Wprowadzenie do technik inżynierii społecznej

„Nigdy nie jesteśmy oszukiwani; oszukujemy samych siebie. "" - Johann Wolfgang von Goethe

Ta część zawiera wprowadzenie do inżynierii społecznej. Ponieważ jest to ogromny temat, nie mogę zacząć przedstawiać więcej niż przegląd. Inżynieria społeczna (zwana również hakowaniem „oprogramowania typu wetware" lub bardziej otwarcie, jak kłamstwo i oszustwo) oznacza uzyskiwanie poufnych lub uprzywilejowanych informacji poprzez manipulowanie legalnymi źródłami lub posiadaczami tych informacji. Zwykle dotyczy to informacji kontroli dostępu, takie jak hasła lub informacje o pracownikach, majątku firmy itp. Mówiąc dalej, inżynieria społeczna może być wykorzystana do skłonienia ludzi do robienia rzeczy, które zagrażają bezpieczeństwu jako całości, takich jak fizyczny dostęp do zasobów lub pomieszczeń, których nie powinieneś mieć. To zawsze wymaga pewnego stopnia oszustwa. Dlatego wiele technik omówionych wcześniej przez wielu byłoby uważanych za inżynierię społeczną. Wiele książek szczegółowo omawia inżynierię społeczną. Jednak chociaż część ta zawiera podejścia przydatne w kontaktach osobistych, są one tak samo odpowiednie przez telefon lub Internet; w rzeczywistości inżynieria społeczna jest znacznie łatwiejsza (i bezpieczniejsza), gdy jest wykonywana w ten sposób. Zapamiętaj następującą frazę: Identyfikacja bez weryfikacji.

Uwzględnienie etyki inżynierii społecznej

Komputery nie dbają o to, czy są wykorzystywane, ludzie (ogólnie) tak robią. Inżynieria społeczna jest, w bardzo realnym sensie, nadużyciem, przynajmniej dlatego, że polega na celowym oszukiwaniu docelowego personelu na polecenie pracodawcy, ale także dlatego, że techniki socjotechniczne są zaprojektowane tak, aby osiągnąć cele poprzez manipulowanie szerokim zakresem emocje, nie wszystkie przyjemne. Chociaż niektóre techniki opisane tutaj mogą być niezwykle skuteczne, to od ciebie zależy, czy są odpowiednie w określonych warunkach. Przeprowadzanie testów, które koncentrują się na spowodowaniu, że dana osoba jest słabym ogniwem w zabezpieczeniach korporacyjnych, spowoduje złe postrzeganie (i utratę zaufania) zarządzania. Ostatecznie wpływ tego może być co najmniej tak samo negatywny jak naruszenie bezpieczeństwa. Co ważniejsze, ataki socjotechniczne mogą wyrządzić szkodę psychiczną osobie, która została oszukana. To nie jest gra i nie jest to zachowanie, w które należy się lekko angażować. Zawsze oceniaj, jak ważne jest korzystanie z poszczególnych pracowników i nigdy nie używaj go więcej niż to konieczne. Na rynku dostępnych jest kilka książek, w których głównym tematem jest inżynieria społeczna; jednak większość zawiera mnóstwo nieistotnych lub bezużytecznych informacji na takie tematy, jak programowanie neurolingwistyczne i fragmenty tekstów z podręczników psychologii uczelni. Jest to przede wszystkim praktyczny tekst, więc nie będę cię nudzić ani marnować czasu na informacje, które nie mają zastosowania. Przykładowe scenariusze i analizy są bezpośrednio związane z testami penetracji fizycznej: uzyskiwanie poufnych lub uprzywilejowanych danych poprzez manipulowanie zaufaniem, ignorancją i kierunkiem emocjonalnym. Dzięki inżynierii społecznej możliwe jest zhakowanie sieci korporacyjnej bez dotykania klawiatury. Jeden z najbardziej znanych inżynierów społecznych, Kevin Mitnick, osiągnął tak wielki sukces, że zaczęły krążyć wokół niego legendy, które tylko sporadycznie kolidowały z faktami - moim ulubionym jest to, że mógł wystrzelić pociski nuklearne, gwiżdżąc dźwięki w telefonie publicznym. Klasyczne rzeczy.

Czy tego naprawdę potrzebujesz?

Przed przeprowadzeniem inżynierii społecznej w ramach testów należy wziąć pod uwagę pewne kwestie. Po pierwsze, czy wykazanie podatności na zagrożenia za pomocą inżynierii społecznej będzie miało jakąś istotną wartość? Pozwól, że wyjaśnię: kiedy przeprowadzasz testy penetracyjne w stosunku do komputerów, sieci lub aplikacji, zastosowane techniki i uzyskane wyniki są mierzalne; ustalenia są

konkretne, a zalecenia jasne. Jeśli test zostanie przeprowadzony dobrze, wyniki są powtarzalne, a za sześć miesięcy raport z powtórki można porównać z oryginałem i wyciągnąć wnioski na temat poprawy ogólnej pozycji bezpieczeństwa. Kiedy „hackujesz ludzi", rzeczy nie są wcale tak wyraźne, jak i wnioski. Jeśli obowiązują już zasady bezpieczeństwa, które instruują personel, aby nie przekazywał uprzywilejowanych informacji nieznajomym (za kogokolwiek się podają), a personel jest przeszkolony w zakresie podstawowych zagrożeń bezpieczeństwa, niewiele więcej możesz zrobić (oprócz personelu dyscyplinującego, który niczego nie rozwiązuje). Pomyśl o tym w kategoriach analogii sieci. W pewnym momencie komputer można uznać za bezpieczny (lub przynajmniej tak bezpieczny, jak to możliwe, aby go uruchomić bez wyłączania go i zakopywania). Tego samego nie można powiedzieć o ludziach. Po pomyślnym teście inżynierii społecznej można podjąć dowolną liczbę kroków naprawczych, ale za sześć miesięcy wyniki będą prawdopodobnie takie same. Ponieważ wynik będzie zły dla celu, czy naprawdę ma sens testowanie? Dobrze . . ., tak. Świadomość, że jesteś narażony, jest pierwszym krokiem do lepszego podejścia do bezpieczeństwa.

