Sztuka podstępu. Łamałem ludzi, nie hasła

Autorzy: Kevin Mitnick, William L. Simon
Tłumaczenie: Jarosław Dobrzański
ISBN: 83-7361-116-9
Tytuł oryginału: The Art of Deception
Format: A5, stron: 380

Kevin Mitnick
najsłynniejszy haker świata i jego książka
"Sztuka podstępu. Łamałem ludzi, nie hasła"
w marcu w Polsce!

(...) Kilka dni później Rifkin poleciał do Szwajcarii, pobrał gotówkę i wyłożył ponad 8 milionów dolarów na diamenty z rosyjskiej agencji. Potem wrócił do Stanów trzymając w czasie kontroli celnej diamenty w pasku na pieniądze. Przeprowadził największy skok na bank w historii, nie używając ani pistoletu, ani komputera. Jego przypadek w końcu dostał się do „Księgi Rekordów Guinessa" w kategorii „największe oszustwo komputerowe".

Stanley Rifikin użył sztuki podstępu – umiejętności i technik, które dziś nazywają się socjotechniką. Wymagało to tylko dokładnego planu i daru wymowy. (...)

Kevina Mitnicka jako superhakera obawiało się tysiące Amerykanów. Był jedną z najintensywniej poszukiwanych osób w historii FBI. Po aresztowaniu groziła mu kara kilkuset lat pozbawienia wolności, mimo że nigdy nie oskarżono go o czerpanie korzyści finansowych z hakerstwa. Wyrokiem sądu zakazano mu jakiegokolwiek dostępu do komputera. Sąd uzasadnił wyrok:

„Uzbrojony w klawiaturę jest groźny dla społeczeństwa".

Po zwolnieniu Mitnick zupełnie odmienił swoje życie. Stał się najbardziej poszukiwanym ekspertem w Stanach od spraw bezpieczeństwa systemów komputerowych.
W „Sztuce podstępu" odkrywa tajemnice swojego „sukcesu", opisuje jak łatwo jest pokonać bariery w uzyskiwaniu ściśle tajnych informacji, jak łatwo dokonać sabotażu przedsiębiorstwa, urzędu czy jakiejkolwiek innej instytucji. Robił to setki razy wykorzystując przemyślne techniki wywierania wpływu na ludzi. Mitnick udowadnia, jak złudna jest opinia o bezpieczeństwie danych prywatnych i służbowych, pokazuje jak ominąć systemy warte miliony dolarów, wykorzystując do tego celu ludzi je obsługujących.

Sensacyjne historie opisane w książce pomogą w obronie przed najpoważniejszym zagrożeniem bezpieczeństwa – ludzką naturą. Pamiętaj, że celem ataku możesz być i Ty.

„Tylko dwie rzeczy są nieskończone: wszechświat i ludzka głupota, chociaż co do pierwszego nie mam pewności"

– Albert Einstein

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Przedmowa

Są na świecie hakerzy, którzy niszczą cudze pliki lub całe dyski twarde — nazywa się ich *crakerami* lub po prostu *wandalami*. Są również niedoświadczeni hakerzy, którzy zamiast uczyć się technologii, znajdują w sieci odpowiednie narzędzia hakerskie, za pomocą których włamują się do systemów komputerowych. Mówi się o nich *script kiddies*. Bardziej doświadczeni hakerzy sami tworzą programy hakerskie, które potem umieszczają w sieci lub na listach dyskusyjnych. Istnieją też takie osoby, których w ogóle nie obchodzi technologia, a komputera używają jedynie jako narzędzia pomagającego im kraść pieniądze, towary i korzystać za darmo z usług.

Wbrew mitowi o Kevinie Mitnicku, jaki stworzyły media, nigdy jako haker nie miałem złych zamiarów.

Wyprzedzam jednak fakty.

Początki

Ścieżka, na którą wstąpiłem, miała zapewne swój początek w dzieciństwie. Byłem beztroskim, ale znudzonym dzieckiem. Mama, po rozstaniu z ojcem (miałem wtedy 3 lata), pracowała jako kelnerka, by nas utrzymać. Można sobie wyobrazić jedynaka wychowywanego przez wiecznie zabieganą matkę — chłopaka samotnie spędzającego całe dnie. Byłem swoją własną nianią.

Dorastając w San Fernando Valley, miałem całą młodość na zwiedzanie Los Angeles. W wieku 12 lat znalazłem sposób na darmowe podróżowanie po całym okręgu Los Angeles. Któregoś dnia, jadąc autobusem, odkryłem, że układ otworów na bilecie tworzony przez kierowcę podczas kasowania oznacza dzień, godzinę i trasę przejazdu autobusu. Przyjaźnie nastawiony kierowca odpowiedział na wszystkie moje dokładnie przemyślane pytania, łącznie z tym, gdzie można kupić kasownik, którego używa.

Bilety te pozwalały na przesiadki i kontynuowanie podróży. Wymyśliłem wtedy, jak ich używać, aby jeździć wszędzie za darmo. Zdobycie nieskasowanych biletów to była pestka: kosze na śmieci w zajezdniach autobusowych pełne były nie do końca zużytych bloczków biletowych, których kierowcy pozbywali się na koniec zmiany. Mając nieskasowane bilety i kasownik, mogłem sam je oznaczać w taki sposób, aby dostać się w dowolne miejsce w Los Angeles. Wkrótce znałem wszystkie układy tras autobusów na pamięć. To wczesny przykład mojej zadziwiającej zdolności do zapamiętywania pewnego rodzaju informacji. Do dzisiaj pamiętam numery telefonów, hasła i tym podobne szczegóły — nawet te zapamiętane w dzieciństwie.

Innym moim zainteresowaniem, jakie ujawniło się dość wcześnie, była fascynacja sztuczkami magicznymi. Po odkryciu, na czym polega jakaś sztuczka, ćwiczyłem tak długo, aż ją opanowałem. W pewnym sensie to dzięki magii odkryłem radość, jaką można czerpać z wprowadzania ludzi w błąd.

Od phreakera do hakera

Moje pierwsze spotkanie z czymś, co później nauczyłem się określać mianem *socjotechniki*, miało miejsce w szkole średniej. Poznałem wtedy kolegę, którego pochłaniało hobby zwane *phreakingiem*. Polegało ono na włamywaniu się do sieci telefonicznych, przy wykorzystaniu do tego celu pracowników służb telefonicznych oraz wiedzy o działaniu sieci. Pokazał mi sztuczki, jakie można robić za pomocą telefonu: zdobywanie każdej informacji o dowolnym abonencie sieci czy korzystanie z tajnego numeru testowego do długich darmowych rozmów zamiejscowych (potem okazało się, że numer wcale nie był testowy — rozmowami, które wykonywaliśmy, obciążany był rachunek jakiejś firmy).

