale najprostszy scenariusz to taki, który wymaga tylko jednego telefonu. Oto on.

Proszę o numer...

Napastnik zadzwonił do mechanicznego centrum przydziału linii (MLAC) firmy telekomunikacyjnej i powiedział do kobiety, która odebrała telefon:

— Dzień dobry, tu Paul Anthony. Jestem monterem kabli. Proszę posłuchać, mam tu spaloną skrzynkę z centralką. Policja podejrzewa, że jakiś cwaniak próbował podpalić swój dom, żeby wyłudzić odszkodowanie. Przysłali mnie tu, żebym połączył od nowa całą centralkę na 200 odczepów. Przydałaby mi się pani pomoc. Które urządzenia powinny działać na South Main pod numerem 6723?

W innych wydziałach firmy telekomunikacyjnej, do której zadzwonił, wiedziano, że jakiekolwiek informacje lokacyjne lub niepublikowane numery telefonów można podawać tylko uprawnionym pracownikom firmy. Ale o istnieniu MLAC wiedzą raczej tylko pracownicy firmy. Co prawda informacje te są zastrzeżone, ale kto odmówi udzielenia pomocy pracownikowi mającemu do wykonania ciężką poważną robotę? Rozmówczyni współczuła mu, jej samej również zdarzały się trudne dni w pracy, więc obeszła trochę zasady i pomogła koledze z tej samej firmy, który miał problem. Podała mu oznaczenia kabli, zacisków i wszystkie numery przyporządkowane temu adresowi.

Analiza oszustwa

Jak wielokrotnie można było zauważyć w opisywanych historiach, znajomość żargonu firmy i jej struktury wewnętrznej — różnych biur i wydziałów, ich zadań i posiadanych przez nie informacji to część podstawowego zestawu sztuczek, używanych przez socjotechników.

Uwaga Mitnicka ➤

Ludzie z natury ufają innym, szczególnie kiedy prośba jest zasadna. Socjotechnicy używają tej wiedzy, by wykorzystać ofiary i osiągnąć swe cele.

Ścigany

Człowiek, którego nazwiemy Frank Parsons, od lat uciekał. Wciąż był poszukiwany przez rząd federalny za udział w podziemnej grupie antywojennej w latach 60. W restauracjach siadał twarzą do wejścia

i miał nawyk ciągłego spoglądania za siebie, wprowadzając w zakłopotanie innych ludzi. Co kilka lat zmieniał adres.

Któregoś razu Frank wylądował w obcym mieście i zaczął rozglądać się za pracą. Dla kogoś takiego jak Frank, który znał się bardzo dobrze na komputerach (oraz na socjotechnice, ale o tym nie wspominał w swoich listach motywacyjnych), znalezienie dobrej posady nie było problemem. Poza czasami recesji talenty ludzi z dużą wiedzą techniczną dotyczącą komputerów zwykle są poszukiwane i nie mają oni problemów z ustawieniem się. Frank szybko odnalazł ofertę dobrze płatnej pracy w dużym domu opieki, blisko miejsca, gdzie mieszkał.

To jest to — pomyślał. Ale kiedy zaczął brnąć przez formularze aplikacyjne, natknął się na przeszkodę: pracodawca wymagał od aplikanta kopii jego akt policyjnych, które należało uzyskać z policji stanowej. Stos papierów zawierał odpowiedni formularz prośby, który zawierał też kratkę na odcisk palca. Co prawda wymagany był jedynie odcisk prawego palca wskazującego, ale jeżeli sprawdzą jego odcisk z bazą danych FBI, prawdopodobnie wkrótce będzie pracował, ale w kuchni „domu opieki" sponsorowanego przez rząd federalny.

Z drugiej strony, Frank uświadomił sobie, że być może w jakiś sposób udałoby mu się przemknąć. Może policja stanowa w ogóle nie przesłała jego odcisków do FBI. Ale jak się o tym dowiedzieć?