Wprowadzenie do psychologii partyzanckiej

Ta sekcja analizuje różne aspekty ludzkiej psychiki, które można wykorzystać w celu uzyskania informacji oraz przewidywania i kontrolowania zachowań. Różni ludzie reagują na różne bodźce zgodnie z makijażem swoich postaci. Jednak osoby o podobnych postaciach często znajdują się w podobnych rolach. W ten sposób możliwe jest przewidywanie z pewnym stopniem dokładności, które techniki będą skuteczne, biorąc pod uwagę wystarczającą wiedzę o docelowej osobie. Podstawowa znajomość następujących pojęć i wektorów zagrożeń jest kluczowa dla osiągnięcia prawdziwego sukcesu w inżynierii społecznej, a także dla szansy na ochronę się przed nią. Inżynierowie społeczni bawią się stanami umysłu, aby uzyskać to, czego chcą. W tej sekcji omówię wykorzystanie następujących elementów:

• zaufanie;

• ignorancja;

• łatwowierność;

• chciwość;

• chęć pomocy;

• chęć bycia lubianym.

Wykorzystanie zaufania

Wykorzystywanie zaufania jest podstawą ataków socjotechnicznych. Ludzie ufają innym. W miejscu pracy większość ludzi ufa swoim kolegom (przynajmniej w kontekście środowiska pracy). My, ludzie z naszej natury, ufamy w naszym własnym klanie lub kręgach, a tym bardziej poza nimi. Ale najczęściej mylimy się po stronie zaufania, chyba że mamy konkretny powód, aby tego nie robić. Na przykład, jeśli ktoś zadzwoni do firmy marketingowej z prośbą o wzięcie udziału w ankiecie, twoją pierwszą skłonnością nie jest „Arrgghh, inżynier społeczny, który ograbił moje tajemnice korporacyjne!", ale „Och nie, inny marketer, który chce zmarnować mój czasu. "Jednak wiele osób regularnie bierze udział w ankietach przez telefon i jest przygotowanych do udzielania wielu informacji o sobie często bez żadnej formy nagrody (rzeczywistej lub postrzeganej). Oferta nagrody (nawet jeśli jest to coś bardzo fałszywego, jak udział w losowaniu nagród) dramatycznie zwiększa szanse na aktywny udział. Ankieta, jeśli rzekomo jest prowadzona w imieniu dużego gracza, takiego jak Microsoft, jest łatwym sposobem na uzyskanie podstawowych informacji o infrastrukturze. Wrzuć bezpłatną kopię systemu Windows 7

i wszystko gotowe. Zdziwcie się, w jakim stopniu ludzie wezmą was za słowo. Dobrym sposobem na ustanowienie zaufania jest rezygnacja z nazwy. Ta technika jest znana jako „wiedza domyślna" i służy do wykazania, choćby na poziomie podświadomości, że jesteś uprawniony i sugeruje, że jesteś osobą wewnętrzną. Jeśli dasz ludziom trochę wiedzy, założą się, że masz dużo. Jest to główna zasada techniki zwanej pretekstem. Pretexting to czynność polegająca na uzyskiwaniu określonych informacji od celu w celu użycia go w innym miejscu ataku. W Stanach Zjednoczonych często używa się numeru ubezpieczenia społecznego (SSN) jako telefonicznej weryfikacji bezpieczeństwa w celu ustalenia czyjejś tożsamości. Jest to niebezpieczne i głupie, ponieważ SSN jest w najlepszym razie tylko częściowo tajny. Wspólnym celem przestępców biorących udział w wielu różnych oszustwach jest uzyskanie SSN dla ataków kradzieży tożsamości. Powszechną techniką uzyskiwania SSN jest nazywanie celu maskaradując się jako bank lub usługa, z której korzystają (lub która mogła być używana w pewnym momencie w przeszłości). Dzwoniący oświadcza, że ma do przekazania jakieś pilne informacje, ale najpierw musi legalnie ustalić tożsamość, weryfikując numer ubezpieczenia społecznego. (W tych okolicznościach większość ludzi ujawni te informacje, aby zapobiec kradzieży tożsamości!) Brzmi prosto i podobnie jak wszystkie najlepsze ataki. Cel zwykle przekazuje te informacje bez zastanowienia, a atakujący może z nich korzystać na wiele różnych sposobów. Działa to w przypadku każdej części tajnych informacji powszechnie używanych do potwierdzania tożsamości przez telefon. To szokujące, jak wiele osób polega na jeszcze mniej poufnych (i łatwiejszych do ustalenia) informacjach, takich jak nazwisko panieńskie ich matki. Czy możesz coś jeszcze wymyślić? Reasumując, większość ludzi ogólnie ufa, dopóki nie ma powodu, aby nie być, na przykład z powodu złych doświadczeń w przeszłości, zakorzenionej paranoi lub po prostu mając wystarczająco dużo czasu, aby dać sytuację wystarczająca myśl. Dobry inżynier społeczny zakończy rozmowę na długo, zanim jakiekolwiek naturalne wątpliwości zaczną wkradać się do umysłów swoich celów. Inną kwestią, o której należy pamiętać, jest to, że zaufanie (lub zaufanie do posłuszeństwa) wzrasta wraz z zauważalnym zmniejszeniem odpowiedzialności lub odroczeniem odpowiedzialności wobec władzy. Jest to typowe podejście w środowisku korporacyjnym; jeśli to nie jest twoja szyja na linii, zazwyczaj mniej uważasz na konsekwencje popełnienia błędu. Dobry inżynier społeczny pielęgnuje takie uczucia, łagodząc wszelkie obawy poprzez upuszczenie imienia (praktyka niedbałego wymieniania ważnych osób, aby wywrzeć wrażenie na ofierze). Więcej na ten temat później.

