

Manipulatorzy umysłów czyli inżynieria społeczna w praktyce.

Jeszcze kilka lat temu aby skutecznie włamać się do czyjegoś komputera czy sieci, należało znać na wylot dany system operacyjny, wszystkie jego silne i słabe punkty, dziury w oprogramowaniu itd. Ogólnie hakerzy posługiwali się głównie własną (i nabytą) wiedzą techniczną. Systemy sieciowe były znacznie słabiej zabezpieczone niż dziś, i dlatego prędzej czy później dało się do nich w jakiś sposób dostać. Dziś naprawdę dobrze zabezpieczone systemy są w zasadzie „nie do ruszenia” za pomocą tradycyjnych narzędzi. Na rynku związanym z bezpieczeństwem sieciowym pojawiają się doskonalsze, bardziej złożone i przez to skuteczniejsze systemy zabezpieczeń. Proste metody filtrowania pakietów powszechnie stosowane w większości ruterów są stopniowo wypierane przez filtry z analizą stanu połączenia i zawartości pakietów. Do rosnącej popularności złożonych systemów firewall przyczynia się również spadek cen. Dziś już nie trzeba być wielką korporacją, żeby pozwolić sobie na kupno urządzenia klasy CISCO ASA czy systemu Checkpoint FireWall-1. Wprawdzie nadal nie są to rozwiązania „pod strzechy” no ale z drugiej strony naprawdę istotne dane znajdują się przecież w firmach, a te stać na takie zakupy. Dlatego coraz większe znaczenie w przełamaniu tego typu zabezpieczeń mają techniki niezupełnie związane z klasyczną informatyką. Należy do nich bez wątpienia właśnie inżynieria społeczna. Nie chronią przed nią najlepsze nawet firewalle i najskuteczniejsze algorytmy ochrony. W poniższym artykule postaram się przybliżyć Czytelnikom zagrożenia związane z tą metodą ataków oraz przedstawić sposoby ochrony przed nimi

Definicja inżynierii społecznej

Social engineering, czyli po polsku inżynieria społeczna, to nic innego, jak zdolność do uzyskiwania informacji o kimś lub umiejętność spowodowania, aby określona osoba zrobiła to, czego się od niej oczekuje. Bardzo często inżynieria społeczna wykorzystywana jest do zbierania informacji koniecznych do przeprowadzenia ataku poprzez Internet. Na przykład w pogawędce z kimś z personelu można poznać nazwiska osób mających niezbędne informacje do włamania do sieci lub nazwy aplikacji przechowujących ważne dane. Do technik inżynierii społecznej zalicza się również wynajdywanie sposobów uzyskania dostępu do określonych budynków, pomieszczeń itp.

Jest to, wbrew pozorom, bardzo trudna sztuka manipulowania ludzkim umysłem. Wymaga doskonałej znajomości logiki, psychologii oraz łatwości w nawiązywaniu kontaktu z ludźmi. Korzyści, jakie można uzyskać poprzez umiejętne jej wykorzystanie, są ogromne. W bardzo krótkim czasie można zdobyć dostęp do czyjegoś konta, otrzymać ważne pliki, poznać strukturę sieci, jej słabe punkty, zapoznać się z procedurami panującymi w danej organizacji i zrobić wiele, wiele innych ciekawych rzeczy. Ogólnie rzecz ujmując, zamiast tracić tygodnie czy nawet miesiące na bezskutecznych próbach odgadnięcia hasła czy wyszukania najsłabszego ogniwa w systemie, tą samą wiedzę można osiągnąć w kilka(naście) minut. Pytanie tylko: Jak to zrobić? Metod jest wiele, my powiemy sobie o najpopularniejszych i najskuteczniejszych.

