Kierowanie i rozpoznawanie

Inżynieria społeczna, w przeciwieństwie do wielu metod atakowania ludzi, jest zazwyczaj zależna od celu. Inżynier społeczny mądrze wybiera, na kogo celować, aby stworzyć idealny atak inżynierii społecznej i ma kilka nieprzewidzianych okoliczności, jeśli niektóre etapy ataku zawiodą. Wybór, kogo zaatakować, rzadko jest trafnym przypuszczeniem; atak rozpoczyna się od zebrania dużej ilości informacji w celu znalezienia celu. Ze względu na charakter tego rodzaju ataku głupotom byłoby, gdyby osoba atakująca polegała na szczęściu. Może się okazać, że wybrany cel nie ma nic do zaoferowania, a zatem wszystkie wysiłki i zasoby wykorzystane w całym ataku marnują się. Atak inżynierii społecznej musi być dostosowany do konkretnego celu, w przeciwnym razie nie zadziała. Udany atak na określony cel niekoniecznie będzie działał na innym ze względu na poziom specyficzności, który należy zastosować. Inżynier społeczny wybierze również swój cel na podstawie innych czynników. W większości przypadków atakujący chce pieniędzy, dlatego ataki te będą koncentrować się głównie na ludziach zamożnych lub kontrolujących pieniądze. Dlatego nawet księgowy zamożnej organizacji może być głównym celem. Innym razem inżynier społeczny szuka informacji. Informacje są bardzo drogie, dlatego konkurenci biznesowi czasami łatwiej zatrudniają napastników w celu uzyskania tajnych informacji o innych organizacjach w ich branży. Skoncentrujemy się na tym, jak inżynierowie społeczni wybierają cele i planują atak. Ucząc się, w jaki sposób inżynierowie społeczni dokonują celowania i rozpoznawania, możemy lepiej chronić się przed tego rodzaju atakami. Lista nie jest wyczerpująca, ale obejmie główne cele inżynierów społecznych. Cele, które zostaną omówione w tym rozdziale, są następujące:

* Banki

* Stare organizacje

* Pracownicy organizacyjni:

- Personel IT

- Agenci wsparcia klienta

- Personel wyższego szczebla

-Personel finansowy

*Starsi ludzie

* Życzliwi

Wprowadzenie

Atak inżynierii społecznej rzadko jest błędem. Nie można go porównać do oszustwa z użyciem karty kredytowej lub włamania do wiadomości e-mail, które mogą być skierowane do każdego. Jest to jeden z powodów, dla których inżynieria społeczna jest bardzo skuteczną metodą ataku z mniejszą szansą na niepowodzenie. Koncentruje się na celu, a atakujący nie traci ostrości na celu, dopóki atak nie zostanie wykonany lub nie będzie można go wykonać. W niefortunnych okolicznościach dla atakującego, czasami atak będzie musiał zostać odwołany, jeśli atakujący uważa, że cel go wykonał lub główny cel został utracony, tak jak cel tracący pieniądze lub dostęp do pieniędzy. Firmy ochroniarskie katalogują typy osób i organizacji, które zostały zaatakowane przez inżynierów społecznościowych i wydaje się, że istnieje pewna spójność. Opierając się na tej spójności, ta część dostarczy więcej informacji na temat rodzajów ludzi i organizacji, na które istnieje duże prawdopodobieństwo, że zostaną dziś obrani. Są one omówione w następujący sposób:

Banki

Gromadzenie informacji można przeprowadzić w dwóch szerokich kategoriach metod - technicznych i nietechnicznych. Jak sama nazwa wskazuje, nietechniczne metody techniczne polegają na komputerowych technikach zbierania informacji. Nie ma jednak pewności, że dane narzędzie lub urządzenie elektroniczne uzyska wystarczające informacje o celu. Dlatego do zebrania informacji o obiektach docelowych można użyć kombinacji wymienionych niżej narzędzi i urządzeń. Inżynierowie społeczni wykorzystają wiele narzędzi / technik gromadzenia informacji i połączą uzyskane informacje, aby zbudować profil dla swoich celów. Nic dziwnego, że pierwszym celem na liście byłyby pieniądze. Inżynierowie społeczni w większości przypadków szukają pieniędzy, dlatego banki są głównym celem. To nie są stare czasy, kiedy pieniądze były trzymane tylko w twardej gotówce i trzeba było fizycznie obrabować bank, aby zdobyć je nielegalnie. Pieniądze są płynne i są przesyłane przez Internet. Dlatego banki są głównie ukierunkowane na ich możliwości bankowości internetowej. Banki to także wrażliwe instytucje, które przechowują poufne informacje o klientach. Informacje te są cenne i jeśli inżynier społeczny może uzyskać do nich dostęp, może uzyskać za nie gruby okup lub sprzedać je po wysokiej cenie na czarnym rynku. Zawsze znajdzie się nabywca chętny do uzyskania tego rodzaju informacji. Z tego powodu banki stosują jedne z najbardziej wodoszczelnych systemów bezpieczeństwa zarówno fizycznie, jak i online, aby chronić przechowywane przez siebie środki pieniężne i poufne informacje o klientach. Inżynieria społeczna to jednak inny rodzaj ataku. Nie próbuje atakować systemów, atakuje ludzi korzystających lub kontrolujących systemy. Dlatego personel bankowy jest celem ataków z zakresu inżynierii społecznej.