Wykorzystywanie ignorancji

Niewiedza nie jest w żadnym wypadku tym samym, co brak inteligencji. Ofiary ataku socjotechnicznego nie są głupie. Kiedy mówię o niewiedzy, mam na myśli to, że ludzie rozpoznają obszary, w których mają wiedzę i te, w których nie mają. Ludzie mają naturalną tendencję do podporządkowywania się autorytetem innych w sytuacjach, w których czują się mniej niż kompetentni. W tym przypadku używamy definicji „autorytetu" Kropotkina, co oznacza autorytet techniczny, a nie kogoś, kto ma władzę. Systemy informatyczne to obszar, w którym większość ludzi odczuwa ignorancję w większym lub mniejszym stopniu, szczególnie gdy rozmawia z kimś, kto ma lub jest postrzegany jako posiadający większą wiedzę niż oni. Wykorzystywanie ludzkiej niewiedzy w zakresie systemów informatycznych jest potężnym narzędziem inżynierii społecznej, gdy towarzyszy temu fakt, że ludzie nie lubią czuć się ignorantami. Ta postawa „Oczywiście wiem, co robię, po prostu powiedz mi, co mam robić!" To subtelna manipulacja ludzką dumą i ignorancją, która zawsze jest niebezpieczną kombinacją. Nowoczesne stacjonarne stacje robocze są bardzo łatwe w obsłudze i faktycznie większość ludzi jest zmuszona do korzystania z nich w środowiskach biznesowych, ale używanie czegoś i wiedza, jak to działa, to dwie zupełnie różne rzeczy. Przekazanie ofierze instrukcji technicznych jest bardzo łatwe, ale nie oznacza to, że rozumieją konsekwencje tego, co robią. Na przykład dodanie użytkownika do stacji roboczej jest poleceniem jednowierszowym w systemie Windows, a instalacja nieuczciwego lub

wrogiego oprogramowania to tylko kilka kliknięć. Każdy w organizacji docelowej jest ignorantem w kilku obszarach, więc ostrożnie wybierz punkt ataku i obszar dźwigni.

Wykorzystywanie umysłu grupy

To naprawdę niezwykłe, w co ludzie są gotowi uwierzyć, jeśli ich rówieśnicy najpierw kupią ten pomysł. Niektóre zjawiska (na przykład reality TV) można wyjaśnić tylko w ten sposób.

W mojej pierwszej pracy, świeżo po studiach, mały sprzedawca o wartości dodanej, dla którego pracowałem, wpadł w gorącą wodę, gdy jeden z naszych klientów złożył oficjalną skargę dotyczącą zdrowia i bezpieczeństwa w odniesieniu do niektórych monitorów typu greenscreen, które im sprzedaliśmy. Oczywiście był to powód do niepokoju ze strony kierownictwa, przynajmniej do czasu wyjaśnienia charakteru skargi. Wygląda na to, że monitory były używane przez lokalną grupę sekretarek. Jedna z pracujących tam dziewcząt zwróciła uwagę współpracowników, że od czasu używania tych nowych monitorów zwiększyła o dwa rozmiary stanika. Jedna z jej koleżanek powiedziała, że to samo przytrafiło się jej i wkrótce ta klątwa rozprzestrzeniła się po całym biurze. Dyskusja dotarła do ich bezpośredniego przełożonego, który eskalował ją do działu HR, stąd skarga. Kiedy przedstawiciel władz lokalnych zadzwonił do mojego szefa w celu omówienia sprawy, jego odpowiedź (bardzo zgodna z jego charakterem) brzmiała: „Nie, nie jestem dostępny ze względu na przeprowadzkę na Karaiby dzięki wszystkim pieniądzom, które zarobiłem na sprzedaży urządzeń do powiększania piers". Skutek tej uwagi był taki, że wszyscy zdali sobie sprawę, jak wielkim głupstwem była ta skarga. Jednak istnienie agencji rządowej przygotowanej do wszczęcia postępowania sądowego przeciwko dostawcy wyłącznie na podstawie rozmowy niektórych administratorów o swoich stanikach pokazuje, że nikt z nas nie jest tak głupi jak my wszyscy. Jeśli możesz sprawić, że ktoś pomyśli, że dana koncepcja już istnieje postrzegane jako fakt przez inną osobę, której ufają, wtedy będzie to gotowe do zaakceptowania.

Wykorzystanie łatwowierności

Poziom łatwowierności osoby polega na tym, jak predysponowana jest ona do wierzenia w coś bez dowodów potwierdzających jego prawdę lub istnienie. Jednak wszyscy ludzie wierzą w rzeczy, których nie mają możliwości zweryfikować. Na przykład akceptuję, że Ziemia krąży wokół Słońca, a nie na odwrót, ponieważ akceptuję autorytet ludzi, którzy mi to mówią. Kilkaset lat temu ludzie wierzyli dokładnie odwrotnie z tego samego powodu. W pewnym sensie prawdę naukową można uznać za absolutną, ale gdy natura tej prawdy nie ma żadnego wpływu na codzienne życie, szybko staje się subiektywna, a subiektywna prawda jest znacznie bardziej podatna na manipulacje: ludzie kiedyś wierzyli że słońce zostało zepchnięte na niebo przez gigantycznego chrząszcza gnojowego i wydawało się, że dla wszystkich będzie to w porządku.

Czy to jednak naprawdę łatwowierność? Czy chrześcijanin czy muzułmanin jest naiwny wierząc w najwyższą istotę? Hmm, jest to pytanie nieco wykraczające poza nasz zakres i to, czy wiara stanowi jakąś formę naiwności grupowego umysłu, pozostawię filozofom. Dla naszych celów łatwowierność można oceniać w skali z głębokim podejrzeniem banalnej lub przyziemnej („sceptycznej" osobowości) na jednym końcu i nadmierną akceptacją niezwykłości lub osobowości („quixotic" osobowości) na inny. Większość ludzi jest oczywiście gdzieś pośrodku, ale można je przesuwać tam i z powrotem wzdłuż skali, w zależności od zewnętrznych bodźców lub zachęt. Najwyraźniej łatwowierna osoba jest najbardziej użyteczna dla inżyniera społecznego. Ciekawym sposobem na zwiększenie łatwowierności osoby jest wykorzystanie jej chciwości. Chciwość i łatwowierność idą w parze, a ludzie wydają się gotowi wierzyć w niektóre, naprawdę absurdalne kłamstwa, jeśli popchniesz ich chciwość do granic możliwości. Rozważ ten klejnot z mojej skrzynki odbiorczej.