Jestem kimś innym, niż jestem

Najpopularniejszą metodą jest podszywanie się pod inną osobę. Najprostszym sposobem zdobycia informacji jest przekonanie osób na odpowiednich stanowiskach do przekazania ich. Można udawać wysokiego rangą przełożonego lub współpracownika z innego działu firmy. Jeśli przedsiębiorstwo jest duże i ma skomplikowaną strukturę kadrową, a dodatkowo wprowadzimy element zaskoczenia („szybciej, szybciej, potrzebuję tego na wczoraj”), to efekt jest prawie gwarantowany. Inną, bardziej ryzykowną metodą, jest podawanie się za pracownika ochrony czy policjanta w cywilu. Zwłaszcza ten drugi przypadek ewidentnie grozi poważnymi konsekwencjami w przypadku zdemaskowania szczególnie jeśli usiłuje się przy tym posługiwać sfałszowanymi dokumentami. Znacznie wygodniejszym sposobem jest podanie się za serwisanta, który miał coś naprawić, i przyszedł po godzinach pracy. Ochrona zwykle nie zadaje kłopotliwych pytań (zwłaszcza jeśli wcześniej się zadzwoni do niej, podając się np. za dyrektora, i zapowie swoją wizytę). Po dotarciu do firmowych komputerów, przed atakującym otwiera się szereg możliwości. Ludzie, zwłaszcza luźno związani z informatyką, potrafią przechowywać najbardziej poufne dane w najdziwniejszych miejscach. Zaiste zwykle nikt nie wie dlaczego najlepszym miejscem na zapisanie hasła jest karteczka przyklejona do monitora lub ścienny kalendarz. Bardzo często zresztą zamiast hasła wystarczy nacisnąć ENTER.

Oczywiście nie zawsze zdobycie hasła czy innych poufnych danych będzie tak trywialne. Dlatego nieocenionym narzędziem w rękach hakera-psychologa jest telefon. To wręcz zadziwiające, jak bardzo ludzie ufają rozmówcy po drugiej stronie linii, jeśli tylko odpowiednio się przedstawi. Przykład umieszczony obok przedstawia przykładową rozmowę, w efekcie której napastnik uzyskał dane do konta, i zajęło mu to raptem kilka minut. Rozmowa telefoniczna ma tą przewagę nad rozmową twarzą w twarz, że nie wymaga tak dużego opanowania, zwłaszcza mimiki i oczu. Z kolei w stosunku do omówionej dalej wymiany maili ma tą zaletę, że ofiara nie jest w stanie sprawdzić prawdziwości słów napastnika, ponieważ musi na bieżąco reagować na jego słowa.

Niebezpieczne prośby

Oprócz telefonu dobrą metodą pozyskiwania poufnych informacji jest wymiana maili. Spreparowanie odpowiedniego listu elektronicznego, z podaniem jako nadawcy kogoś „ważnego” lub „upoważnionego” jest banalnie proste, za to skuteczne. Jeśli weźmiemy pod uwagę, że powszechnie używany program pocztowy, jakim jest Outlook Express, standardowo nie wyświetla pełnego adresu nadawcy a jedynie imię i nazwisko (które możemy przecież wpisać dowolnie), widać prostą drogę do nadużycia. Metoda ta jest odpowiednia zwłaszcza dla początkujących „manipulatorów” ponieważ nie wymaga błyskawicznych reakcji na działania ofiary i pozwala precyzyjnie przeprowadzić zaplanowane działanie. Z drugiej strony pozostawia potraktowanemu w ten sposób użytkownikowi czas na sprawdzenie, czy mail jest autentyczny. Na szczęście (niestety?) większość osób nie zaprzęta sobie głowy sprawdzaniem prawdziwości takich wiadomości i wręcz machinalnie spełnia zawartą w niej prośbę. Obok umieściłem przykładowy mail, dzięki któremu napastnik uzyskał dostęp do systemu z limitowanym dostępem.

Propozycja nie do odrzucenia

Tam gdzie nie da się prośbą, można spróbować groźbą. Technika ta wymaga silnych nerwów, ale będąc odpowiednio przekonującym, osiągnie się niesamowite efekty. W współczesnych firmach można zaobserwować zaawansowany „wyścig szczurów”, w którym każda niekompetencja może okazać się tą ostatnią. Dlatego właśnie wprowadzając atmosferę zagrożenia („stała się straszna rzecz, ale możemy to jeszcze rozwiązać, oczywiście jeśli będzie pan/pani współpracować”) można łatwo ogłupić ofiarę do tego stopnia, że przez myśl jej nie przejdzie zapytać, o co właściwie chodzi i jakim prawem się od niej czegośkolwiek żąda. Lęk przed utratą pracy jest dominujący. Metoda ta działa najlepiej na osoby o niewielkim doświadczeniu informatycznym, które komputer traktują jak „skrzynkę robiącą dziwne rzeczy”. Jednak zdarzyć się może również, że ofiarą takiej manipulacji padnie ktoś znacznie bardziej doświadczony, ale np. nowozatrudniony w danej firmie, chociażby nawet administrator. Wszystko zależy od inwencji, tupetu i pewności siebie atakującego. Stosowny przykład takiej sytuacji znajduje się w ramce obok.