W 2011 r. Forum cyberbezpieczeństwa opublikowało artykuł o inżynierze społecznym, który dokonuje profesjonalnych napadów na banki. Mówi się, że socjotechnik, Jim Stickley, odniósł tak wielki sukces, że dokonał ponad tysiąc napadów na banki, wciąż licząc. Został zatrudniony przez wiele banków w celu zidentyfikowania luk w ich bankowych systemach bezpieczeństwa, a jego główną atrakcją były szkolenia i polityki bezpieczeństwa. Powiedział, że nawet jeśli bank ma silną politykę, ale strzegą banku osoby niedoinformowane, inżynierowie społeczni z łatwością wejdą do środka bez prawie żadnych barier, aby je powstrzymać. Naprawdę niewiele można zrobić, aby wzmocnić ludzki element w konfiguracji zabezpieczeń. Inżynier społeczny, odnosząc sukces w kradzieży banków, powiedział, że zawsze używa pretekstów, z których najczęstszym jest inspektor przeciwpożarowy. Ma odpowiedni mundur i odznaki, dzięki czemu szybko wchodzi do banku bez wzbudzania alarmu. Według niego bardzo trudno jest odmówić wstępu inspektorowi przeciwpożarowemu. Będąc w budynku, Stickley powiedział, że zawsze nosi pustą torbę we wszystkich swoich misjach. Ludzie nie chodzą do banków, aby kraść pieniądze, kradną informacje. W lokalu zbierze między innymi dyski twarde, dokumenty leżące na stołach i zewnętrzne dyski twarde. Spróbuje również podłączyć urządzenie do gromadzenia danych do sieci organizacji, aby mieć dostęp do sieci po wyjściu z lokalu. Powiedział, że używa urządzeń bezprzewodowych, które może łatwo kontrolować poza lokalem, i próbuje zhakować obecne zabezpieczenia sieci. W niektórych przypadkach Stickley mówi, że wyjdzie z serwerem. Wszyscy zakładają, że nie można sobie wyobrazić, aby serwer był przenoszony bez zgody kogoś. Poprzedni przykład dotyczący profesjonalnego rabusia banków pokazuje, że nie tylko rabowanie banków jest możliwe, ale czasami jest łatwe. Celem wydają się być wrażliwe dane, które najwyraźniej nigdy nie są daleko, gdy inżynier społeczny znajdzie się w banku. Zebrane zewnętrzne urządzenia pamięci masowej i urządzenie podłączone do sieci dostarczą tony informacji inżynierowi społecznemu. Informacje te są bardzo wrażliwe i równie drogie. W 2015 r. Haker zdobył niektóre dane klientów należących do klientów banku w Zjednoczonych Emiratach Arabskich (ZEA). Haker zażądał okupu w wysokości około 3 USD, ale bank odmówił zapłaty. Po tej odpowiedzi haker opublikował wyciągi bankowe 500 klientów i skontaktował się z klientami grożącymi ujawnieniem poufnych informacji, jeśli nie zostanie mu zapłacony okup. Szkodziło to reputacji banku, a skutki tego były ogromne. Dlatego jeśli inżynier

społeczny wejdzie do banku i ujawni poufne informacje, może zażądać ogromnych kwot okupu, tak jak w przypadku banku ZEA. Możliwość rake'owania w takich kwotach po prostym zadaniu chodzenia po terenie banku sprawia, że banki są głównym celem inżynierów społecznych.