Z mojej skrzynki odbiorczej

Przedmiot: Astronauta z Nigerii chce wrócić do domu

Dr Bakare Tunde

Kierownik projektu Astronautics

National Space Research and Development Agency (NASRDA)

Działka 555

Misau Street

PMB 437

Garki, Abudża, FCT NIGERIA

Szanowny Panie,

WNIOSEK O WYSOKĄ POUFNOŚĆ POMOCY

Jestem dr Bakare Tunde, kuzyn nigeryjskiego astronauty z lotnictwa, major Abacha Tunde. Był pierwszym Afrykaninem w kosmosie, kiedy to zrobił sekretny lot do stacji kosmicznej Salyut 6 w 1979 r. Był na pokładzie później radziecki statek kosmiczny Sojuz T-16Z do tajnej radzieckiej wojskowej stacji kosmicznej Salyut 8T w 1989 r. Został tam osierocony w 1990 r., kiedy Związek Radziecki został rozwiązany. Jego inni sowieccy członkowie załogi wrócili na ziemię Sojuzem T-16Z, ale jego miejsce zajął ładunek powrotny. Od czasu do czasu odbywały się loty zaopatrzeniowe Progreza. Ma dobry humor, ale chce wrócić do domu. W ciągu 14 lat, odkąd był na stacji, zgromadził wynagrodzenie za przelot i odsetki w wysokości prawie 15 000 000 dolarów amerykańskich. Odbywa się to w ramach trustu w Lagos National Savings and Trust Association. Jeśli uda nam się uzyskać dostęp do tych pieniędzy, możemy wpłacić zaliczkę u rosyjskich władz kosmicznych za lot powrotny w Sojuz, aby przywieźć go z powrotem na Ziemię. Powiedziano mi, że będzie to kosztować 3 000 000 dolarów amerykańskich. Aby uzyskać dostęp do jego funduszu powierniczego, potrzebujemy twojej pomocy. W związku z tym moi koledzy i ja jesteśmy gotowi przelać całkowitą kwotę na twoje konto lub późniejszą wypłatę, ponieważ my, jako urzędnicy służby cywilnej, Kodeks Postępowania (przepisy o służbie cywilnej) zabrania nam otwierania i / lub prowadzenia zagranicznych rachunków w naszych imieniu. Nie trzeba dodawać, że zaufanie, którym obdarzyli cię w tym momencie, jest ogromne. W zamian uzgodniliśmy, że zaoferujemy ci 20 procent przeniesionej kwoty, podczas gdy 10 procent zostanie przeznaczone na dodatkowe koszty (wewnętrzne i zewnętrzne) między stronami w trakcie transakcji. Będziesz zobowiązany do przekazania salda w 70% na inne konta w odpowiednim czasie. Uprzejmie przyspiesz działanie, ponieważ jesteśmy opóźnieni, aby umożliwić nam włączenie zaliczka w tym kwartale finansowym. Proszę potwierdzić otrzymanie tej wiadomości wyłącznie za pośrednictwem mojego bezpośredniego numeru 234 (0) 9-234-2220.

Z poważaniem, dr Bakare Tunde

Astronautics Project Manager tip@nasrda.gov.ng

http://www.nasrda.gov.ng/

Jest to skrajny przykład oszustwa dotyczącego zaliczki w Nigerii 419. Mimo że naprawdę trzeba było na to wpaść, wiele osób zostało pochłoniętych przez oszustwa, o wiele bardziej wiarygodne niż to. Nie

wiem, czy naprawdę jest dr Bakare Tunde pracujący dla nigeryjskiego programu kosmicznego (czy istnieje coś takiego jak nigeryjski program kosmiczny jest wystarczająco niepokojące), ale zgaduję, że podany numer telefonu nie będzie połączyć cię z nim. Nie ma nic nowego w 419 oszustwach, mimo że cieszy się dużym zainteresowaniem prasy, ludzie wciąż zakochują się w tym nonsensie. Co ciekawe, kraje pochodzenia pozostają takie same: Nigeria, Sierra Leone lub gdzieś indziej w Afryce Zachodniej. Oszuści najwyraźniej odnoszą wystarczające sukcesy dzięki takiemu podejściu, że nie odczuwają potrzeby zbytniej zmiany parametrów swojego ataku. 419 oszustw działa, ponieważ ludzie chcą wierzyć, że szklany kamień to naprawdę diament, że na końcu tęczy jest złoto i że mogą się wzbogacić przy niewielkim postrzeganym ryzyku. (Wiele osób prawdopodobnie wierzy, że mogą same dokonać oszustwa ze względu na zaufanie, jakie zostanie im powierzone przy przekazywaniu środków - zawsze jest to oznaka dobrego oszustwa). Nigdy nie lekceważ potęgi wiary.