Takie były moje początki w dziedzinie socjotechniki — swojego rodzaju przedszkole. Ten kolega i jeszcze jeden *phreaker*, którego wkrótce poznałem, pozwolili mi posłuchać rozmów telefonicznych, jakie prze-

prowadzali z pracownikami firm telekomunikacyjnych. Wszystkie rzeczy, które mówili, brzmiały bardzo wiarygodnie. Dowiedziałem się o sposobie działania różnych firm z tej branży, nauczyłem się żargonu i procedur, stosowanych przez ich pracowników. „Trening" nie trwał długo — nie potrzebowałem go. Wkrótce sam robiłem wszystkie te rzeczy lepiej niż moi nauczyciele, pogłębiając wiedzę w praktyce.

W ten sposób wyznaczona została droga mojego życia na najbliższe 15 lat.

Jeden z moich ulubionych kawałów polegał na uzyskaniu dostępu do centrali telefonicznej i zmianie rodzaju usługi przypisanej do numeru telefonu znajomego *phreakera*. Kiedy ten próbował zadzwonić z domu, słyszał w słuchawce prośbę o wrzucenie monety, ponieważ centrala odbierała informację, że dzwoni on z automatu.

Absorbowało mnie wszystko, co dotyczyło telefonów. Nie tylko elektronika, centrale i komputery, ale również organizacja, procedury i terminologia. Po jakimś czasie wiedziałem o sieci telefonicznej chyba więcej niż jakikolwiek jej pracownik. Rozwinąłem również swoje umiejętności w dziedzinie socjotechniki do tego stopnia, że w wieku 17 lat byłem w stanie wmówić prawie wszystko większości pracownikom firm telekomunikacyjnych, czy to przez telefon, czy rozmawiając osobiście.

Moja znana ogółowi kariera hakera rozpoczęła się właściwie w szkole średniej. Nie mogę tu opisywać szczegółów, wystarczy, że powiem, iż głównym motywem moich pierwszych włamań była chęć bycia zaakceptowanym przez grupę podobnych mi osób.

Wtedy określenia *haker* używaliśmy w stosunku do kogoś, kto spędzał dużo czasu na eksperymentowaniu z komputerami i oprogramowaniem, opracowując bardziej efektywne programy lub znajdując lepsze sposoby rozwiązywania jakichś problemów. Określenie to dzisiaj nabrało pejoratywnego charakteru i kojarzy się z „groźnym przestępcą". Ja używam go tu jednak w takim znaczeniu, w jakim używałem go zawsze — czyli tym wcześniejszym, łagodniejszym.

Po ukończeniu szkoły średniej studiowałem informatykę w Computer Learning Center w Los Angeles. Po paru miesiącach szkolny administrator komputerów odkrył, że znalazłem lukę w systemie operacyjnym i uzyskałem pełne przywileje administracyjne w systemie. Najlepsi eksperci spośród wykładowców nie potrafili dojść do tego, w jaki sposób to zrobiłem. Nastąpił wówczas być może jeden z pierwszych przypadków „zatrudnienia" hakera — dostałem propozycję nie do odrzucenia: albo w ramach pracy zaliczeniowej poprawię bezpieczeństwo szkolnego systemu komputerowego, albo zostanę zawieszony za włamanie się do systemu. Oczywiście wybrałem to pierwsze i dzięki temu mogłem ukończyć szkołę z wyróżnieniem.

Socjotechnik

Niektórzy ludzie wstają rano z łóżka, by odbębniać powtarzalne czynności w przysłowiowym kieracie. Ja miałem to szczęście, że zawsze lubiłem swoją pracę. Najwięcej wyzwań, sukcesów i zadowolenia przyniosła mi praca prywatnego detektywa. Szlifowałem tam swoje umiejętności w sztuce zwanej *socjotechniką* — skłanianiem ludzi do tego, by robili rzeczy, których zwykle nie robi się dla nieznajomych. Za to mi płacono.

Stanie się biegłym w tej branży nie było dla mnie trudne. Rodzina ze strony mojego ojca od pokoleń zajmowała się handlem — może więc umiejętność perswazji i wpływania na innych jest cechą dziedziczną. Połączenie potrzeby manipulowania ludźmi z umiejętnością i talentem w dziedzinie perswazji i wpływu na innych to cechy idealnego socjotechnika.

Można powiedzieć, że istnieją dwie specjalizacje w zawodzie artysty-manipulatora. Ktoś, kto wyłudza od ludzi pieniądze, to pospolity oszust. Z kolei ktoś, kto stosuje manipulację i perswazję wobec firm, zwykle w celu uzyskania informacji, to *socjotechnik*. Od czasu mojej pierwszej sztuczki z biletami autobusowymi, kiedy byłem jeszcze zbyt młody, aby uznać, że robię coś złego, zacząłem rozpoznawać w sobie talent do dowiadywania się o rzeczach, o których nie powinienem wiedzieć. Rozwijałem ten talent, używając oszustw, posługując się żargonem i rozwiniętą umiejętnością manipulacji.

Jednym ze sposobów, w jaki pracowałem nad rozwijaniem umiejętności w moim rzemiośle (jeżeli można to nazwać rzemiosłem), było próbowanie uzyskania jakiejś informacji, na której nawet mi nie zależało. Chodziło o to, czy jestem w stanie skłonić osobę po drugiej stronie słuchawki do tego, by mi jej udzieliła — ot tak, w ramach ćwiczenia. W ten sam sposób, w jaki kiedyś ćwiczyłem sztuczki magiczne, ćwiczyłem teraz sztukę motywowania. Dzięki temu wkrótce odkryłem, że jestem w stanie uzyskać praktycznie każdą informację, jakiej potrzebuję.

Wiele lat później, zeznając w Kongresie przed senatorami, Liebermanem i Thompsonem, powiedziałem:

Udało mi się uzyskać nieautoryzowany dostęp do systemów komputerowych paru największych korporacji na tej planecie, spenetrować najlepiej zabezpieczone z istniejących systemów komputerowych. Używałem narzędzi technologicznych i nie związanych z technologią, aby uzyskać dostęp do kodu źródłowego różnych systemów operacyjnych, urządzeń telekomunikacyjnych i poznawać ich działanie oraz słabe strony.

Tak naprawdę, zaspakajałem jedynie moją własną ciekawość, przekonywałem się o możliwościach i wyszukiwałem tajne informacje o systemach operacyjnych, telefonach komórkowych i wszystkim innym, co budziło moje zainteresowanie.

Podsumowanie

Po aresztowaniu przyznałem, że to, co robiłem, było niezgodne z prawem i że dopuściłem się naruszenia prywatności.

Moje uczynki były powodowane ciekawością — pragnąłem wiedzieć wszystko, co się dało o tym, jak działają sieci telefoniczne oraz podsystemy wejścia–wyjścia komputerowych systemów bezpieczeństwa. Z dziecka zafascynowanego sztuczkami magicznymi stałem się najgroźniejszym hakerem świata, którego obawia się rząd i korporacje. Wracając pamięcią do ostatnich trzydziestu lat mojego życia, muszę przyznać, że dokonałem paru bardzo złych wyborów, sterowany ciekawością, pragnieniem zdobywania wiedzy o technologiach i dostarczania sobie intelektualnych wyzwań.