Stare organizacje

Kolejnym celem, na który inżynierowie społeczni są zawsze gotowi rzucić się, jest każda stara organizacja. Większość młodych firm będzie miała nowych pracowników, a nowi pracownicy zapewnią, że określą pewne podstawowe zasady, takie jak ścisłe zasady informatyczne i zaawansowane mechanizmy bezpieczeństwa, aby zapobiec wielu zagrożeniom cybernetycznym. Z drugiej strony stare firmy są atakowane, ponieważ są prawdopodobnie winowajcami korzystania ze starszych systemów informatycznych, które są podatne na awarie i ciągle się zawieszają. Istnieje co najmniej szansa, że będą mieli komputer, który był używany od dziesięcioleci i zwykle jest planowany na jakąś konserwację. Dlatego inżynierowi socjalnemu łatwo będzie udać się pod pretekstem wykonawcy wysłanego do naprawy kilku starych komputerów. Będąc w organizacji, inżynier społeczny z łatwością zbierze więcej informacji. Bardziej prawdopodobne jest, że organizacja będzie mieć łagodniejsze zasady bezpieczeństwa IT, które są przestarzałe i rzadko przestrzegane przez pracowników. Dlatego pracownicy będą mieli hasła zapisane na biurkach, będą to dokumenty poufne niepewnie przechowywane, a zewnętrzne nośniki danych zawierające kopie zapasowe będą otwarcie przechowywane. Inżynier społeczny może wyrządzić ogromne szkody takiej organizacji. Ten rodzaj ataku jest zwykle przeprowadzany w organizacjach, które zlecają stronom trzecim konserwację sprzętu IT z powodu gwałtownych awarii. Nowsze organizacje mają zwykle nowy sprzęt, a personel jest bardziej wyszkolony w zakresie przestrzegania zasad bezpieczeństwa IT. Dlatego będą bardziej uważać na to, co pozostawiają na zewnątrz, na wypadek, gdyby inżynier społeczny z powodzeniem dostał się do organizacji.

Pracownicy organizacji

Czasami ataki socjotechniczne nie są przeprowadzane przeciwko jednostkom, koncentrują się na organizacji. Ponieważ konkurencja na niektórych rynkach jest sztywna, niektóre organizacje przechodzą na złośliwe sposoby uzyskania przewagi konkurencyjnej. Jednym z tych sposobów jest nielegalne pozyskiwanie poufnych informacji o ich konkurentach. Inżynierowie społeczni są więc czasami zatrudniani przez organizacje do zbierania tajemnic handlowych, planów, poufnych dokumentów, komunikacji wewnętrznej, a nawet danych konsumentów od konkurentów. Jak zobaczymy w następnej części, szeroko rozpowszechniono inżynierię społeczną w szpiegostwie korporacyjnym, w którym inżynierowie społeczni są wynagradzani za ukierunkowanie na konkretną organizację. Niektórzy pracownicy są zatem głównymi celami, kiedy należy to zrobić. Są to:

Personel IT

Czy istnieje lepszy cel na początek niż osoba odpowiedzialna za zapewnienie bezpieczeństwa danych organizacyjnych? Każdego roku wielu pracowników IT jest atakowanych przez hakerów z nadzieją na zdobycie ich uprzywilejowanych kont w sieci. Dzięki dostępowi do tych kont dane z organizacji mogą zostać łatwo skradzione, a komunikacja wewnętrzna może wyciec poza organizację. Pracownicy IT dużych organizacji często padają ofiarą wiadomości e-mail typu phishing ze złośliwymi linkami, o których wiedzą i których można łatwo uniknąć. Nie są jednak w połowie tak gotowi, aby odeprzeć atak inżynierii społecznej. Inżynierowie społeczni mają w zanadrzu wiele sztuczek, aby uzyskać informacje na temat personelu IT, które mogą wykorzystać do udanego ataku. W poprzednim rozdziale omówiono kilka narzędzi, które umożliwiają inżynierom społecznym zbieranie informacji o celach. Od mediów społecznościowych po obserwacje. Inżynierowie społeczni wykorzystają najmniej oczywiste metody pozyskiwania personelu IT, ponieważ tego rodzaju cele są zwykle podejrzane. W związku z tym nie