Na administratora-rozmowa telefoniczna

Rozmowa telefoniczna w firmie X. Rozmawiają Haker (H) i Administrator (A).

- H: Halo, z tej strony Adam Malinowski z firmy Y. Jesteśmy państwa dostawcą internetowym. Czy mam przyjemność z panem Janem Kowalskim ?
- A: Tak, to ja, w czym mogę pomóc ?
- H: Świetnie. Widzi Pan, mamy pewien problem. Zauważyliśmy zwiększoną aktywność robaków internetowych i w związku z tym zainstalowaliśmy w naszym serwerach nowe oprogramowanie antywirusowe. Oczywiście jako stali klienci macie u nas tą usługę za darmo, musimy tylko uzyskać potwierdzenie, że wyrażacie zgodę na korzystanie z niej. Oczywiście maile będą skanowane automatycznie z zachowaniem pełnej poufności. Dzwonię, żeby sprawdzić, czy jesteście Państwo zainteresowani.
- A: Tak, myślę, że tak. Co muszę zrobić?
- H: Z naszej strony w zasadzie wszystko jest gotowe. Muszę tylko sprawdzić, czy jest Pan dysponentem konta. Pozwoli Pan, że przeprowadzę uwierzytelnienie? Niech Pan sprawdzi, czy nikt nie przysłuchuje się naszej rozmowie. Możemy kontynuować ?
- A: Tak, nikogo nie ma, proszę...
- H: Więc Pana login to firma 1234...tak?
- A: Tak, zgadza się...
- H: Dobrze....wszystko czego jeszcze potrzebuję do potwierdzenia to hasło...
- A: Proszę, oto one....

Na VIPa - kradzież informacji

Do sekretariatu filii dużej firmy X. wszedł zdecydowanym krokiem dobrze ubrany mężczyzna w średnim wieku. Już od progu zażądał widzenia się z dyrektorem, który akurat musiał kilka minut wcześniej wyjechać w teren. W sekretariacie była tylko sekretarka. Gość przedstawił się jako wicedyrektor z centrali, machnął wizytówką, rozsiadł się i „poprosił” o kawę. Nerwowo zaczął przebierać palcami, demonstracyjnie patrząc na zegarek. Po upływie kilku minut wstał, stwierdził, że nie ma czasu czekać, i że w tej chwili musi dostać listę zamówień na następny tydzień oraz pełen wykaz klientów firmy, ponieważ w centrali są nieścisłości i on przyjechał wyjaśnić sprawę. Sekretarka zaczęła nerwowo walczyć z drukarką, która nie chciała drukować, ale w tym momencie gość jakby złagodniał i stwierdził, że wystarczy mu plik w wersji elektronicznej. Uszczęśliwiona sekretarka szybko skopiowała zawartość bazy danych na dyskietkę. „Wicedyrektor” podziękował stwierdzając, że będzie pamiętać o jej uczynności, natomiast jej szefowi to jeszcze pokaże. Następnie wyszedł. Po jakimś czasie okazało się, że firma zaczyna tracić klientów, ponieważ konkurencja dotarła do każdego z nich i zaproponowała lepsze warunki.

Nikt nie skojarzył tego z wizytą tajemniczego „wicedyrektora”.

Na litość – koleżeństwo dobra rzecz, ale nie zawsze

W firmie komputerowej pracowało kilkunastu techników. Ich praca polegała między innymi na wdrażaniu klientów końcowych, więc stale kilku z nich było poza firmą. Pewnego dnia przyszedł mail następującej treści:

*„Cześć, tu Janek. Siedzę na jakiejś zakazanej wiosce, gdzie nawet komórki zasięgu nie mają. Piszę z cudzego konta, bo laptop padł, a nie wziąłem zasilacza. Mam prośbę: muszę ściągnąć z serwera skrypt konfiguracyjny, a nie mogę się zalogować, bo mnie firewall nie wpuszcza. Nasze łącze jeszcze nie gotowe, więc łącze się przez Telekomunikację. Zróbcie mi wejście z maską *.elblag.cvx.ppp.tpnet.pl. Aaa... i jeszcze jedno, załóżcie konto janelb z hasłem elbjan, takie tymczasowe, nie chcę na obcym kompie wklepywać naszego stałego hasła. Chcę mieć na nim dostęp do naszego katalogu z konfiguracjami i softem. Jak tylko wrócę to je usunę. Z góry dzięki, trzymajcie się, i przestańcie grać w Quake jak pracujecie ☺”.*