Wykorzystywanie chciwości

Wykorzystanie chciwości jest potężnym wektorem ataku. Nawet ludzie, którzy nie uważają się za chciwych, są podatni na tę formę manipulacji, ale chęć pragnienia czegoś więcej niż ty jest podstawową motywacją człowieka. Wykorzystanie chciwości w praktycznym (zainscenizowanym) ćwiczeniu inżynierii społecznej polega na tym, aby wiedzieć, czego ludzie chcą, czego potrzebują (lub myślą, że potrzebują) i zapewnić to, choć nie do końca tak, jak się spodziewają. Stanowi to podstawę jednego z najbardziej niszczycielskich ataków, jaki może mieć koń trojański. Jeśli pamiętacie, Odyseusz i jego towarzysze Grecy ukryli się w wielkim drewnianym koniu, który trojanie niemądrze holowali w obrębie murów miejskich (uważając, że jest to prezent od pokonanego wroga). W nocy Grecy wymknęli się, wpuścili resztę armii, a reszta to historia (lub przynajmniej cholernie dobre opowiadanie historii). Jeśli chodzi o współczesne bezpieczeństwo, koń trojański robi dokładnie to samo: jest czymś, co wydaje się być prezentem lub zrobić coś pożytecznego (takiego jak darmowe oprogramowanie), ale kradnie same klucze do twojego bezpieczeństwa. Przykłady ataków koni trojańskich obejmują:

• Wiele firm rozdaje markowe gratisy, takie jak napędy USB, długopisy, gadżety itp. Włączanie sprzętu powodującego błędy w takich urządzeniach jest banalne. Możesz dowiedzieć się, z którymi firmami współpracuje firma, i wykorzystać ich branding w takich atakach. Pracownik mojego klienta był zachwycony, gdy otrzymała od współpracownika drogą lampę biurową; niestety zawierał także miniaturową kamerę bezprzewodową.

• Oprogramowanie podszywające się pod łatki bezpieczeństwa, aktualizacje lub prawie wszystko, co przemawia do celu, może przenosić wiele różnych ładunków, takich jak rejestratory kluczy lub złodzieje haseł. Kiedyś odkryłem konia trojańskiego na komputerze klienta, który przesyłał strumieniowo wideo z kamery internetowej i dźwięk z mikrofonu w czasie rzeczywistym. Chociaż źle napisana i wyraźnie praca amatora, działała wystarczająco dobrze, co powinno być wystarczającym wskaźnikiem tego, jak łatwe jest opracowanie takich narzędzi. Jak mówi stare powiedzenie, strzeż się Greków niosących dary. Innymi słowy, nie przyjmuj hojnych prezentów bez pytania: nic nie jest za darmo.

Wykorzystanie pragnienia pomocy

Pomoc jest potrzebna wszystkim pracownikom w firmie, szczególnie dla nowo przybyłych i klientów. Właśnie dlatego nowi pracownicy i odwiedzający klienci są bardzo popularnymi postaciami dla inżynierów społecznych. Oczekuje się, że ktoś nowy w firmie zadaje pytania i nie zna lin. Klient jest źródłem dochodów, a większość firm pochyla się w tył, aby upewnić się, że są zadowolone. Pierwsza trasa - udawanie nowej wypożyczalni - jest najłatwiejsza do wykorzystania. Wszyscy pamiętają swój pierwszy dzień w pracy i to, jak może to być zastraszające, więc wśród obecnych pracowników istnieje naturalna tendencja do udzielania pomocy. Będąc nowym najemcą, możesz także odrzucić szereg trudnych pytań: nie otrzymałeś jeszcze odznaki, nie wiedziałeś, że nie powinieneś tu być, i tak dalej.

Pozwala również zadawać pytania bez wzbudzania podejrzeń. Na przykład pytanie o drogę, pomoc w wejściu do sieci, przesuwanie przez drzwi, ponieważ znowu nie otrzymałeś jeszcze odznaki. (Nie ma znaczenia, że pierwszą rzeczą, którą robi ochrona, jest przyznanie ci odznaki i wszyscy o tym wiedzą - to wciąż skuteczne kłamstwo.) Aby przeprowadzić ten rodzaj ataku, musisz dobrze przygotować swój urok i mieć imiona menedżerowie wyższego szczebla, aby dołączyć do rozmowy, aby dać Ci trochę wiarygodności. W rzeczywistości pozwala to na ustanowienie łańcucha wiarygodności poprzez zachęcanie ludzi do robienia rzeczy za Ciebie. Na przykład pytasz urzędnika o informacje. (Potrzebujesz go, ponieważ pan X mówi, że go potrzebujesz). Urzędnik następnie dzwoni, aby uzyskać te informacje. Nazywa cię przez telefon „nowo zatrudnionym" lub „nowym facetem" (co zwykle wystarcza, aby zagwarantować sukces). Ona z kolei może również upuścić nazwisko Pana X, a łańcuch jest zakończony. Wykorzystywanie autorytetu innych osób w ten sposób (w tym przypadku zarówno urzędnika biurowego, jak i pana X) jest zwykle bardzo skuteczne.

Wykorzystywanie pragnienia bycia lubianym

Praktycznie każdy lubi mieć wrażenie, że jest lubiany lub dobrze przemyślany. Klasyczny atak socjotechniki polega na wywołaniu tego uczucia u tych, którymi manipulujesz. Jest to zaskakująco łatwe i pomimo pozorów, im zimniej można się spotkać, tym łatwiej. Ludzie, którzy są zimni dla innych, często są w ten sposób, ponieważ są przyzwyczajeni do niewdzięcznego traktowania lub patrzenia z góry; to naturalny mechanizm obronny. Zachowuj się tak, jakbyś naprawdę czegoś potrzebował i okazuj prawdziwą wdzięczność, gdy ktoś wydaje się być gotowym ci to dać. Uśmiechaj się, bądź przyjazny i uważaj, aby nie podświadomie odzwierciedlać chłodną sylwetkę innej osoby. O wiele łatwiej jest polubić kogoś, jeśli można oszukać się w przekonanie, że tak naprawdę jest. Pomyśl o tych wszystkich sprzedawcach, z którymi się spotkałeś: z którymi odniosłeś największy sukces i z którymi łatwo się rozmawia?

Zastanów się, dlaczego tak było. Dobry sprzedawca to taki, do którego możesz natychmiast się ogrzać; zły wygląda tak, jakby desperacko próbował być twoim przyjacielem.