Zmieniłem się. Dzisiaj wykorzystuję mój talent i wiedzę o bezpieczeństwie informacji i socjotechnice, jaką udało mi się zdobyć, aby pomagać rządowi, firmom i osobom prywatnym w wykrywaniu, zapobieganiu i reagowaniu na zagrożenia bezpieczeństwa informacji.

Książka ta to jeszcze jeden sposób wykorzystania mojego doświadczenia w pomaganiu innym w radzeniu sobie ze złodziejami informacji. Mam nadzieję, że opisane tu przypadki będą zajmujące, otwierające oczy i mające jednocześnie wartość edukacyjną.

1

Pięta achillesowa systemów bezpieczeństwa

Firma może dokonać zakupu najlepszych i najdroższych technologii bezpieczeństwa, wyszkolić personel tak, aby każda poufna informacja była trzymana w zamknięciu, wynająć najlepszą firmę chroniącą obiekty i wciąż pozostać niezabezpieczoną.

Osoby prywatne mogą niewolniczo trzymać się wszystkich najlepszych zasad zalecanych przez ekspertów, zainstalować wszystkie najnowsze produkty poprawiające bezpieczeństwo i skonfigurować odpowiednio system, uruchamiając wszelkie jego usprawnienia i wciąż pozostawać niezabezpieczonymi.

Czynnik ludzki

Zeznając nie tak dawno temu przed Kongresem, wyjaśniłem, że często uzyskiwałem hasła i inne poufne informacje od firm, podając się za kogoś innego i *po prostu o nie prosząc*.

Tęsknota za poczuciem absolutnego bezpieczeństwa jest naturalna, ale prowadzi wielu ludzi do fałszywego poczucia braku zagrożenia.

Weźmy za przykład człowieka odpowiedzialnego i kochającego, który zainstalował w drzwiach wejściowych Medico (zamek bębnowy słynący z tego, że nie można go otworzyć wytrychem), aby ochronić swoją żonę, dzieci i swój dom. Po założeniu zamka poczuł się lepiej, ponieważ jego rodzina stała się bardziej bezpieczna. Ale co będzie, jeżeli napastnik wybije szybę w oknie lub złamie kod otwierający bramę garażu? Niezależnie od kosztownych zamków, domownicy wciąż nie są bezpieczni. A co w sytuacji, gdy zainstalujemy kompleksowy system ochrony? Już lepiej, ale wciąż nie będzie gwarancji bezpieczeństwa.

Dlaczego? Ponieważ to *czynnik ludzki* jest piętą achillesową systemów bezpieczeństwa.

Bezpieczeństwo staje się zbyt często iluzją. Jeżeli do tego dodamy łatwowierność, naiwność i ignorancję, sytuacja dodatkowo się pogarsza. Najbardziej poważany naukowiec XX wieku, Albert Einstein, podobno powiedział: „Tylko dwie rzeczy są nieskończone: wszechświat i ludzka głupota, chociaż co do pierwszego nie mam pewności". W rezultacie atak socjotechnika udaje się, bo ludzie bywają głupi. Częściej jednak ataki takie są skuteczne, ponieważ ludzie nie rozumieją sprawdzonych zasad bezpieczeństwa.

Mając podobne podejście jak uświadomiony w sprawach bezpieczeństwa pan domu, wielu zawodowców z branży IT ma błędne mniemanie, że w dużym stopniu uodpornili swoje firmy na ataki poprzez zastosowanie standardowych produktów typu *firewall*, systemów detekcji intruzów i zaawansowanych rozwiązań uwierzytelniających, takich jak kody zależne od czasu lub karty biometryczne. Każdy, kto uważa, że same produkty zabezpieczające zapewniają realne bezpieczeństwo, tworzy jego *iluzję*. To klasyczny przypadek życia w świecie fantazji: osoby takie mogą prędzej czy później stać się ofiarami ataku.

Jak ujmuje to znany konsultant ds. bezpieczeństwa, Bruce Schneider: „Bezpieczeństwo to nie produkt — to proces". Rozwińmy tę myśl: bezpieczeństwo nie jest problemem technologicznym, tylko problemem związanym z ludźmi i zarządzaniem.

W miarę wymyślania coraz to nowych technologii zabezpieczających, utrudniających znalezienie technicznych luk w systemie, napastnicy będą zwracać się w stronę ludzkich słabości. Złamanie „ludzkiej" bariery jest o wiele prostsze i często wymaga jedynie inwestycji rzędu kosztu rozmowy telefonicznej, nie mówiąc już o mniejszym ryzyku.

Klasyczny przypadek oszustwa

Kto stanowi największe zagrożenie bezpieczeństwa kapitału firmy? Odpowiedź jest prosta: socjotechnik — pozbawiony skrupułów magik, który, gdy patrzysz na jego lewą rękę, prawą kradnie Twoje tajemnice. Do tego często bywa tak miły, elokwentny i uprzejmy, iż naprawdę cieszysz się, że go spotkałeś.

Spójrzmy na przykład zastosowania socjotechniki. Niewielu dziś pamięta jeszcze młodego człowieka, który nazywał się Stanley Mark Rifkin, i jego przygodę z nieistniejącym już Security Pacific National Bank w Los Angeles. Sprawozdania z jego eskapady różnią się między sobą, a sam Rifkin (podobnie jak ja) nigdy nie opowiedział swojej wersji tej historii, dlatego zawarty tu opis opiera się na opublikowanych informacjach.

Łamanie kodu

Któregoś dnia roku 1978 Rifkinowi udało się dostać do przeznaczonego tylko dla personelu pokoju kontrolnego przelewów elektronicznych banku Security Pacific, z którego pracownicy wysyłali i odbierali przelewy na łączną sumę miliarda dolarów dziennie.

Pracował wtedy dla firmy, która podpisała z bankiem kontrakt na stworzenie systemu kopii zapasowych w pokoju przelewów na wypadek awarii głównego komputera. To umożliwiło mu dostęp do procedur transferowych, łącznie z tymi, które określały, w jaki sposób były one zlecane przez pracowników banku. Dowiedział się, że osoby upoważnione do zlecania przelewów otrzymywały każdego ranka pilnie strzeżony kod używany podczas dzwonienia do pokoju przelewów.

Urzędnikom z pokoju przelewów nie chciało się zapamiętywać codziennych kodów, zapisywali więc obowiązujący kod na kartce papieru i umieszczali ją w widocznym dla nich miejscu. Tego listopadowego dnia Rifkin miał szczególny powód do odwiedzin pomieszczenia. Chciał rzucić okiem na tę kartkę.