Jak? Przecież był socjotechnikiem — jak myślicie, w jaki sposób się dowiedział? Oczywiście wykonał telefon na policję: „Dzień dobry. Prowadzimy badania dla Departamentu Sprawiedliwości New Jersey. Badamy wymagania dla nowego systemu identyfikacji odcisków palców. Czy mógłbym rozmawiać z kimś, kto jest dobrze zorientowany w waszych zadaniach i mógłby nam pomóc?".

Kiedy lokalny ekspert podszedł do telefonu, Frank zadał szereg pytań o systemy, jakich używają, możliwości wyszukiwania i przechowywania odcisków. Czy mieli jakieś problemy ze sprzętem? Czy korzystają z wyszukiwarki odcisków NCIC (Narodowego Centrum Informacji o Przestępstwach), czy mogą to robić tylko w obrębie stanu? Czy nauka obsługi sprzętu nie była zbyt trudna?

Chytrze przemycił pośród innych pytań jedno kluczowe.

Odpowiedź była muzyką dla jego uszu. Nie, nie byli związani z NCIC, sprawdzali tylko ze stanowym CII (Indeks Informacji o Przestępstwach). To było wszystko, co Frank chciał wiedzieć. Nie był notowany w tym stanie, więc przesłał swoją aplikację, został zatrudniony i nikt nigdy nie pojawił się u niego ze słowami: „Ci panowie są z FBI i mówią, że chcieliby z tobą porozmawiać".

Jak sam twierdził, okazał się idealnym pracownikiem.

Uwaga Mitnicka ➤

Zmyślni złodzieje informacji nie obawiają się dzwonienia do urzędników federalnych, stanowych lub przedstawicieli władzy lokalnej, aby dowiedzieć się czegoś o procedurach wspomagających prawo. Posiadając takie informacje, socjotechnik jest w stanie obejść standardowe zabezpieczenia w firmie.

Na portierni

Niezależnie od wprowadzanej komputeryzacji, firmy wciąż drukują codziennie tony papierów. Ważne pismo może być w naszej firmie zagrożone nawet, gdy zastosujemy właściwe środki bezpieczeństwa i opieczętujemy je jako tajne. Oto historia, która pokazuje, jak socjotechnik może wejść w posiadanie najbardziej tajnych dokumentów.

W pętli oszustwa

Każdego roku firma telekomunikacyjna publikuje książkę zwaną „Spis numerów testowych" (a przynajmniej publikowała, a jako że jestem nadal pod opieką kuratora, wolę nie pytać, czy robią to nadal). Dokument ten stanowił ogromną wartość dla phreakerów, ponieważ wypełniała go lista pilnie strzeżonych numerów telefonów, używanych przez firmowych specjalistów, techników i inne osoby do testowania łączy międzymiastowych i sprawdzania numerów, które były wiecznie zajęte.

Jeden z tych numerów, określany w żargonie jako *pętla*, był szczególnie przydatny. Phreakerzy używali go do szukania innych phreakerów i gawędzenia z nimi za darmo. Poza tym tworzyli dzięki niemu numery do oddzwaniania, które można było podać np. w banku. Socjotechnik zostawiał urzędnikowi w banku numer telefonu, pod którym można było go zastać. Kiedy bank oddzwaniał na numer testowy (tworzył pętlę), phreaker mógł spokojnie odebrać telefon, zabezpieczając się użyciem numeru, który nie był z nim skojarzony.

Spis numerów testowych udostępniał wiele przydatnych danych, które mogłyby być użyte przez głodnego informacji phreakera. Tak więc każdy nowy spis, publikowany co roku, stawał się obiektem pożądania młodych ludzi, których hobby polegało na eksploracji sieci telefonicznej.

Uwaga Mitnicka ➤

Trening bezpieczeństwa, przeprowadzony zgodnie z polityką firmy, stworzoną w celu ochrony zasobów informacyjnych, musi dotyczyć wszystkich jej pracowników, a w szczególności tych, którzy mają elektroniczny lub fizyczny dostęp do zasobów informacyjnych firmy.