można im przekazać pendrive'a obciążonego złośliwym oprogramowaniem i zostać poproszonym o włożenie go do komputera. Trudno będzie ich przestrzegać. Są atakowani pośrednio, dopóki nie zaufają inżynierom społecznemu na tyle, że wpadną w pułapkę. Mogą być również kierowani na odwiedzane witryny zewnętrzne. Jeśli osoba atakująca byłaby w stanie skompromitować witrynę forum IT, taką jak https://stackoverflow.com/ lub https://stackexchange.com/, aby wykonać atak wodopoju, wielu specjalistów IT mogłoby zostać trafionych. Weźmy przykład, w jaki sposób możemy inżynierię społeczną starszego oficera IT hipotetycznej firmy ABC. Pierwszym przystankiem będzie LinkedIn, gdzie zgromadzimy wiele informacji o docelowym pracowniku. Mamy nadzieję, że cel opublikował wszystkie informacje o swojej edukacji i historii pracy. Dzięki tym informacjom możemy przejść do Facebooka i spojrzeć na profil tego pracownika. Możemy również odwiedzić jego konta na Twitterze i Instagramie, jeśli ma jakieś informacje na temat tego, co zwykle publikuje na Twitterze i jakie typy zdjęć publikuje. Po zebraniu wszystkich tych informacji tworzymy fałszywe konto na Facebooku i LinkedIn młodej, atrakcyjnej dziewczyny, która ma takie same zainteresowania jak informatyk i obecnie pracuje na poziomie podstawowym w organizacji położonej niedaleko firmy ABC. Możemy wysłać pracownikowi zaproszenie do znajomych na Facebooku, a ponieważ odrobiliśmy pracę domową, najprawdopodobniej ją zaakceptuje. Następnie możemy się z nim połączyć na innych platformach społecznościowych. Po nawiązaniu z nim kontaktu w co najmniej dwóch sieciach społecznościowych możemy porozmawiać z nim więcej na temat zainteresowań, naszych zainteresowań związanych z uczeniem się nowych rzeczy i perspektyw na przyszłość. Po zbudowaniu z nim relacji możemy wysłać mu plik obciążony złośliwym oprogramowaniem i poprosić go o pomoc w pilnej sprawie. Gdy pobierze plik, nasze złośliwe oprogramowanie po prostu zaatakuje jego komputer i zgromadzi informacje z jego komputera. Przykład może wydawać się prosty, ale sprawdził się w rzeczywistych sytuacjach. W lipcu 2017 roku ujawniono, że fałszywy profil dziewczyny o imieniu Mia Ash był wykorzystywany do inżynierii społecznej pracowników płci męskiej. Fałszywe konto było skierowane do pracowników płci męskiej w dużych firmach, a jej celem było szpiegostwo korporacyjne. Badania przeprowadzono na jej profilu i odkryto, że profil był kontrolowany przez grupę hakerów, o której uważa się, że OilRig jest wspierany przez Iran. Fałszywy profil został wykorzystany do zainfekowania komputera docelowego złośliwym oprogramowaniem o nazwie PupyRAT, które zapewniłoby zdalny dostęp do hakerów. Personel IT ma kontakt z wieloma innymi rodzajami ataków socjotechnicznych. Mają klucze do prawie wszystkiego w organizacji, a jeśli zostaną zaatakowani, atakujący zdobędzie bardzo wrażliwe dane i dostęp do poufnych wiadomości.

Agenci obsługi klienta

Agenci obsługi klienta również są atakowani przez inżynierów społecznych ze złośliwymi intencjami. W przeciwieństwie do pracowników IT, pracownicy ci nie mają wątpliwości co do ostrożności w kontaktach z domniemanymi klientami. Chcą utrzymać dobry wizerunek organizacji i będą chcieli zrobić wszystko, aby zaspokoić potrzeby klienta. Ponieważ przede wszystkim zajmują się komunikacją ze światem zewnętrznym, prawie zawsze otwierają wszystkie wiadomości e-mail wysyłane na adres e-mail firmy. Jest to droga, którą inżynierowie społeczni nie wahają się wykorzystać, aby wprowadzić złośliwe oprogramowanie do organizacji. Agent obsługi klienta, o ile nie zostanie przeszkolony inaczej, zastosuje się do żądania klienta, aby upewnić się, że klient jest zadowolony. Dlatego jeśli klient powie, że załączy plik, aby lepiej wyjaśnić wymagania, agent pomocy technicznej pobierze taki plik. Inżynierowie społeczni mogą również wykorzystywać tych pracowników, aby uzyskać więcej informacji na temat innych celów w organizacji. Agenci poinformują dzwoniącego, jeśli jakiś pracownik jest w pobliżu lub jest nieobecny. Ponieważ chcą być pomocni, wystarczy uzasadnić chęć poznania tych informacji. Jeśli chcemy zaatakować organizację udającą techników kontraktowych, najlepiej unikać starszego oficera IT. Dlatego najlepszym dniem do strajku jest nieobecność starszego oficera IT, tworząc w ten sposób idealny scenariusz, w którym inżynier społeczny może powiedzieć, że został