Po pojawieniu się w pokoju zwrócił uwagę na procedury operacyjne, prawdopodobnie w celu upewnienia się, że system kopii zapasowych będzie poprawnie współpracował z podstawowym systemem, jednocześnie ukradkiem odczytując kod bezpieczeństwa z kartki papieru i zapamiętując go. Po kilku minutach wyszedł. Jak później powiedział, czuł się, jakby właśnie wygrał na loterii.

Było sobie konto w szwajcarskim banku

Po wyjściu z pokoju, około godziny 15:00, udał się prosto do automatu telefonicznego w marmurowym holu budynku, wrzucił monetę i wykręcił numer pokoju przelewów. Ze Stanleya Rifkina, współpracownika banku, zmienił się w Mike'a Hansena — pracownika Wydziału Międzynarodowego banku.

Według jednego ze źródeł rozmowa przebiegała następująco:

— Dzień dobry, mówi Mike Hansen z międzynarodowego — powiedział do młodej pracownicy, która odebrała telefon.

Dziewczyna zapytała o numer jego biura. Była to standardowa procedura, na którą był przygotowany.

— 286 — odrzekł.

— Proszę podać kod — powiedziała wówczas pracownica.

Rifkin stwierdził później, że w tym momencie udało mu się opanować łomot napędzanego adrenaliną serca.

— 4789 — odpowiedział płynnie.

Potem zaczął podawać szczegóły przelewu: dziesięć milionów dwieście tysięcy dolarów z Irving Trust Company w Nowym Jorku do Wozchod Handels Bank of Zurich w Szwajcarii, gdzie wcześniej założył konto.

— Przyjęłam. Teraz proszę podać kod międzybiurowy.

Rifkin oblał się potem. Było to pytanie, którego nie przewidział, coś, co umknęło mu w trakcie poszukiwań. Zachował jednak spokój, udając, że nic się nie stało, i odpowiedział na poczekaniu, nie robiąc nawet najmniejszej pauzy: „Muszę sprawdzić. Zadzwonię za chwilę". Od razu zadzwonił do innego wydziału banku, tym razem podając się za pracownika pokoju przelewów. Otrzymał kod międzybiurowy i zadzwonił z powrotem do dziewczyny w pokoju przelewów.

Zapytała o kod i powiedziała: „Dziękuję" (biorąc pod uwagę okoliczności, jej podziękowanie można by odebrać jako ironię).

Dokończenie zadania

Kilka dni później Rifkin poleciał do Szwajcarii, pobrał gotówkę i wyłożył ponad 8 milionów dolarów na diamenty z rosyjskiej agencji. Potem wrócił do Stanów, trzymając w czasie kontroli celnej diamenty w pasku na pieniądze. Przeprowadził największy skok na bank w historii, nie używając ani pistoletu, ani komputera. Jego przypadek w końcu

dostał się do *Księgi Rekordów Guinessa* w kategorii „największe oszustwo komputerowe".

Stanley Rifkin użył sztuki manipulacji — umiejętności i technik, które dziś nazywa się socjotechniką. Wymagało to tylko dokładnego planu i daru wymowy.

O tym właśnie jest ta książka — o metodach socjotechnicznych (w których sam jestem biegły) i o sposobach, jakimi jednostki i organizacje mogą się przed nimi bronić.

Natura zagrożenia

Historia Rifkina jest dowodem na to, jak złudne może być nasze poczucie bezpieczeństwa. Podobne incydenty — może nie dotyczące 10 milionów dolarów, niemniej jednak szkodliwe — zdarzają się *codziennie*. Być może w tym momencie tracisz swoje pieniądze lub ktoś kradnie Twoje plany nowego produktu i nawet o tym nie wiesz. Jeżeli coś takiego nie wydarzyło się jeszcze w Twojej firmie, pytanie nie brzmi, *czy* się wydarzy, ale *kiedy*.

Rosnąca obawa

Instytut Bezpieczeństwa Komputerowego w swoich badaniach z 2001 roku, dotyczących przestępstw komputerowych, stwierdził, że w ciągu roku 85% ankietowanych organizacji odnotowało naruszenie systemów bezpieczeństwa komputerowego. Jest to zdumiewający odsetek: tylko piętnaście z każdych stu firm mogło powiedzieć, że nie miało z tym kłopotów. Równie szokująca jest ilość organizacji, która zgłosiła doznanie strat z powodu włamań komputerowych — 64%. Ponad połowa badanych firm poniosła straty finansowe w ciągu jednego roku.

Moje własne doświadczenia każą mi sądzić, że liczby w tego typu raportach są przesadzone. Mam podejrzenia co do trybu przeprowadzania badań, nie świadczy to jednak o tym, że straty nie są w rzeczywistości wielkie. Nie przewidując tego typu sytuacji, skazujemy się z góry na przegraną.

Dostępne na rynku i stosowane w większości firm produkty poprawiające bezpieczeństwo służą głównie do ochrony przed atakami ze strony amatorów, np. dzieciaków zwanych *script kiddies*, które wcielają się w hakerów, używając programów dostępnych w sieci, i w większo-

ści są jedynie utrapieniem. Największe straty i realne zagrożenie płynie ze strony bardziej wyrafinowanych hakerów, którzy mają jasno określone zadania, działają z chęci zysku i koncentrują się podczas danego ataku na wybranym celu, zamiast infiltrować tyle systemów, ile się da, jak to zwykle robią amatorzy. Przeciętni włamywacze zwykle są nastawieni na ilość, podczas gdy profesjonaliści są zorientowani na informacje istotne i wartościowe.

Technologie takie jak uwierzytelnianie (sprawdzanie tożsamości), kontrola dostępu (zarządzanie dostępem do plików i zasobów systemowych) i systemy detekcji intruzów (elektroniczny odpowiednik alarmów przeciwwłamaniowych) są nieodzownym elementem programu ochrony danych firmy. Typowa firma wydaje dziś jednak więcej na kawę niż na środki zabezpieczające przed atakami na systemy bezpieczeństwa.

Podobnie jak umysł kleptomana nie może oprzeć się pokusie, tak umysł hakera jest owładnięty żądzą obejścia systemów zabezpieczających. Hakerzy potwierdzają w ten sposób swój intelektualny kapitał.

Metody oszustwa

Popularne jest powiedzenie, że bezpieczny komputer to wyłączony komputer. Zgrabne, ale nieprawdziwe: oszust po prostu namawia kogoś do pójścia do biura i włączenia komputera. Przeciwnik, który potrzebuje informacji, zwykle może ją uzyskać na parę różnych sposobów. Jest to tylko kwestia czasu, cierpliwości, osobowości i uporu. W takiej chwili przydaje się znajomość sztuki manipulacji.