Szwindel Steve'a

Oczywiście firmy telekomunikacyjne nie ułatwiają zdobycia takiego spisu, dlatego phreakerzy muszą wykazać się tu kreatywnością. W jaki sposób mogą tego dokonać? Gorliwy młodzieniec, którego marzeniem jest zdobycie spisu, mógł odegrać następujący scenariusz.

* * *

Pewnego ciepłego wieczoru południowokalifornijskiej jesieni Steve zadzwonił do biura niewielkiej centrali telekomunikacyjnej. Stąd biegną linie telefoniczne do wszystkich domów, biur i szkół w okolicy.

Kiedy technik będący na służbie odebrał telefon, Steve oświadczył, że dzwoni z oddziału firmy, który zajmuje się publikacją materiałów drukowanych.

— Mamy wasz nowy „Spis telefonów testowych" — powiedział — ale z uwagi na bezpieczeństwo nie możemy dostarczyć wam nowego spisu, dopóki nie odbierzemy starego. Gość, który odbiera spisy, właśnie się spóźnia. Gdyby pan zostawił wasz spis na portierni, mógłby on szybko wpaść, wziąć stary, podrzucić nowy i jechać dalej.

Niczego niepodejrzewający technik uznaje, że brzmi to rozsądnie. Robi dokładnie to, o co go poproszono, zostawiając na portierni swoją kopię spisu. Napisano na niej wielkimi czerwonymi literami tekst ostrzeżenia: „**TAJEMNICA FIRMY** — Z CHWILĄ DEZAKTUALIZACJI TEGO DOKUMENTU NALEŻY GO ZNISZCZYĆ".

Steve podjeżdża i rozgląda się uważnie dookoła, sprawdzając, czy nie ma policji lub ochrony firmy, która mogłaby zaczaić się za drzewami lub obserwować go z zaparkowanych samochodów. Nikogo nie widzi. Spokojnie odbiera upragnioną książkę i odjeżdża.

Jeszcze jeden przykład na to, jak łatwe dla socjotechnika jest otrzymanie czegoś, po prostu o to prosząc.

Atak na klienta

Nie tylko zasoby firmy mogą stać się obiektem ataku socjotechnika. Czasami jego ofiarą padają klienci firmy.

Praca w dziale obsługi klienta przynosi po części frustrację, po części śmiech, a po części niewinne błędy — niektóre z nich mogą mieć przykre konsekwencje dla klientów firmy.

Historia Josie Rodriguez

Josie Rodriguez pracowała od trzech lat na jednym ze stanowisk w biurze obsługi klienta w firmie Hometown Electric Power w Waszyngtonie. Uważano ją za jedną z lepszych pracownic. Była bystra i przytomna.

* * *

W tygodniu, w którym wypadało Święto Dziękczynienia, zadzwonił telefon. Rozmówca powiedział:

— Mówi Eduardo z działu fakturowania. Mam pewną panią na drugiej linii. To sekretarka z dyrekcji, która pracuje dla jednego z wiceprezesów. Prosi mnie o pewną informację, a ja nie mogę w tej chwili skorzystać z komputera. Dostałem e-maila od jednej dziewczyny z kadr zatytułowanego „ILOVEYOU" i kiedy otwarłem załącznik, komputer się zawiesił. Wirus. Dałem się nabrać na głupi wirus. Czy w związku z tym, mogłaby pani poszukać dla mnie informacji o kliencie?

— Pewnie — odpowiedziała Josie. — To całkiem zawiesza komputer? Straszne.

— Tak.

— Jak mogę pomóc? — zapytała Josie.

W tym momencie napastnik powołał się na informację, którą zdobył wcześniej podczas poszukiwań różnych danych pomocnych w uwiarygodnieniu się. Dowiedział się, że informacja, której poszukiwał, jest przechowywana w tak zwanym „systemie informacji o fakturach klienta" i dowiedział się, jak nazywali go pracownicy (CBIS).