pilnie wysłany przez starszego pracownika, aby spojrzał na coś w serwerowni. Weźmy przykład, w jaki sposób możemy wykorzystać agenta do otwarcia złośliwego pliku. Załóżmy, że celowaliśmy w firmę zajmującą się częściami samochodowymi o nazwie XYZ. Możemy zadzwonić do biura obsługi klienta i powiedzieć, że chcemy konkretnej części, o której nie jesteśmy zaznajomieni, ale mechanik napisał jej opis i dał nam kilka zdjęć. Aby uniemożliwić pracownikowi działu obsługi klienta nakłanianie nas do korzystania z innych sposobów uzyskania tych informacji, musimy wywrzeć na nich presję, aby ułatwić przejście naszego ataku. Dlatego informujemy agenta, że spieszymy się na spotkanie, ale wyślemy załączniki do wiadomości e-mail ze wszystkimi informacjami i zdjęciami. Możemy podwoić presję, mówiąc, że część jest pilnie potrzebna, ponieważ samochód ma gotowego nabywcę czekającego na ten przedmiot. Powiedziawszy to, zalecamy im sprawdzenie wiadomości e-mail i niezwłoczne udzielenie odpowiedzi. Należy pamiętać, że wywieramy presję na agenta, a jedynym sposobem na złagodzenie tej presji jest spojrzenie na opis, o którym mówimy, sprawdzenie, czy część jest dostępna i skontaktowanie się z nami. Bezpieczeństwo nie jest już dla agenta priorytetem; zaspokojenie naszej pilnej potrzeby jest. Oprócz oryginalnych załączników możemy załączyć plik obciążony złośliwym oprogramowaniem, zaczekać, aż agent go pobierze i otworzy, a następnie złośliwe oprogramowanie zainfekuje jego komputer. Inną odmianą tego jest zachęcanie agentów do zapoznania się z opisem na naszej stronie internetowej, wywierania na nich presji, a następnie umieszczenia linku do złośliwej witryny. Tak czy inaczej, zanim agent zorientuje się, że to oszustwo, złośliwe oprogramowanie już zainfekowało swój komputer i zaczęło przesyłać nam informacje.

Personel wyższego szczebla

Kierownicy stali się wspólnymi celami inżynierów społecznych, głównie z powodu tego, co mają do zaoferowania. Ci starsi ludzie mają dostęp do bardzo wrażliwych danych korporacyjnych, są stronami poufnej komunikacji, a także mają własne zasoby osobiste, które można atakować. Dlatego nawet jeśli inżynier społeczny nie jest w stanie ukraść czegoś z organizacji, w których pracują, ich zasoby osobiste są nadal zagrożone i mogą być celem. Ze względu na ich starszeństwo kierownictwo jest mniej świadome bezpieczeństwa, ponieważ uważa się je za potężne, a zatem nie można ich ukarać, jeśli zignorują zasady bezpieczeństwa organizacji. Są również uważani za zajętych i dlatego są zwolnieni z udziału w szkoleniach z zakresu bezpieczeństwa z innymi pracownikami. Dlatego stają się łatwymi celami, ponieważ mają najmniejszą wiedzę na temat cyberzagrożeń i nie są świadomi, w jaki sposób powinni reagować na ataki skierowane na nich. Dodaj to do faktu, że nikt nie wywiera na nich presji, aby przestrzegali zasad bezpieczeństwa organizacji. Widzą zasady bezpieczeństwa jako niedogodności i prawie ich nie przestrzegają, chyba że nie będzie ich można obejść.