Aby pokonać zabezpieczenia, napastnik, intruz lub socjotechnik musi znaleźć sposób na oszukanie zaufanego pracownika w taki sposób, aby ten wyjawił jakąś informację, trik lub z pozoru nieistotną wskazówkę umożliwiającą dostanie się do systemu. Kiedy zaufanych pracowników można oszukiwać lub manipulować nimi w celu ujawnienia poufnych informacji lub kiedy ich działania powodują powstawanie luk w systemie bezpieczeństwa, umożliwiających napastnikowi przedostanie się do systemu, wówczas nie ma takiej technologii, która mogłaby ochronić firmę. Tak jak kryptografowie są czasami w stanie odszyfrować tekst zakodowanej wiadomości dzięki odnalezieniu słabych miejsc w kodzie, umożliwiających obejście technologii szyfrującej, tak socjotechnicy używają oszustwa w stosunku do pracowników firmy, aby obejść technologię zabezpieczającą.

Nadużywanie zaufania

W większości przypadków socjotechnicy mają duże zdolności oddziaływania na ludzi. Potrafią być czarujący, uprzejmi i łatwo ich polubić — posiadają cechy potrzebne do tego, aby zyskać sobie zrozumienie i zaufanie innych. Doświadczony socjotechnik jest w stanie uzyskać dostęp do praktycznie każdej informacji, używając strategii i taktyki przynależnych jego rzemiosłu.

Zmyślni technolodzy drobiazgowo opracowali systemy zabezpieczania informacji, aby zminimalizować ryzyko związane ze stosowaniem komputerów; zapomnieli jednak o najistotniejszej kwestii — czynniku ludzkim. Pomimo naszego intelektu, my, ludzie, pozostajemy największym zagrożeniem dla swojego bezpieczeństwa.

Amerykańska mentalność

Nie jesteśmy w pełni świadomi zagrożeń, szczególnie w świecie zachodnim. W USA w większości przypadków ludzie nie są uczeni podejrzliwości wobec drugiego człowieka. Są przyzwyczajani do zasady „kochaj sąsiada swego", ufają sobie nawzajem. Organizacje ochrony sąsiedzkiej mają często problemy z nakłonieniem ludzi do zamykania domów i samochodów. Te środki ochrony wydają się oczywiste, jednak wielu Amerykanów je ignoruje, wybierając życie w świecie marzeń — do pierwszej nauczki.

Zdajemy sobie sprawę, że nie wszyscy ludzie są dobrzy i uczciwi, ale zbyt często zachowujemy się, jakby tacy właśnie byli. Amerykanie są tego szczególnym przypadkiem — jako naród stworzyli sobie koncepcję wolności polegającą na tym, że najlepsze miejsce do życia jest tam, gdzie niepotrzebne są zamki ani klucze.

Większość ludzi wychodzi z założenia, że nie zostaną oszukani przez innych, ponieważ takie przypadki zdarzają się rzadko. Napastnik, zdając sobie sprawę z panującego przesądu, formułuje swoje prośby w bardzo przekonujący, nie wzbudzający żadnych podejrzeń sposób, wykorzystując zaufanie ofiary.

Naiwność organizacyjna

To swoiste domniemanie niewinności, będące składnikiem amerykańskiej mentalności, ujawniło się szczególnie w początkach istnienia sieci komputerowych. ARPANET, przodek Internetu, został

stworzony do wymiany informacji pomiędzy rządem a instytucjami badawczymi i naukowymi. Celem była dostępność informacji i postęp technologiczny. Wiele instytucji naukowych tworzyło wczesne systemy komputerowe z minimalnymi tylko zabezpieczeniami lub zupełnie ich pozbawione. Jeden ze znanych głosicieli wolności oprogramowania, Richard Stallman, zrezygnował nawet z zabezpieczenia swojego konta hasłem. W czasach Internetu używanego jako medium handlu elektronicznego zagrożenie związane ze słabościami systemów bezpieczeństwa drastycznie wzrosło. Zastosowanie dodatkowych technologii zabezpieczających nigdy nie rozwiąże jednak kwestii czynnika ludzkiego.

Spójrzmy np. na dzisiejsze porty lotnicze. Są dokładnie zabezpieczone, ale co jakiś czas słyszymy o podróżnych, którym udało się przechytrzyć ochronę i przenieść broń przez bramki kontrolne. Jak to jest możliwe w czasach, kiedy nasze porty lotnicze są praktycznie w ciągłym stanie alertu? Problem zwykle nie leży w urządzeniach zabezpieczających, tylko w ludziach, którzy je obsługują. Władze lotniska mogą wspierać się Gwardią Narodową, instalować detektory metalu i systemy rozpoznawania twarzy, ale zwykle bardziej pomaga szkolenie pracowników ochrony wzmacniające skuteczność kontroli pasażerów.

Ten sam problem ma rząd oraz firmy i instytucje edukacyjne na całym świecie. Mimo wysiłków specjalistów od bezpieczeństwa informacja w każdym miejscu jest narażona na atak socjotechnika, jeżeli nie zostanie wzmocniona największa słabość systemu — czynnik ludzki.

Dzisiaj bardziej niż kiedykolwiek musimy przestać myśleć w sposób życzeniowy i uświadomić sobie, jakie techniki są używane przez tych, którzy próbują zaatakować poufność, integralność i dostępność naszych systemów komputerowych i sieci. Nauczyliśmy się już prowadzić samochody, stosując zasadę ograniczonego zaufania. Najwyższy czas nauczyć się podobnego sposobu obsługi komputerów.

Zagrożenie naruszenia prywatności, danych osobistych lub systemów informacyjnych firmy wydaje się mało realne, dopóki faktycznie coś się nie wydarzy. Aby uniknąć takiego zderzenia z realiami, wszyscy musimy stać się świadomi, przygotowani i czujni. Musimy też intensywnie chronić nasze zasoby informacyjne, dane osobiste, a także, w każdym kraju, krytyczne elementy infrastruktury i jak najszybciej zacząć stosować opisane środki ostrożności.

Oszustwo narzędziem terrorystów

Oczywiście oszustwo nie jest narzędziem używanym wyłącznie przez socjotechników. Opisy aktów terroru stanowią znaczącą część doniesień agencyjnych i przyszło nam zdać sobie sprawę jak nigdy wcześniej, że świat nie jest bezpiecznym miejscem. Cywilizacja to w końcu tylko maska ogłady.

Ataki na Nowy Jork i Waszyngton dokonane we wrześniu 2001 roku wypełniły serca nie tylko Amerykanów, ale wszystkich cywilizowanych ludzi naszego globu, smutkiem i strachem. Cywilizacja to delikatny organizm. Zostaliśmy zaalarmowani faktem, że po całym świecie rozsiani są owładnięci obsesją terroryści, którzy są dobrze wyszkoleni i czekają na możliwość ponownego ataku.

Zintensyfikowane ostatnio wysiłki rządu zwiększyły poziom świadomości dotyczącej spraw bezpieczeństwa. Musimy pozostać w stanie gotowości wobec wszelkich przejawów terroryzmu. Musimy uświadomić sobie, w jaki sposób terroryści tworzą swoje fałszywe tożsamości, wchodzą w rolę studentów lub sąsiadów, wtapiają się w tłum. Maskują swoje prawdziwe zamiary, knując przeciwko nam intrygę, pomagając sobie oszustwami podobnymi do opisanych w tej książce.

