ŁAMAŁEM LUDZI, NIE HASŁA

SZTUKA PODSTĘPU

WYDANIE II

KEVIN D. MITNICK

& William L. Simon

Helion

Tytuł oryginału: The Art of Deception: Controlling the Human Element of Security

Tłumaczenie: Jarosław Dobrzański

ISBN: 978-83-283-9248-9

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

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/art2vv
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

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 większości 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.

O czym jest ta książka?

Bezpieczeństwo firmy to kwestia równowagi. Zbyt mało zabezpieczeń pozostawia firmę w zagrożeniu, a zbyt dużo przeszkadza w prowadzeniu działalności, powstrzymując wzrost zysków i pomyślny rozwój przedsiębiorstwa. Zadanie polega na odnalezieniu równowagi między bezpieczeństwem a produktywnością.

Inne książki traktujące o bezpieczeństwie firm koncentrują się na sprzęcie i oprogramowaniu, nie poświęcając należnej uwagi najpoważniejszemu z wszystkich zagrożeń — oszustwu. Celem tej książki jest dla odmiany pomoc w zrozumieniu, w jaki sposób ludzie w firmie mogą zostać zmanipulowani i jakie bariery można wznieść, aby temu zapobiec. Książka ta koncentruje się głównie na pozatechnologicznych metodach, jakie stosują intruzi w celu zdobycia informacji, naruszenia integralności danych, które wydając się bezpiecznymi nie są takimi w istocie, lub wręcz niszczenia efektów pracy firmy.

Moje zadanie jest jednak utrudnione z jednego prostego powodu: każdy czytelnik został zmanipulowany przez największych ekspertów od socjotechniki — swoich rodziców. Znaleźli oni sposoby, aby skłonić nas, byśmy „dla naszego własnego dobra" robili to, co według nich jest najlepsze. Rodzice są w stanie wszystko wytłumaczyć, w taki sam sposób jak socjotechnicy umiejętnie tworzą wiarygodne historie, powody i usprawiedliwienia, aby osiągnąć swoje cele.

W wyniku takich doświadczeń wszyscy staliśmy się podatni na manipulację. Nasze życie stałoby się trudne, gdybyśmy musieli zawsze stać na straży, nie ufać innym, brać pod uwagę możliwość, że ktoś nas wykorzysta. W idealnym świecie można by bezwarunkowo ufać innym i mieć pewność, że ludzie, których spotykamy, będą uczciwi i godni zaufania. Nie żyjemy jednak w takim świecie, dlatego musimy wyćwiczyć nawyk czujności, aby zdemaskować ludzi próbujących nas oszukać.

Większość książki (część druga i trzecia), składa się z historii przedstawiających socjotechników w akcji. Opisano tam tematy takie jak:

- Sprytna metoda uzyskiwania od firmy telekomunikacynej numerów telefonu spoza listy — phreakerzy wpadli na to już dobre parę lat temu.
- Kilka metod, jakich używają napastnicy do przekonania nawet najbardziej podejrzliwych pracowników, aby podali swoje nazwy użytkownika i hasła.
- Kradzież najlepiej strzeżonej informacji o produkcie, w której to kradzieży dopomógł hakerom menedżer z Centrum Operacji.
- Metoda, jaką haker przekonał pewną panią do pobrania programu, który śledzi wszystkie jej poczynania i wysyła mu e-maile z informacjami.
- Uzyskiwanie przez prywatnych detektywów informacji o firmach i osobach prywatnych. Gwarantuję ciarki na grzbiecie podczas czytania.

Po przeczytaniu niektórych opowieści z części drugiej i trzeciej można dojść do wniosku, że to nie mogło się wydarzyć, że nikomu nie udałoby się nic zdziałać za pomocą kłamstw, sztuczek i metod tam opisanych. Historie te są jednak potencjalnie prawdziwe — przedstawiają wydarzenia, które mogą się zdarzyć i zdarzają się. Wiele z nich ma miejsce każdego dnia gdzieś na świecie, być może nawet w Twojej firmie, w chwili, gdy czytasz tę książkę.

Materiał tu przedstawiony może nam również otworzyć oczy, kiedy przyjdzie nam się zetrzeć z umiejętnościami socjotechnika i chronić przed nim nasze osobiste dobra informacyjne.

W części czwartej role zostają odwrócone. Staram się pomóc w stworzeniu nieodzownej polityki bezpieczeństwa i programu szkolenia minimalizującego szansę, że któryś z naszych pracowników padnie ofiarą socjotechnika. Zrozumienie strategii, metod i taktyk socjotechnika pomoże zastosować odpowiednie środki ochrony zasobów informatycznych bez narażania produktywności przedsiębiorstwa.

Krótko mówiąc, napisałem tę książkę, aby zwiększyć świadomość poważnego zagrożenia, jakie reprezentuje sobą socjotechnik, i pomóc w zmniejszeniu szans wykorzystania przez niego firmy lub któregoś z jej pracowników.

A może powinienem powiedzieć — *ponownego* wykorzystania.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

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

„New York Times"

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 hollywoodzkiej wersji. Genialny informatyk czy mistrz manipulacji? Jak naprawdę działał człowiek, wokół 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 swojej 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?

OPINIE CZYTELNIKÓW O KSIĄŻCE SZTUKA PODSTĘPU. ŁAMAŁEM LUDZI, NIE HASŁA
(źródło: www.helion.pl)

_DAMIAN
Książka pokazuje, jak łatwo można oszukać ludzki umysł, jak skrótowo myśli, jak szybko wpada w rutynę i tendencyjne wyciąga wnioski.

_ADAM
Najsłynniejszy haker świata Kevin Mitnick uczy nas, jak bronić samych siebie i nasze firmy przed atakami socjotechników.

_TOMASZ
Jeśli ktoś ma cokolwiek wspólnego z bezpieczeństwem jakiegokolwiek systemu komputerowego, to NIEprzeczytanie tej książki jest grzechem ciężkim!

_GRZEGORZ
Mitnick przedstawia scenariusze ataków hakerskich w postaci wyjątkowo barwnych i wciągających opowieści. *Sztukę podstępu* czyta się jak doskonały kryminał, kryminał z wyjątkowo cennym morałem.

PRZEKONAJ SIĘ, ŻE „ŚCIŚLE TAJNE" TO FIKCJA.
A BEZPIECZEŃSTWO SYSTEMU TO TYLKO TWOJE ZŁUDZENIE...

Książka wzbogacona o wstęp do polskiego wydania.

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

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-9248-9
9 788328 392489

INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 54,90 zł