Proste zadanie, takie jak zmiana hasła po upływie 90 dni, jest postrzegane jako niedogodność i zmieniają się tylko wtedy, gdy systemy odmawiają zalogowania się. Nie chcą, aby ich działania w sieci były rejestrowane lub monitorowane, dlatego też będą chcieli host- oparte na zaporach ogniowych, które należy wyłączyć. Pomijają także prawie wszystkie inne zasady bezpieczeństwa, zwłaszcza jeśli nie są egzekwowane przez systemy, ponieważ znajdują się wyżej niż pracownicy IT. Jednocześnie, jeśli zostaną trafieni przez napastników, nie przyznają się do winy, a raczej obwinią dział IT za nie oferowanie im ochrony. Dlatego są bardzo łatwym celem dla inżynierów społecznych i stanowią poważne ryzyko dla każdej organizacji. Tego rodzaju cele przypadają na zaskakująco popularne oszustwa techniczne. Ponieważ jest to kadra kierownicza, wiele informacji na ich temat prawdopodobnie nie będzie dostępnych, dlatego gromadzenie danych nie jest tak trudne dla inżyniera społecznościowego. Dzięki zgromadzeniu wystarczającej ilości informacji na ich temat można łatwo ich oszukać, aby podjąć działania, które zagrażają ich bezpieczeństwu i organizacji, w której pracują. Są unikalnym celem, który zakłada, że bezpieczeństwo jest zapewnione, nawet jeśli nie działają zgodnie z zasadami bezpieczeństwa organizacji. Dlatego nawet jeśli klikną linki wysłane do nich pocztą e-mail

zakładają, że dział IT wprowadził wystarczające zabezpieczenia, aby zapobiec wystąpieniu złośliwego oprogramowania. Gdy podłączą swoje urządzenia osobiste do sieci organizacyjnej, ignorują ryzyko, że jeśli na ich komputerach osobistych znajduje się złośliwe oprogramowanie, przeskoczy on do sieci organizacyjnej. Ponieważ osoby atakujące zwykle chcą wybrać najmniej skomplikowany sposób, aby dostać się do sieci organizacyjnej w celu gromadzenia informacji, kierownictwo jest optymalną drogą do wykorzystania. Próba bezpośredniego ataku na sieć najprawdopodobniej zakończy się niepowodzeniem, ponieważ istnieje wiele zabezpieczeń zapobiegających tego rodzaju próbom. Jednak komputer osobisty dyrektora jest zawsze pożądaną opcją. Dlatego inżynierowie społeczni będą czekać w pokojach hotelowych na kradzież danych od kadry kierowniczej, która łączy się z hotelowym Wi-Fi. Będą też czaić się na lotniskach, szczególnie w salonach pierwszej klasy i klasy biznesowej pod pretekstem bycia bogatymi ludźmi, podczas gdy w rzeczywistości infekują komputery podłączone do Wi-Fi złośliwym oprogramowaniem. Dlatego niezwykle ważne jest unikanie przechowywania poufnych danych w miejscu pracy na komputerach osobistych. W przeciwieństwie do komputerów w miejscu pracy, komputery osobiste nie korzystają z takiej samej ochrony ze strony zespołu IT organizacji. Dlatego łatwo jest przeniknąć do takich maszyn i zainstalować złośliwe oprogramowanie, aby skopiować poufne dane i ujawnić poufne wiadomości. Jak powiedziano, pracownicy wykonawczy będą mieli niezabezpieczone wrażliwe dane na swoich komputerach osobistych, a gdy złośliwe oprogramowanie znajdzie się na ich komputerach, wszystko jest na łasce atakującego. Weźmy scenariusz, w którym chcemy ukraść dane dyrektorowi finansowemu amerykańskiego kontrahenta wojskowego. Musimy dołożyć należytej staranności, aby poznać jego codzienne harmonogramy. Możemy dowiedzieć się o jego ulubionych hotelach, planach podróży i wyjazdach weekendowych. Kiedy znajdziemy miejsce, które odwiedza w weekend lub w wakacje, musimy zebrać informacje wywiadowcze na temat tego miejsca, ponieważ jest to punkt, w którym go uderzymy. Zapewniamy, że otrzymamy hasła Wi-Fi, przeprowadzimy testowy atak na urządzenie, aby upewnić się, że etap jest ustawiony. Kiedy przychodzi CFO, możemy po prostu pokazać się jako normalni klienci i strategicznie siedzieć w miejscu, w którym fizycznie możemy zobaczyć CFO. Kiedy podłączy swoje urządzenie osobiste do sieci, możemy zainstalować w nim złośliwe oprogramowanie i rozpocząć z niego zbieranie danych. Jedynym wyzwaniem będzie, jeśli jego urządzenie ma program zabezpieczający hosta końcowego, który może zapobiec zainfekowaniu urządzenia przez złośliwe oprogramowanie. Ale są szanse, że uda nam się zainstalować złośliwe oprogramowanie.