Z moich informacji wynika, że dotychczas terroryści nie posunęli się jeszcze do stosowania zasad socjotechniki w celu infiltrowania korporacji, wodociągów, elektrowni i innych istotnych komponentów infrastruktury państwa. W każdej chwili mogą jednak to zrobić — bo jest to po prostu łatwe. Mam nadzieję, że świadomość i polityka bezpieczeństwa zajmą należne im miejsce i zostaną docenione przez kadrę zarządzającą firm po przeczytaniu tej książki. Wkrótce jednak może okazać się, że to za mało.

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, wole 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 nie podejrzewający 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 nie korzystający 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.

10

Na terenie firmy

Dlaczego tak łatwo obcemu podać się za pracownika firmy i udawać go w przekonujący sposób, nabierając nawet ludzi o dużej świadomości tego typu zagrożeń? Dlaczego tak łatwo oszukać człowieka w pełni świadomego procedur bezpieczeństwa, nawet jeśli osoba ta nie ufa ludziom, których nie zna, i dba o ochronę zasobów informacyjnych swojej firmy?

Zastanówmy się nad powyższymi pytaniami, czytając historie zawarte w tym rozdziale.

Strażnik

Czas: wtorek, 17 października, 2:16 w nocy.

Miejsce: Skywatcher Aviation, Inc., zakład produkcyjny firmy na przedmieściach Tucson w stanie Arizona.

Historia strażnika

Leroy Greene czuł się o wiele lepiej, słysząc stukanie swoich obcasów o posadzki opuszczonych hal fabrycznych, niż spędzając długie nocne godziny na wpatrywaniu się w monitory w biurze straży przemysłowej. Nie mógł tam robić niczego poza gapieniem się na ekrany. Nie wolno mu było nawet przeczytać gazety lub zajrzeć do swojej oprawionej w skórę Biblii. Musiał siedzieć i patrzeć na zastygłe obrazy, na których nigdy nic nie chciało się poruszyć.

Chodząc po halach, mógł przynajmniej rozprostować nogi, a jeżeli pamiętał by w chód zaangażować bardziej ręce i ramiona, to miał namiastkę gimnastyki. Choć trudno uważać coś takiego za gimnastykę dla byłego prawego napastnika najlepszej drużyny footbalowej w mieście. No cóż, taka praca.

Gdy doszedł do rogu, zmienił kierunek marszu i poszedł wzdłuż galerii, z której rozciągał się widok na kilkusetmetrowej długości halę produkcyjną. Spojrzał w dół i zauważył dwie osoby przechodzące obok rzędu helikopterów będących w trakcie produkcji. Po chwili postacie zatrzymały się i zaczęły oglądać maszyny. Dość dziwny widok, biorąc pod uwagę, że był środek nocy.

— Lepiej to sprawdzę — pomyślał.

Leroy udał się w kierunku schodów i wszedł do hali w taki sposób, żeby zajść intruzów od tyłu. Nie zauważyli go do momentu, kiedy się odezwał.

— Dzień dobry. Mogę zobaczyć panów identyfikatory? — powiedział. Leroy starał się w takich momentach używać łagodnego tonu. Zdawał sobie sprawę, że jego słuszne rozmiary mogły niejednego wystraszyć.

— Cześć Leroy — powiedział jeden z nich, odczytując imię z identyfikatora. — Tom Stilton z działu marketingu z centrali w Phoenix. Mam tu u was parę spotkań i chciałem przy okazji pokazać mojemu koledze, jak buduje się największe helikoptery na świecie.

— Dobrze. Proszę pokazać identyfikator — rzekł Leroy. Zauważył, że byli bardzo młodzi. Gość od marketingu wyglądał, jakby właśnie skończył liceum, a drugi, z włosami do ramion, na 15 lat.

Pierwszy z nich sięgnął do kieszeni po identyfikator, po czym zaczął nerwowo przeszukiwać wszystkie swoje kieszenie. Leroy zaczynał podejrzewać, że coś tu nie gra.

— Cholera — powiedział. — Musiałem zostawić go w samochodzie. Mogę przynieść, to mi zajmie dziesięć minut. Pójdę na parking i wrócę.

Leroy zdążył już wyjąć swój notes.

— Mogę jeszcze raz prosić pana nazwisko? — zapytał i uważnie zanotował odpowiedź. Następnie poprosił, aby udali się z nim do biura straży przemysłowej. Kiedy jechali windą na trzecie piętro, Tom mówił, że pracuje tu dopiero od sześciu miesięcy i ma nadzieję, że Leroy nie będzie robił mu problemów w związku z tym incydentem.

W biurze ochrony Leroy wraz z kolegami zaczęli zadawać dwójce pytania. Stilton podał swój numer telefonu i powiedział, że jego szefem jest Judy Underwood, po czym podał również jej numer telefonu.

Informacje zgadzały się z danymi w komputerze. Leroy wziął swoich kolegów na stronę, aby naradzić się, co robić w tej sytuacji. Nie chcieli popełnić jakiegoś błędu. Uznali więc, że najlepiej zadzwonić do jego szefowej, nawet gdyby miało to oznaczać zbudzenie jej w środku nocy.

Leroy sam zadzwonił do pani Underwood, wyjaśnił kim jest i zapytał, czy pracuje dla niej pan Stilton.

— Tak — odpowiedziała w półśnie.

— Natknęliśmy się na niego w hali produkcyjnej o 2:30 w nocy bez identyfikatora.

— Proszę mi go dać do telefonu — powiedziała pani Underwood.

Stilton podszedł do telefonu i powiedział:

— Judy, przykro mi, że strażnicy musieli cię obudzić w środku nocy. Mam nadzieję, że nie będziesz mi miała tego za złe.

Chwilę słuchał i kontynuował:

— To przez to, że i tak muszę tu być rano na spotkaniu w związku z nową publikacją prasową. Przy okazji, odebrałaś e-mail na temat Thompsona? Musimy się spotkać z Jimem w poniedziałek, żeby to nie przeszło nam koło nosa. Aha, i jesteśmy umówieni na lunch we wtorek, tak?

Słuchał jeszcze chwilę, po czym pożegnał się i odłożył słuchawkę.

To zaskoczyło Leroya, bo spodziewał się, że odda mu jeszcze słuchawkę, a jego szefowa potwierdzi, że wszystko jest w porządku. Zastanawiał się, czy nie zadzwonić do niej jeszcze raz. Pomyślał jednak, że już raz ją zbudził w środku nocy. Jeżeli zadzwoniłby po raz drugi, mogłaby się zdenerwować i donieść o tym jego szefowi.

— *Nie będę robił zamieszania* — pomyślał.