Podejścia taktyczne do inżynierii społecznej

Po omówieniu ogólnie ogólnej filozofii inżyniera społecznego, w tej sekcji znajdują się wskazówki i porady dla inżynierów społecznych. Patrzy na konkretne taktyki, które można zastosować w rozmowach, aby osiągnąć swoje cele (lub przynajmniej przyspieszyć proces). Po przeczytaniu każdej sekcji zastanów się nad osobami, które znasz i jak Twoim zdaniem zareagują na każde podejście. Jest to o wiele łatwiejsze niż można sobie wyobrazić. Na przykład zachowanie wojowniczego i władczego ze średnim kierownictwem doprowadzi cię szybko do nikąd (chyba że uda ci się przekonać ofiarę, że jesteś kierownictwem wyższego szczebla), podobnie nie oczekujesz udanego ataku informatycznego na personel IT. Ten rodzaj mentalnego szablonowania okaże się bardzo przydatny.

Działając niecierpliwie

Zachowanie się z niecierpliwością, gdy ktoś porusza się zbyt wolno lub wydaje się, że zastanawia się nad zweryfikowaniem Twojej historii, może skutecznie wykoleić się na przestrzeganiu przez niektórych osób przyjętych protokołów bezpieczeństwa. Zwykle można oczekiwać jednej z trzech odpowiedzi:

• Skołatany cel - wtedy ludzie wpadają w panikę, ponieważ nie ma ich głębokości i wyczucia, że poradzą sobie z sytuacją, z którą nie zostali przeszkoleni. Ludzi, którzy nie wiedzą, co robić, można łatwo manipulować. Jeśli wystąpi taka reakcja, należy natychmiast zmienić przyczepność - uspokój się, ale jednocześnie stanowczo. Przyjmij osobowość alfa, co oznacza, że wiesz, co należy zrobić, a ty zajmiesz się sytuacją w celu rozwiązania problemu. Ludzie reagują bardzo dobrze na to podejście,

ponieważ rozwiązujesz ich problem, a jednocześnie bierzesz na siebie odpowiedzialność (tj. odbierasz im odpowiedzialność). Pokazujesz również, że jesteś rozsądną osobą i nie tylko się na nich gniewasz.

• Cel kooperacyjny lub obojętny - są to dwa bardzo różne stany mentalne, ale wynik końcowy jest taki sam. Większość ludzi nie lubi konfliktu i zrobi wszystko, co w jego mocy, aby go uniknąć. Często oznacza to po prostu uniknięcie problemu. Współpraca ma miejsce, gdy cel po prostu chce odejść i podświadomie zracjonalizuje to w stosunku do danego ryzyka. Obojętność polega na tym, że (ponownie często podświadome) cele nastawienia rozwijają się, gdy decydują, że po prostu nie otrzymują wystarczających wynagrodzeń, aby mogli być traktowani w ten sposób i dlatego nie można oczekiwać, że będą działać w tych warunkach. W związku z tym nie mogą oni ponosić odpowiedzialności za robienie tego, co konieczne, aby szybko pozbyć się tej niegrzecznej osoby. Wynik każdej reakcji jest taki sam.

• Stonewaller - Powoduje to, że jesteś ignorowany, dopóki nie odejdziesz i nie wrócisz trochę milej. To nie jest pożądany wynik ale można go uniknąć, jeśli lepiej sobie radzisz z odczytywaniem celu aby zacząć. Różne podejścia działają na różnych ludzi; w twarzy sfrustrowanej niecierpliwością, po prostu zamknie się i zignoruje cię.

Zatrudnianie grzeczności

Osoba, która cię kamienowała, prawdopodobnie zareagowałaby o wiele lepiej na odrobinę grzeczności. Grzeczność to nie to samo, co bycie formalnym. Wielu ludzi myli to. To ci sami ludzie, którzy myślą, że niegrzeczność jest tym samym, co bycie szczerym. Uprzejmość to połączenie szacunku, szacunku i uspokojenia kogoś. Istnieją niezliczone przypadki przestępców, którzy wcielili się w zaufanie innej osoby, a później, gdy rzeczywistość tego, kim są, została odkryta (wraz z brakującą biżuterią), wszyscy ludzie powiedzą: „Ale on był takim miłym człowiekiem!". lub „Prawdziwy dżentelmen, taki uprzejmy". Dlaczego grzeczność jest tak skuteczna? Ponieważ bardzo niewielu z nas jest na to narażonych. Prawdziwa uprzejmość nie zależy od tego, co ktoś może dla ciebie zrobić. Na przykład, maitre d'naprawdę nie przejmowałoby się tym, czy lubisz jeść posiłek, o ile zostawisz dobrą wskazówkę, więc możesz mieć pewność, że dziecko w McDonald's nie jest szczególnie zainteresowane tym, czy masz miły dzień. Takie wyrażenia są grzecznością jak polityka korporacyjna. W świecie biznesu ludzie są przyzwyczajeni do bycia stosunkowo nieformalnymi z bliskimi współpracownikami i angażowania się w różne formalności z szefami, menedżerami, klientami i tak dalej. Zastanów się nad tym przy następnym logowaniu na stronie klienta, a nawet po prostu przestań rozmawiać z personelem sprzątającym.

Wywoływanie strachu

Jest to nieprzyjemna, ale niezwykle skuteczna taktyka, do której często sięgają kryminalni inżynierowie społeczni. Zasadniczo tworzysz problem (lub przekonanie, że problem istnieje) i przekonujesz cel, że on lub ona jest przyczyną. To wywołuje strach - w szczególności wywołuje strach przed pracą. Prawdopodobnie słyszałeś stare powiedzenie, że jeśli możesz przestraszyć ludzi, możesz zmusić ich do zrobienia czegokolwiek. (Jeśli pracujesz dla jednej z czterech dużych firm księgowych, jest to praktycznie motto korporacyjne, ale to dygresja). Strach jest silnym czynnikiem motywującym. Ostatnio okazało się, że księgowy otrzymał telefon od mężczyzny, który rzekomo pochodzi z „bezpieczeństwa wewnętrznego", który przedstawił się jako „John Richards". Jego identyfikator dzwoniącego to potwierdził. „Pan Richards" był najwyraźniej wściekły, ponieważ księgowy próbował zhackować serwery, co doprowadziło do awarii serwera księgowego i znacznej utraty danych. „Pan Richards" użył słów takich jak „zwolnienie" i „rażące przewinienie" i szybko potrzebował wyjaśnienia ponieważ policja była w drodze. Nic dziwnego, że księgowy spanikował i zaprotestował przeciwko swoje winnie. „Pan Richards" powiedział, że jedyną inną możliwością było przejęcie jego stacji roboczej