List wydawał się trochę dziwny, ale Janek faktycznie nie odbierał komórki. Zdążyli zapomnieć, że miał uszkodzony aparat (szukał zresztą porady na newsach, ale na razie nie udało mu się naprawić). Nie chcąc utrudniać koledze życia jeden z obecnych w firmie założył konto i zrobił odpowiedni wpis na firewallu. Po kilku dniach okazało się, że oprogramowanie używane do instalacji u klientów zawierało konia trojańskiego, który zbierał i wysyłał gdzieś w sieć poufne dane z komputerów klientów. Sprawa wydała się dopiero **wtedy**, gdy w firmie pojawił się Janek i stwierdził, że ostatnie 5 dni spędził na urlopie, nie wysyłając żadnych maili.

Na zastraszenie – panika nie sprzyja myśleniu

Udając pracownika z działu księgowości tajny konsultant do spraw bezpieczeństwa zwrócił się do administratora systemu z pretensjami, że nie może dostać się do systemu. Wyjaśnił następnie, że musi uruchomić pewne procesy, bo w przeciwnym wypadku nie zostanie wygenerowana lista płac. Oczywiście wina za to, że ludzie nie dostaną pensji, spadnie na administratora, co z pewnością spowoduje, że wyleci on z pracy. Gość zachowywał się wręcz arogancko twierdząc, że on i tak jest już po godzinach i że w sumie to go nie powinno w ogóle obchodzić, bo to przecież nie on za to odpowie. Spanikowany admin przyznał mu znacznie większe uprawnienia niż powinien, byle tylko płace były gotowe na czas. Przez myśl mu nie przeszło sprawdzić, kim naprawdę jest awanturujący się facet. W efekcie faktycznie musiał szukać nowej posady.

Na pochlebstwo – próżność ludzka jest wielka

Haker odwiedził biuro gorliwego kierownika jednego z działów firmy produkującej oprogramowanie narzędziowe. Przekonał go, że jest nowym konsultantem do spraw marketingu, słyszał o jego dokonaniach i że przyszedł sprawdzić pracę działu oraz obejrzeć produkt z punktu widzenia programisty. W ten sposób mógł dokładnie zorientować się, w jaki sposób program jest opracowywany, gdzie przechowywany jest kod źródłowy, które komputery do czego służą. Prawiąc komplementy kierownikowi na temat sprawności działania, udało mu się nawet zdobyć dokładną dokumentację całej sieci.

Rozochocony malującym się w oczach hakera uwielbieniem kierownik opowiedział mu o stosowanych zabezpieczeniach, zwierzył się także ze słabych elementów systemu. W międzyczasie kilkakrotnie logował się na swoje konto, umożliwiając hakerowi podejrzenie hasła. W efekcie w ciągu kilkudziesięciu minut napastnikowi udało się zdobyć dane, które normalnie gromadziłyby przez długie tygodnie skanowania portów, nie wspominając o śladach jakie musiałyby zostawić, oraz wywołanych alarmach. Dodatkowo poznał słabości systemu oraz zdobył hasło osoby o dużych uprawnieniach. A wszystko dlatego, że kierownik lubił być doceniany

5 (pozorowanych i nie tylko) cech dobrego manipulanta

Cierpliwość - nie zawsze już pierwsza rozmowa czy email przyniesie sukces, a wręcz przeciwnie, zbyt duża nachalność wzbudzi podejrzenia. Sieć trzeba zastawiać powoli i w sposób mniej więcej naturalny. Prośba o hasło w pierwszych 3 zdaniach to nie jest dobry pomysł.

Uprzejmość – bądźmy mili dla naszego rozmówcy. Jeśli stosujemy jedną z technik bardziej agresywnych, należy sprawiać wrażenie zatroskanej życzliwości. Ofiara nie powinna się nas od razu bać (oprócz naprawę przemyślanych skrajnych przypadków), a wręcz przeciwnie, powinniśmy sprawiać wrażenie ostatniej deski ratunku godnej ze wszech miar zaufania. Po zdobyciu tego, co chcieliśmy, należy grzecznie, acz nie gwałtownie zakończyć rozmowę - tak, żeby rozmówca miał wrażenie, że jeszcze się spotkamy (co nie jest wcale nieprawdopodobne).