— Czy może pani wywołać konto z CBIS? — zapytał.

— Tak, jaki jest numer konta?

— Nie mam numeru, musimy znaleźć po nazwisku.

— Dobrze. Jakie nazwisko?

— Heather Marning — przeliterował nazwisko, a Josie je wpisała.

— Już mam.

— Świetnie. To jest rachunek bieżący?

— Mhm, bieżący.
— Jaki ma numer? — zapytał.
— Ma pan coś do pisania?
— Mam.
— Konto numer BAZ6573NR27Q.
Odczytał jej zapisany numer i zapytał:
— A jaki jest adres obsługi?
Podała mu adres.
— A numer telefonu?
Josie posłusznie odczytała również tę informację.

Rozmówca podziękował jej, pożegnał się i odwiesił słuchawkę. Josie odebrała kolejny telefon, nawet nie myśląc o tym, co się stało.

Badania Arta Sealy'ego

Art Sealy porzucił pracę jako niezależny redaktor pracujący dla małych wydawnictw, kiedy wpadł na to, że może zarabiać, zdobywając informacje dla pisarzy i firm. Wkrótce odkrył, że honoraria, jakie mógłby pobierać, rosną proporcjonalnie do zbliżania się do subtelnej granicy linii oddzielającej działania legalne od nielegalnych. Nie zdając sobie z tego sprawy, i oczywiście nie nazywając rzeczy po imieniu, Art stał się socjotechnikiem używającym technik znanych każdemu poszukiwaczowi informacji. Okazał się naturalnym talentem w tej branży, dochodząc samemu do metod, których socjotechnicy muszą uczyć się od innych. Wkrótce przekroczył wspomnianą granicę bez najmniejszego poczucia winy.

* * *

Wynajął mnie człowiek, który pisał książkę o gabinecie prezydenta w czasach Nixona i szukał informatora, który dostarczyłby mu mniej znanych faktów na temat Williama E. Simona, będącego Sekretarzem Skarbu w rządzie Nixona. Pan Simon zmarł, ale autor znał nazwisko kobiety, która dla niego pracowała. Był prawie pewny, że mieszka ona w Waszyngtonie, ale nie potrafił zdobyć jej adresu. Nie miała również telefonu, a przynajmniej nie było go w książce. Tak więc, kiedy zadzwonił do mnie, powiedziałem mu, że to żaden problem.

Jest to robota, którą można załatwić zwykle jednym lub dwoma telefonami, jeżeli zrobi się to z głową. Od każdego lokalnego przedsiębiorstwa użyteczności publicznej raczej łatwo wyciągnąć informacje. Oczywiście trzeba trochę nakłamać, ale w końcu czym jest jedno małe niewinne kłamstwo?

Lubię stosować za każdym razem inne podejście — wtedy jest ciekawiej. „Tu mówi ten-a-ten z biura dyrekcji" zawsze nieźle działało. Albo „mam kogoś na linii z biura wiceprezesa X", które zadziałało też tym razem.

Trzeba wyrobić w sobie pewnego rodzaju instynkt socjotechnika. Wyczuwać chęć współpracy w osobie po drugiej stronie. Tym razem poszczęściło mi się — trafiłem na przyjazną i pomocną panią. Jeden telefon wystarczył, aby uzyskać adres i numer telefonu. Misja została wykonana.

Analiza oszustwa

Oczywiście Josie zdawała sobie sprawę, że informacja o kliencie jest poufna. Nigdy nie pozwoliłaby sobie na rozmowę na temat rachunku jakiegoś klienta z innym klientem lub na publiczne ujawnianie prywatnych informacji.

Jednak dla dzwoniącego z tej samej firmy stosuje się inne zasady. Kolega z pracy to członek tej samej drużyny — musimy sobie pomagać w wykonywaniu pracy. Człowiek z działu fakturowania mógł sam sobie sprawdzić te informacje w swoim komputerze, gdyby nie zawiesił go wirus. Cieszyła się, że mogła pomóc współpracownikowi.