przez hakerów - wystarczyłoby kilka prostych testów. Księgowy powiedział, że zrobi wszystko, co w jego mocy, aby pomóc i chętnie wpisał polecenia, które mu przekazano, czytając informacje „Panu Richardsowi". Prawdopodobnie możesz zobaczyć, gdzie idę z tym. Nie było „Mr Richards" ani „bezpieczeństwa wewnętrznego", hakerów i awarii serwera. Atakującym był sam „Richards", który był w stanie wykorzystać strach księgowego, aby zmusić go do zainfekowania swojej maszyny koniem trojańskim. Jeśli chodzi o identyfikator dzwoniącego, manipulowanie nim jest banalne. Możliwe, że ktoś powie telefonowi, że jesteś Świętym Mikołajem, jeśli chcesz.

Fałszywe błaganie

Ta metoda polega na rzuceniu się na czyjąś łaskę lub błaganiu o pomoc. Jest to skuteczna technika uzyskiwania pomocy (szczególnie jeśli jesteś dobry w udawaniu silnych emocji), ponieważ nie jest to coś, z czym wiele osób wie, jak sobie z tym poradzić. Chociaż ludzie mogą być stosunkowo nieformalni w kontaktach z bliskimi kolegami, to tylko w czasach wielkiego stresu, presji lub katastrofy w ich życiu osobistym (jeśli wtedy) wykazują silne emocje lub płacz przed sobą (nie mówiąc już o całkowitych nieznajomych). Takie podejście ma zdolność do całkowitego toczenia się po ścianach, które inni budują wokół siebie w profesjonalnym środowisku. Kiedy ktoś staje w obliczu prawdziwego niebezpieczeństwa, reaguje na różne sposoby (zwykle z pewnym zakłopotaniem), ale instynkty ogromnej większości ludzi pomogą, jeśli mogą, niezależnie od konsekwencji bezpieczeństwa. Generując poczucie kryzysu, sugerujesz pilność. Przykłady sposobów zastosowania tej techniki obejmują:

• pozyskiwanie danych kontaktowych („To nagły wypadek!").

• uzyskanie podwyższonego poziomu dostępu do systemu lub aktywów w nim lub obszar budynku („Mój kontakt nie jest chory. Jeśli tego nie zrobię, stracę pracę! ").

Tak jak w przypadku każdego scenariusza inżynierii społecznej, dobrym pomysłem jest postawienie się w miejscu docelowym i zastanowienie się, jak zareagujesz w danych okolicznościach.

Przywoływanie władzy

Jednym z najsilniejszych ataków socjotechnicznych jest wykorzystywanie zakorzenionej tendencji docelowego personelu, by nie kwestionować osób sprawujących władzę. Jest to podobne podejście do wzbudzania strachu, z tym że jest ono bardziej subtelne. W tym przypadku nie musisz wyjaśniać pracownikom, że nieposłuszeństwo oznacza utratę zatrudnienia: ludzie wiedzą, skąd pochodzą pieniądze na czynsz. Aby przeprowadzić ten atak w wiarygodny sposób, niezbędny jest dostęp do informacji o hierarchii docelowej, aby być wystarczająco przekonującym. Istnieją dwa podejścia: pierwsze obejmuje bezpośrednie maskowanie się jako postać władzy; drugi obejmuje maskoanie się jako ktoś działający w ich imieniu. Wykorzystywanie potęgi władzy jest powszechną techniką podczas przeprowadzania telefonicznych ataków socjotechnicznych, szczególnie w szpiegostwie korporacyjnym. Im bardziej młodszy i niedoświadczony cel, tym skuteczniejszy staje się atak, ponieważ mieli oni mniej czasu na zapoznanie się z procedurą operacyjną i innymi pracownikami. Powszechnym podejściem jest wywoływanie celu pod postacią starszego kierownika projektu (najlepiej kogoś, kogo cel nie osiągnął) i dawanie wymówki, dlaczego nie możesz uzyskać dostępu do swoich danych - na przykład, jesteś w drodze i zgubiłeś BlackBerry - i zażądaj dokumentów projektu na pilne spotkanie. Jedną z korzyści korzystania z autorytetów jest to, że mają moc nagradzania i karania. Sprytny inżynier społeczny rozumie to i dalej motywuje swój cel, obiecując, że taka pomoc nie zostanie zapomniana. Istnieją różne warianty tego podejścia: możesz podejrzewać menedżera klienta, który potrzebuje kopii wszystkich ostatnich dokumentów. Atakujący często się maskują dosłownie jako postacie władzy, takie jak policjanci prowadzący dochodzenie w sprawie przestępstwa. Jak stwierdza Niccolo Machiavelli w

Księciu: „Najlepiej się bać i kochać; jeśli jednak nie można być obojgiem, lepiej się bać niż kochać. ”Inżynier społeczny lepiej motywuje pracowników, jeśli to możliwe, ale najważniejszym czynnikiem motywującym jest zawsze strach. Może wydawać się dziwne lub niewiarygodne, że ludzie zareagują na pojęcie władzy od ludzi, których nie znają lub myślą, że znają, ale nie mogą zweryfikować. Jest to jednak jedno z najbardziej udanych podejść, jakie może zastosować inżynier społeczny i, podobnie jak poprzednie ataki, wymaga silnego poczucia pilności, aby osiągnąć zgodność z celem, zanim zdąży się zastanowić. Firmy powinny wyjaśnić swoim pracownikom, że nie ma to wpływu na nieprzestrzeganie instrukcji podanych przez telefon z niezweryfikowanych źródeł.