Zrozumienie – istotne zwłaszcza w przypadku, gdy pozorujemy katastrofę. Wykażmy zainteresowanie problemem, który właśnie stworzyliśmy. Starajmy się sprawiać wrażenie żywo zainteresowanego jego rozwiązaniem. W trakcie konwersacji wykorzystujmy wszystkie informacje, jakie posiadamy na temat rozmówcy (skąd je wziąć, o tym za chwilę). Okazujmy współczucie, ale nie od razu chęć pomocy. Usiłujmy

doprowadzić do sytuacji, gdy ofiara sama zapyta, czy przypadkiem nie wiemy jak rozwiązać problem, oczywiście przy jej daleko idącej współpracy.

Koleżeństwo – powołujemy się na dowolny rodzaj solidarności („pracujemy przecież w jednej firmie”, „ja też jestem z X, krajanom trzeba pomagać”, czy chociażby „w końcu obaj jesteście facetami”). To sprawi, że wytworzymy przyjazną atmosferę, jednocześnie usypiając podejrzliwość. Jeśli dodatkowo wspomnimy, że nie ma sensu informować o incydencie nikogo więcej, zyskamy często wdzięczność, a jednocześnie zapewnimy sobie bezpieczeństwo.

Pewność siebie – rozpoczynając grę nie można się z niej wycofać. Dlatego należy rozmawiać płynnie, bez zacięć i wahań. Musimy sprawiać wrażenie człowieka, który wie czego chce i któremu się to należy. Jeśli nie będziemy umieli zapanować nad mimiką, to nawet nie próbujemy metod polegających na kontakcie bezpośrednim. Jeśli nie jesteśmy w stanie szybko reagować na zmiany sytuacji, to zdecydowanie odpuścimy sobie rozmowę telefoniczną na rzecz kontaktu mailowego lub za pomocą komunikatora.

5 miejsc zawierających informacje przydatne do ataku

Katalog zatrudnionych, firmowa WWW – kopalnia wiedzy o strukturze organizacji, baza numerów telefonicznych, adresów email i numerów pokojów. Większość z nich jest dostępną na firmowych stronach WWW także żeby je zdobyć, nie trzeba nawet pojawiać się w siedzibie firmy. Ustawa o ochronie danych osobowych trochę ograniczyła możliwość publikacji danych osobowych, ale nie wszystkie firmy się do niej stosują.

System telefoniczny firmy – niektóre systemy z centralkami wewnętrznymi umożliwiają wybieranie według nazw i zawierają listę stanowisk i nazwisk, co udostępnia atakującemu dane, których mógł nie znaleźć w serwisie WWW.

Tablica informacyjna – umieszczona w większości dużych firm zawiera większość danych potrzebnych do zidentyfikowania danego pracownika.

Archiwa list dyskusyjnych, grupy usenetowe – wiedząc kogo szukamy, możemy łatwo zapoznać się z poglądami danej osoby, zainteresowaniami, poznać jej styl pisanie itd. Informacje bardzo przydatne w późniejszym podszywaniu się lub wykorzystywaniu „słabości charakteru”.

Strony domowe – część firm, zwłaszcza uczelniane, umożliwiają swoim pracownikom prowadzenie własnych stron domowych w firmowej/uczelnianej domenie. Z takiej strony można dowiedzieć się wszystkiego o zainteresowaniach delikwenta, często poznać jego życiorys, przebieg kariery zawodowej, rodzinę itp. Zwykle dowiemy się jak wygląda, czym jeździ, gdzie mieszka (z umieszczonych zdjęć).

5 sposobów, jak nie dać się zmanipulować

Bądź czujny – większość z nas jest z natury ufna. A przecież stare przysłowie mówi, że „ludziom trzeba wierzyć ale nie wolno im ufać”. Haker chcący przeprowadzić jeden z opisanych ataków na pewno nie wybierze człowieka energicznego i dociekliwego. Jeśli otrzymamy dziwną wiadomość email, sprawdźmy dokładnie w jej właściwościach kto naprawdę ją wysłał i skąd.

Czasami warto być służbiwą – jeśli ktoś twierdzi, że czegoś potrzebuje, to jeszcze nie świadczy o tym, że powinien to dostać. Każdą dziwną prośbę należy sprawdzić. Zadawajmy mnóstwo pytań, starając się dowiedzieć po co danej osobie są potrzebne akurat te informacje. Proponujmy inne rozwiązania przedstawionego problemu. Starajmy się postępować zgodnie z regulaminem, zwłaszcza w przypadku danych poufnych i tajnych. Wszelkie próby zastosowania „drogi na skróty” w takim przypadku są z miejsca podejrzane.