— Mogę pokazać mojemu koledze resztę linii produkcyjnej? — zapytał Stilton Leroya. — Może pan iść z nami.

— Idźcie, oglądajcie — powiedział Leroy — tylko następnym razem proszę nie zapominać o identyfikatorze. I proszę wcześniej informować ochronę, jeżeli zamierza pan przebywać na terenie zakładu po godzinach — jest taki wymóg.

— Będę o tym pamiętał, Leroy — powiedział Stilton i obaj wyszli.

Nie minęło nawet dziesięć minut, kiedy w biurze ochrony odezwał się telefon. Dzwoniła pani Underwood.

— Co to był za facet?! — dopytywała się. Powiedziała, że próbowała zadawać mu pytania, a on mówił jakieś dziwne rzeczy o lunchu. Nie ma pojęcia, kto to był.

Ochroniarz zadzwonił do strażników w korytarzu i na bramie przy parkingu. Obydwaj widzieli wychodzących kilka minut temu dwóch młodych mężczyzn.

Opowiadając później tę historię, Leroy mówił zawsze na koniec:

— Boże, myślałem że mój szef mnie zabije. Mam szczęście, że mnie nie wyrzucił z pracy.

Historia Joe Harpera

Siedemnastoletni Joe Harper od ponad roku zakradał się do różnych budynków. Czasami w dzień, czasem w nocy — za każdym razem chciał przekonać się, czy ujdzie mu to na sucho. Był synem muzyka i kelnerki — obydwoje pracowali na nocne zmiany, a Joe zbyt dużo czasu spędzał samotnie. Jego opis tych samych wydarzeń pozwala lepiej zrozumieć, co zaszło.

* * *

Mam takiego kumpla, Kenny'ego, który chce być pilotem helikoptera. Zapytał mnie, czy mogę wprowadzić go do fabryki Skywatcher, żeby pooglądać linię produkcyjną helikopterów. Wiedział, że szwendałem się już po różnych budynkach. Zakradanie się do miejsc, gdzie wstęp jest zabroniony, to niezła dawka adrenaliny.

Nie polega to jednak po prostu na wejściu na teren fabryki czy biura. Najpierw trzeba wszystko dokładnie przemyśleć, zaplanować i zrobić pełny rekonesans obiektu. Trzeba wejść na stronę internetową firmy, poszukać nazwisk i stanowisk, struktury podległości i numerów telefonów. Przeczytać wycinki prasowe i artykuły w magazynach. Metodyczne badania to mój własny sposób na bezpieczeństwo — dzięki temu mogę rozmawiać z każdym, podając się za pracownika.

Od czego więc zacząć? Na początku zajrzałem do Internetu, aby sprawdzić, gdzie znajdują się biura firmy. Okazało się, że główna siedziba jest w Phoenix. Doskonale. Zadzwoniłem tam i poprosiłem o połączenie z działem marketingu. Każda firma ma taki dział. Odebrała kobieta, a ja powiedziałem, że dzwonię z firmy Blue Pencil Graphics i chciałem zorientować się, czy są zainteresowani korzystaniem z naszych usług. Zapytałem, z kim mogę na ten temat porozmawiać. Powiedziała, że najlepiej z Tomem Stiltonem. Poprosiłem wiec o jego numer telefonu, na co odpowiedziała, że nie udzielają takich informacji, ale może mnie z nim połączyć. Dodzwoniłem się do jego automatycznej sekretarki. Nagrana wiadomość brzmiała następująco: „Dzień dobry, tu Tom Stilton, dział marketingu, wewnętrzny 3147, proszę zostawić wiadomość". Dobre! Ponoć nie udzielają takich informacji, a tu gość zostawił swój wewnętrzny na sekretarce. Dla mnie bomba — miałem już nazwisko i numer.

Kolejny telefon do tego samego biura.

— Dzień dobry, szukam Toma Stiltona, ale nie ma go u siebie. Chciałbym zapytać o coś jego szefa.

Szefowej też nie było, ale zdążyłem w trakcie rozmowy uzyskać jej nazwisko. Ona również zostawiła swój numer wewnętrzny na sekretarce — bardzo ładnie!

Na pewno udałoby mi się bez specjalnego zachodu przeprowadzić nas obok strażnika w korytarzu, ale kiedyś przejeżdżałem w pobliżu tej fabryki i chyba widziałem tam płot dookoła parkingu. W takim razie na pewno strażnik sprawdza tam, kto wjeżdża na parking. W nocy pewnie spisują dodatkowo numery rejestracyjne, więc będę musiał kupić na pchlim targu jakieś stare tablice.

Najpierw muszę jednak zdobyć numer telefonu do budki strażników. Odczekałem chwilę, aby w sytuacji, gdy odbierze ta sama osoba, mój głos nie wydał jej się znajomy. Po jakimś czasie zadzwoniłem i powiedziałem:

— Ktoś nam zgłaszał, że są problemy z telefonem w budce strażników przy Ridge Road — czy dalej coś się dzieje?

Moja rozmówczyni powiedziała, że nie wie, ale połączy mnie z budką.

Odebrał mężczyzna:

— Brama przy Ridge Road, mówi Ryan.

— Cześć Ryan, tu Ben. Mieliście ostatnio jakieś problemy z telefonem?

Strażnik był chyba przeszkolony, bo zapytał od razu:

— Jaki Ben? Mogę prosić twoje nazwisko?

— Ktoś od was zgłaszał problemy — kontynuowałem tak, jakbym nie słyszał pytania.

Odsunąwszy słuchawkę od ucha, zawołał:

— Hej, Bruce, Roger, były jakieś problemy z telefonem?

Zbliżył z powrotem słuchawkę i powiedział:

— Nie wiemy nic o żadnych problemach.

— Ile macie tam linii telefonicznych?

Zdążył zapomnieć o moim nazwisku.

— Dwie — powiedział.

— A na której teraz rozmawiamy?

— Na 3410.

Bingo!

— I obydwie działają bez problemów?

— Raczej tak.

— Dobrze — powiedziałem. — Tom, jeżeli pojawią się u was jakiekolwiek problemy z telefonami, dzwoń do nas, do Telecom. Jesteśmy od tego, żeby wam pomagać.

Zdecydowaliśmy z Kennym, że odwiedzimy fabrykę jeszcze tej nocy. Późnym popołudniem zadzwoniłem do budki strażniczej, przedstawiając się jako pracownik działu marketingu. Powiedziałem:

— Dzień dobry, tu Tom Stilton z marketingu. Mamy napięty termin i dwóch ludzi jedzie do nas z pomocą. Nie dotrą wcześniej niż o pierwszej, drugiej w nocy. Będzie pan wtedy jeszcze na zmianie?

Odpowiedział radośnie, że kończy o północy.

— Może pan zostawić wiadomość dla swojego zmiennika? — spytałem. — Kiedy pojawi się dwóch ludzi i powiedzą, że przyszli do Toma Stiltona, proszę ich wpuścić, dobrze?