Stosując wdzięczność lub szacunek

To jest odwrotna forma ataku mocy władzy, w której grasz do postrzeganego przez innych znaczenia. Jest to forma manipulacji, w której uznajesz władzę innej osoby nad tobą. Sugerujesz: „Wiem, że jestem tylko kiepskim trybikiem w wielkim schemacie rzeczy, ale masz moc, aby to zrobić, prawda?” Ten atak działa, ponieważ masz czyjś (często złudzony) zmysł bycia niezastąpionym i ważnym i urzeczywistnienia go, przynajmniej dla nich i na krótki okres czasu. Ponadto, im bardziej przesadne poczucie znaczenia, jakie dana osoba ma dla swojej pozycji w maszynie korporacyjnej, tym niższe są szczeble, które skłonni są do ciągłego umacniania własnej wartości.

Granie w często błędne postrzeganie własnego znaczenia przez ludzi nie ogranicza się wyłącznie do autorytetu. Kilka lat temu, kiedy przeprowadzałem wiele konsultacji dla różnych departamentów brytyjskiego rządu w Londynie, często słyszeliśmy, że konsultanci z sektora prywatnego odnoszą się do urzędników służby cywilnej, z którymi współpracowaliśmy, jako „Mittys” - nawiązanie do Waltera Mitty , fikcyjna postać, która żyła w iluzorycznym świecie snów, w którym ratował ludzkie życie i wykonywał ściśle tajne prace. Samoocena osoby jest zazwyczaj zabarwiona otoczeniem. Na przykład portier wpuszcza cię do swojego teatru i podobnie urzędnik służby cywilnej w wydziale zajmującym się bezpieczeństwem często myśli o sobie jako o krok od Jamesa Bonda. Psychologicznie jest to rekompensata za poczucie bezwartościowości i niepowodzenia, na które cierpi wiele osób w dzisiejszych czasach. Jest to w większości nieszkodliwe, ale można przekształcić je w słabość, którą można wykorzystać, dzięki poprawnie sformułowanemu żądaniu, na przykład: „Cześć, rozumiem, że jesteś tutaj autorytetem, wszyscy tak mówią” lub „Moja wiedza na temat takich i takie jest dość słabe, naprawdę doceniłbym wkład kogoś z twojej pozycji. ”Jakiego pochlebstwa potrzebowałbyś, abyś się otworzył i porozmawiał? Czego potrzeba, aby ktoś poczuł się ważny? Czy bylibyście bardziej otwarci, gdyby tak zrobili?

Korzystanie z manipulacji seksualnej

Inną popularną techniką inżynierii społecznej stosowaną od zarania dziejów jest manipulacja seksualna. Pomimo tego, co może powiedzieć podręcznik firmy na temat unikania pozwów o molestowanie, w większości środowisk pracy występuje flirt między pracownikami płci przeciwnej lub czasem tej samej płci. (Pracuję w Holandii.) W każdym miejscu pracy jest ładna dziewczyna, która może mrugać powiekami do mężczyzny i zmuszać go do naprawy komputera (lub cokolwiek innego). Mężczyźni (i, co ciekawe, mężczyźni pracujący w branży IT) są znacznie bardziej podatni na manipulowanie w ten sposób niż kobiety. (Dlaczego powoduje to zabawną spekulację i dyskusję.) Podczas wdrażania tego rodzaju taktyki w ćwiczeniach socjotechnicznych wykorzystywanie kobiet do wykorzystywania mężczyzn jest znacznie bardziej niezawodne niż na odwrót. Jest również całkowicie możliwe, aby mężczyźni używali zmieniaczy głosu, aby uzyskać przekonujący kobiecy głos przez telefon. Przeprowadzeniu inżynierii społecznej w ramach testu zawsze powinna towarzyszyć ocena ryzyka prawnego metod, które zamierzasz wdrożyć. Takie podejście może spowodować poważne komplikacje prawne w Stanach Zjednoczonych i innych środowiskach spornych. Zarządzanie zaangażowaniem jest

kluczowe. Istnieje kilka powodów, dla których ta technika jest skuteczna w prawdziwym świecie; wszyscy mężczyźni są wdzięczni za uwagę kobiet, które są postrzegane jako atrakcyjne, a także fakt, że kobieta potrzebuje pomocy i prosi ją o nią, jest potężną siłą motywującą dla wielu mężczyzn. Poprzez utrwalenie obrazu własnego celu osoby, która pomaga damie w niebezpieczeństwie, usuwasz wszelkie naturalne podejrzane mechanizmy obronne, które może ona posiadać. Wielu mężczyznom bardzo trudno jest odmówić kobiecie proszącej o pomoc, a to ma tyle samo wspólnego z zakorzenionymi uwarunkowaniami kulturowymi, jak wszystko inne. Bardzo trudno jest zabezpieczyć się przed tą techniką. Nie możesz po prostu powiedzieć swoim pracownikom, aby nie ufali kobietom. W związku z tym istnieje wiele przykładów skutecznego wdrożenia tej strategii w fikcji i świecie rzeczywistym.

Podsumowanie

Ta część niekoniecznie różni się nieco od innych . Chociaż łatwo jest pokazać komuś, jak wybrać blokadę lub zhackować sieć bezprzewodową, inżynieria społeczna jest tematem o wiele bardziej subiektywnym i dlatego należy ją opisać bardziej abstrakcyjnie. Najważniejsze jest to, że możesz dużo przeczytać na ten temat i, ogólnie, na temat psychologii, ale twój sukces w tej dziedzinie będzie w dużej mierze zależał od twojej osobowości i umiejętności ludzi. Możesz mieć wrażenie, że nie posiadasz wymaganej natury - bardzo niewiele osób, a problem ten pogarsza fakt, że takich umiejętności nie da się ćwiczyć - przynajmniej w ten sposób, że możesz ćwiczyć hakowanie lub wybieranie zamków. W każdym razie prawdopodobnie masz w zespole jedną osobę, która może kompetentnie wykonać aspekt socjotechniczny testu. Jeśli nie, sugeruję zwrócić się do sprzedawców. W końcu wiele technik omówionych tutaj jest podobnych do stosowanych przez sprzedawców.