Sprawdź z kim rozmawiasz – dopóki nie jesteśmy pewni na 100%, kim jest nasz rozmówca, należy uważać co mówimy i robimy. Jeśli niezwykła prośba przychodzi za pośrednictwem poczty elektronicznej, poprośmy o potwierdzenie telefoniczne. W trakcie rozmowy telefonicznej zażądajmy podania numeru i wykonajmy telefon zwrotny, sprawdzając do kogo należy podany numer. Pytajmy o numer pracownika, identyfikator, stanowisko, nazwisko przełożonego, u którego można potwierdzić tożsamość rozmówcy. Pamiętajmy, że haker, który „odrobił pracę domową” będzie posiadał większość informacji o strukturze firmy, możliwe też że uda mu się za pomocą wcześniej wspomnianego podszywania się uzyskać dostęp do firmowego telefonu. Czasami więc

dopiero weryfikacja u przełożonego, co do którego mamy pewność że jest tym za kogo się podaje, może rozwiązać wątpliwości.

Naucz się mówić „nie” – w przypadku, gdy coś wydaje się wyjątkowo podejrzane, zaufaj instynktowi. Haker wykorzystujący taktykę inżynierii społecznej zwykle narusza przyjęte w firmie procedury. Żądajmy potwierdzenia na piśmie, zezwoleń, upoważnień. Postępujmy zgodnie z procedurami. W przypadku niedostarczenia takich potwierdzeń, odmawiajmy.

Szkolenie uświadamia – jako administrator systemu, zadbajmy, żeby nasi użytkownicy przeszli szkolenie z zakresu inżynierii społecznej. Nic tak skutecznie nie eliminuje zagrożeń, jak ich znajomości i świadomość ich istnienia.

Podsumowując...

Powyższe rozważania mają charakter czysto akademicki i w zamierzeniu autora nie powinny służyć propagowaniu stosowania technik inżynierii społecznej do przenikania do systemów. Każdy kto chciałby spróbować swoich sił w tym procederze, powinien być świadomy ryzyka, jakie wiąże się z jego zdemaskowaniem, co może skończyć się sprawą w sądzie. Administratorzy natomiast mogą sprawdzić za pomocą opisanych „sztuczek” świadomość swoich użytkowników, żeby wiedzieć, jak podatni na takie techniki są pracownicy i jakie to może nieść zagrożenie dla administrowanego systemu. Każdemu, kto chciałby szerzej zapoznać się z inżynierią społeczną, mogę polecić książkę panów Briana Hacha, Jamesa Lee i Geoga Kurtza „Hakerzy w Linuxie”. Drugą ciekawą pozycją pomagającą tropić takie przypadki ataku jest książka Edwarda Amaroso „Sieci: Wykrywanie intruzów”. Zupełną klasyką gatunku jest natomiast „Książę” Niccolo Machiavellego. Ciekawe adresy WWW dotyczące *social engineeringu* znajdziemy pod adresem <http://www.hackinglinux.com>. Warto zauważyć, że nie istnieje i raczej nieprędko powstanie techniczna metoda ochrony przed atakami bazującymi na inżynierii społecznej, dlatego tak ważna jest, oprócz skutecznego firewalla, spójna polityka bezpieczeństwa w firmie. Pewnym rozwiązaniem może być np. automatyczne skanowanie wiadomości pocztowych pod kątem zadanych wyrazów (np. „hasło”, „użytkownik”, „kod”) ale po pierwsze narusza to w pewien sposób poufność korespondencji, a po drugie jest to półśrodek wymagający przy tym dużej mocy obliczeniowych. Włamanie przy użyciu technik inżynierii społecznej trudno wykryć, chociażby ze względu na brak śladów „próbkiwania” systemu. Napastnik dostaje się do niego w najzupełniej legalny sposób, przy użyciu konta istniejącego użytkownika. Dlatego, jak już wcześniej wspomniałem, najskuteczniejszą metodą walki jest stałe uświadamianie użytkowników o istniejącym zagrożeniu i wprowadzenie skutecznych procedur w przypadku wykrytych prób wyłudzenia informacji.

Michał Zimmicki