Powiedział, że nie ma sprawy. Zanotował moje nazwisko, wydział i numer wewnętrzny, po czym powiedział, że się tym zajmie.

Podjechaliśmy pod bramę trochę po drugiej. Powiedziałem, że przyjechaliśmy do Toma Stiltona. Zaspany strażnik wskazał tylko drzwi, którymi mamy wejść, i miejsce do zaparkowania.

Po wejściu do budynku natrafiliśmy na kolejną bramkę ochrony w korytarzu i książkę do odnotowywania pobytu po godzinach. Powiedziałem strażnikowi, że muszę na rano opracować raport, a kolega chciał po prostu zobaczyć fabrykę.

— On ma bzika na punkcie helikopterów — powiedziałem. — Chce zostać pilotem.

Strażnik poprosił o mój identyfikator. Sięgnąłem do kieszeni, po czym sięgnąłem do paru innych i powiedziałem, że chyba zostawiłem go w samochodzie i że zaraz po niego pójdę.

— Dziesięć minut — powiedziałem.

— Dobra, nie trzeba. Wystarczy się wpisać — powiedział strażnik.

Spacer wzdłuż linii produkcyjnej był niesamowity. Dopóki nie zatrzymał nas ten olbrzym Leroy.

W biurze straży zdałem sobie sprawę, że intruz wyglądałby w tym momencie na nerwowego i wystraszonego. Kiedy rzecz stanęła na ostrzu noża, udawałem oburzenie. Tak jakbym w rzeczywistości był tym, za kogo się podaję, i wyprowadził mnie z równowagi fakt, że nie chcieli mi uwierzyć.

Kiedy zaczęli mówić o tym, że chyba powinni zadzwonić do mojej szefowej i zaczęli szukać w komputerze jej domowego numeru telefonu, stałem tam i myślałem: „Chyba czas wiać. Ale co z bramą na parkingu — nawet jeżeli uda się nam wydostać z budynku, zamkną bramę i nas złapią".

Kiedy Leroy zadzwonił do kobiety, która była szefową Stiltona, i oddał mi słuchawkę, zaczęła do mnie wrzeszczeć:

— Kto mówi? Kim pan jest?!

A ja po prostu gadałem tak, jakbyśmy prowadzili normalną rozmowę i po jakiejś chwili odłożyłem słuchawkę.

Ile czasu potrzeba, aby w środku nocy zdobyć numer telefonu do fabryki? Szacowałem, że mamy mniej niż kwadrans na to, żeby wydostać się stamtąd, zanim ta kobieta zadzwoni i zaalarmuje strażników.

Wychodziliśmy z fabryki tak szybko, jak się dało, ale żeby nie wyglądało, że bardzo nam się spieszy. Odetchnąłem, kiedy strażnik przy bramie parkingu tylko machnął, żebyśmy przejechali.

Analiza oszustwa

Warto wspomnieć, że bohaterami prawdziwego incydentu, na którym oparta jest ta historia, byli nastoletni młodzieńcy. Dla nich to był wygłup, przygoda — chcieli się przekonać, czy im się uda. Jeżeli dla pary nastolatków wejście na teren firmy okazało się takie proste, to jak proste może być dla złodziei, szpiegów przemysłowych lub terrorystów?

Jak to się stało, że trzech doświadczonych strażników pozwoliło dwóm intruzom po prostu wyjść z fabryki? Tym bardziej, że już ich młody wiek powinien być wysoce podejrzany.

Leroy *miał* z początku słuszne podejrzenia. Dobrze zrobił, zabierając ich do biura straży przemysłowej i sprawdzając chłopaka podającego się za Toma Stiltona oraz numery telefonów i nazwiska, które podał. Z pewnością słuszny był również telefon do jego domniemanego zwierzchnika.

W końcu jednak zwiodła go pewność siebie i oburzenie młodego człowieka. Nie było to zachowanie, którego mógł spodziewać się po złodzieju lub intruzie — tylko pracownik firmy mógł zachowywać się w taki sposób. Tak przynajmniej sądził. Leroy powinien zostać przeszkolony, aby działał, opierając się na solidnych procedurach identyfikacyjnych, a nie na swojej własnej ocenie.

Dlaczego jego podejrzenia nie wrosły, kiedy chłopak odłożył słuchawkę, nie podając jej z powrotem Leroyowi, aby ten usłyszał, jak Judy Underwood potwierdza, że jej pracownik ma powód, by przebywać o tej porze w fabryce?

Było to szyte tak grubymi nićmi, że trudno uwierzyć, iż Leroy dał się nabrać. Spójrzmy jednak na sytuację z jego perspektywy: ukończył

ledwo liceum, zależało mu na pracy, nie był pewny, czy nie narazi się, dzwoniąc drugi raz w środku nocy do osoby na kierowniczym stanowisku. Czy będąc w jego skórze zdecydowalibyśmy się na ponowny telefon?

Oczywiście drugi telefon to nie było jedyne wyjście z sytuacji. Co jeszcze mógł zrobić strażnik?

Jeszcze przed wykonaniem telefonu powinien poprosić obu młodzieńców o jakiś dowód tożsamości ze zdjęciem. Skoro przyjechali do fabryki samochodem, przynajmniej jeden z nich powinien mieć przy sobie prawo jazdy. W tym momencie fakt podania przez nich fałszywych nazwisk stałby się oczywisty (profesjonalista zapewne pojawiłby się z fałszywym dowodem, ale ci chłopcy na pewno o tym nie pomyśleli). W każdym razie Leroy powinien sprawdzić ich informacje identyfikacyjne i zanotować je. Jeżeli obaj oświadczyliby, że nie mają przy sobie żadnych dowodów tożsamości, powinien pójść z nimi do samochodu po identyfikator, który chłopak podający się za Toma Stiltona rzekomo tam zostawił.

Po rozmowie z szefową jeden z ochroniarzy powinien towarzyszyć im do wyjścia, a następnie odprowadzić do samochodu i spisać jego numer rejestracyjny. Jeżeli byłby spostrzegawczy, być może zauważyłby, że jedna z tablic (kupiona na pchlim targu) nie miała ważnej nalepki rejestracyjnej — a to już powód, aby zatrzymać dwójkę w celu dalszego dochodzenia ich tożsamości.

Uwaga Mitnicka ➤

Ludzie posiadający dar manipulowania innymi zwykle cechują się bardzo „magnetycznym typem osobowości". Przeważnie są to osoby rzutkie i elokwentne. Socjotechników wyróżnia też umiejętność rozpraszania procesów myślowych swoich rozmówców, co w efekcie prowadzi do szybkiego nawiązania współpracy z ofiarą ataku. Sądząc, że istnieje chociaż jedna osoba, która nie podda się tego typu manipulacji, nie doceniamy umiejętności i instynktu socjotechników.

Dobry socjotechnik za to nigdy nie pozwala sobie na lekceważenie swego przeciwnika.