Art stopniowo dochodził do kluczowej informacji, której naprawdę szukał, zadając po drodze pytania o rzeczy dla niego nieistotne, jak numer konta. Jednocześnie informacja o numerze konta stanowiła drogę ucieczki — gdyby Josie zaczęła coś podejrzewać, wykonałby drugi telefon, z większą szansą na sukces — znajomość numeru konta uczyniłaby go jeszcze bardziej wiarygodnym w oczach kolejnego urzędnika.

Josie nigdy nie zdarzyło się, by ktoś kłamał w taki sposób — nie przyszłoby jej do głowy, że rozmówca mógł nie być tak naprawdę z działu fakturowania. Oczywiście wina nie leży po stronie Josie, która nie została dobrze poinformowana o zasadach upewniania się co do tożsamości dzwoniącego przed omawianiem z nim informacji dotyczących czyjegoś konta. Nikt nigdy nie powiedział jej o niebezpieczeństwie takiego telefonu, jaki wykonał Art. Nie stanowiło to części polityki firmy, nie było elementem szkolenia i jej przełożony nigdy o tym nie wspomniał.

Uwaga Mitnicka ➤

Nigdy nie należy sądzić, że wszystkie ataki socjotechniczne muszą być gruntownie uknutą intrygą, tak skomplikowaną, że praktycznie niewykrywalną. Niektóre z nich to szybkie ataki z zaskoczenia, bardzo proste w formie. Jak widać, czasami wystarczy po prostu zapytać.

Zapobieganie oszustwu

Punkt, który należy umieścić w planie szkolenia z zakresu bezpieczeństwa, dotyczy faktu, że jeśli nawet dzwoniący lub odwiedzający zna nazwiska jakichś osób z firmy lub zna żargon i procedury, nie znaczy to, że podaje się za tego, kim jest. Zdecydowanie nie czyni go to w żaden sposób uprawnionym do otrzymywania wewnętrznych informacji lub wykonywania operacji na naszym komputerze lub sieci.

Szkolenie takie musi jasno uczyć, żeby w razie wątpliwości sprawdzać, sprawdzać i jeszcze raz sprawdzać.

W dawnych czasach dostęp do informacji wewnątrz firmy był oznaką rangi i przywilejem. Pracownicy otwierali piece, uruchamiali maszyny, pisali listy, wypełniali raporty. Brygadzista lub szef mówił im, co robić, kiedy i jak. Tylko brygadzista lub szef wiedzieli, ile elementów musi wyprodukować dany pracownik na jednej zmianie, jakie kolory i rozmiary mają być wypuszczone w tym tygodniu, w następnym i na koniec miesiąca.

Pracownicy obsługiwali maszyny, narzędzia i korzystali z materiałów. Szefowie dysponowali informacją, a pracownicy dowiadywali się jedynie tego, co niezbędne w ich pracy.

Prawda, że dziś wygląda to nieco inaczej? Wielu pracowników w fabryce obsługuje jakiś komputer lub maszynę sterowaną komputerowo. Dla zatrudnionych dostępne są krytyczne informacje, co ułatwia im wykonanie swojej części pracy — w obecnych czasach większość rzeczy, które robią, jest związana z informacją.

Dlatego też polityka bezpieczeństwa firmy musi sięgać wszędzie, niezależnie od stanowiska. Każdy musi zrozumieć, że nie tylko szefowie i dyrekcja są w posiadaniu informacji, których poszukiwać może napastnik. Dziś pracownik na każdym szczeblu, nawet niekorzystający z komputera, może stać się obiektem ataku. Nowo zatrudniony konsultant w dziale obsługi klienta może stanowić słabe ogniwo, które zostanie wykorzystane przez socjotechnika do swoich celów.

Szkolenie w zakresie bezpieczeństwa i polityka bezpieczeństwa firmy musi wzmacniać takie słabe ogniwa.