Personel finansowy

Pracownicy działu finansowego są kierowani przez inżynierów społecznych, którzy są zainteresowani tylko pieniędzmi, a nie danymi. Pracownicy ci kontrolują ogromne sumy pieniędzy, płacąc dostawcom, kontrahentom, pracownikom, a także otrzymują pieniądze ze sprzedaży i innych źródeł dochodów. Zwykle zachowują się systematycznie i trzymają się wytycznych określonych w książce. Dlatego inżynierowie społecznościowi nie mogą ich łatwo oszukać za pomocą tanich oszustw, takich jak wiadomości phishingowe nigeryjski księcia. Phishingowy e-mail nigeryjskiego księcia to taki, w którym fałszywy e-mail jest wysyłany do celu wyjaśniającego kłopoty nigeryjskiego księcia, który chce wypłacić pieniądze, ale potrzebuje twojej pomocy. Jest to stara próba phishingu i nie odniesie sukcesu wśród personelu zajmującego się finansami . Aby ich zaatakować, musisz wyprowadzić ich poza znane im systematyczne środowiska operacyjne. Musisz je zmusić do pominięcia niektórych czeków przy wysyłaniu pieniędzy. Jednym ze sposobów, w jaki można to zrobić, jest wybranie pretekstu autorytatywnej postaci, która może nakazać im porzucenie regularnych procedur.

Przyjrzyjmy się prawdziwemu scenariuszowi sieci Ubiquity, który został oszukany przez atak inżynierii społecznej w sierpniu 2015 r. Okazało się, że członek personelu finansowego otrzymał od swojego szefa e-maila z prośbą o podanie poświadczeń logowania do firmy online konta Pracownik sprawdził

wiadomość e-mail, a ponieważ był podobny do tego, z którego korzystał jego przełożony, zastosował się do niej i podał poufne informacje. Uważa się, że napastnik użył sfałszowanego e-maila, aby udawać szefa. Ponieważ młodszym pracownikom nie zadaje się pytań o wiarygodne dane, np. Dlaczego złożono prośbę o informacje, informacje zostały podane. Atakującemu udało się przelać blisko 50 milionów dolarów z kont firmy na zagraniczne konto bankowe. Zanim pracownicy zdali sobie sprawę, że wiadomość e-mail nie pochodzi od ich szefa, haker zdążył już pozbyć się tych pieniędzy. Firma była jednak w stanie odzyskać blisko 10 milionów dolarów skradzionych pieniędzy, ale to nie wystarczyło do uzyskania ulgi. W podanym przykładzie organizacja została obrabowana w bardzo prosty i niedrogi sposób.

Koszt rejestracji nowej nazwy domeny, za pomocą której można utworzyć fałszywy adres e-mail, to zaledwie 1 USD. Jedyną zastosowaną sztuczką był ton autorytatywny, a pracownik zastosował się do niej. Ten sam atak można dziś z powodzeniem powielić w wielu organizacjach. Ponieważ raz się to powiodło, inżynierowie społeczności wykorzystają go ponownie w innym miejscu. Pracownicy finansowi są oddaleni o zaledwie 1 USD od atakującego, którego dokona ten atak. Przy tak wielu sposobach fałszowania wiadomości e-mail i szablonów wiadomości e-mail należy ostrzec personel finansowy, aby sprawdził całość adresu e-mail przy ujawnianiu niektórych informacji.

Starsi ludzie

Starsi ludzie są mniej dobrze poinformowani o atakach i często są naiwni. Prawdopodobnie będą daleko, żyją samotnie i będą chętnie słuchać ludzi, którzy wydają się potrzebować pomocy. Ich współczucie jest bezlitośnie wykorzystywane przez inżynierów społecznych każdego roku, w wyniku czego oszukani tracą miliony dolarów. Uważa się, że osoby starsze mają znaczne kwoty na koncie bezczynnie i jeśli zostaną przekonane, przekażą je tym, którzy wydają się być w potrzebie. Istnieje wiele sposobów wykorzystywania osób starszych, a my przyjrzymy się dziesięciu najczęstszym:

Medicare. ubezpieczenie: zwykle dzieje się tak w Stanach Zjednoczonych, ponieważ seniorzy, którzy przekroczyli wiek 65 lat, kwalifikują się do ubezpieczenia Medicare. Dlatego inżynier społeczny nie musi przeprowadzać żadnych badań na ten temat, jeśli może stwierdzić, że cel ma ponad 65 lat, Medicare będzie łatwą drogą do wykorzystania celu. Zazwyczaj inżynierowie społeczni nazywają się udawanymi przedstawicielami Medicare i proszą osoby starsze o podanie im swoich danych osobowych, a czasem proszą o pieniądze. Gdy otrzymają informacje o osobach starszych, mogą obciążyć Medicare i uzyskać z tego pieniądze. Czasami inżynierowie społeczni również zwracają się do osób starszych i żądają od nich pieniędzy na odnowienie rzeczy, takich jak nieistniejące subskrypcje. Sprawiają, że ofiary zobowiązują się do płacenia kwot przez długi czas, zanim odkryje się oszustwo.

Fałszywe leki w Internecie są inżynierowie społeczni, którzy sprzedają podrobione leki osobom starszym, które rzekomo leczą wiele specjalnych chorób. Inżynierowie społecznościowi używają określonych słów kluczowych, aby uzyskać swoje cele na swoich stronach internetowych. Stamtąd przekonują ich, że muszą używać tych leków przez dłuższy czas, podczas gdy w rzeczywistości leki te nie zapewniają żadnej pomocy i czasami mają negatywny wpływ. Starsi ludzie chcą mieć nadzieję, że jeśli wezmą narkotyki, wszystkie choroby, o których mówiono, że zostaną wyleczone. Inżynierowie społeczni sprzedają im tę nadzieję poprzez fałszywe narkotyki.

Pogrzeby: Oczywiście osoby starsze są bliżej granic wieku niż ktokolwiek i dlatego czasami będą chcieli zaplanować, co się stanie po ich śmierci. Inżynierowie społeczni nigdy nie sprzedają im nieistniejących pakietów na te wysyłki. Czasami inżynierowie społeczni wykorzystają zmarłego, aby uzyskać pieniądze od ich rodzin. Jest jeszcze jedna szczególnie smutna sztuczka, której używają, gdy przechodzą przez nekrologi lub nawet biorą udział w pogrzebach tylko po to, by zebrać szczegółowe informacje o

pogrążonej w smutku rodzinie. Następnie skontaktują się z rodziną i wyłudzą od nich pieniądze, aby uregulować nieistniejące długi zmarłego

Produkt przeciw starzeniu się: to znowu jest w linii do sprzedawania starszym ludziom nadziei, w których mówi się im, że mogą zachować młodość i piękno, jeśli przyjmą jakieś leki. W końcu potrzeba pozostania młodym jest dość paląca, kto nie chciałby wyglądać na 40 lat po 60 latach? Inżynierowie społeczni będą mieli szereg leków, które obiecają osobom starszym, aby nadać im młodzieńczy wygląd. Skuteczny inżynier społeczny został aresztowany i skazany w Arizonie za prowadzenie tego rodzaju oszustwa, ale nie wcześniej niż w ciągu roku zarobił ponad 1,5 miliona dolarów na osobach starszych. Wciąż jest wielu sprzedawców, którzy oferują te leki i kremy przeciw starzeniu się osobom starszym, a ze względu na ich przekonujący charakter zarabiają mnóstwo gotówki. Niektóre z tych leków są nie tylko nieprzydatne, są toksyczne, a zatem prowadzą do bardziej pomarszczonej skóry.

Oszustwa telefoniczne: Seniorzy statystycznie dokonują podwójnej liczby zakupów telefonicznych niż średnia dokonana przez inne grupy. Kupują wiele rzeczy za pośrednictwem telefonów, ale są one wykorzystywane przez inżynierów społecznych do ich wykorzystania. Inżynierowie społeczni sprzedają i wystawiają rachunki osobom starszym, których nigdy nie otrzymają. Istnieją również inne podejścia, w których inżynierowie społeczni proszą o pilne przekazanie pieniędzy, ponieważ krewny przebywa w szpitalu i potrzebuje pieniędzy. Jeśli inżynier społeczny poda nazwisko prawdziwego krewnego, osoba starsza będzie bardziej niż przekonana i pośpiesznie wyśle pieniądze.

Oszustwa internetowe: W Internecie jest wielu starszych ludzi, którzy nie są świadomi niebezpieczeństw, które się w nich czają. Młodsi ludzie często zauważają oszustwo i nie zakochują się w nim, ale osoby starsze nie mają tyle szczęścia. Istnieje powszechne oszustwo internetowe uruchamiane przez adware, które wyświetla w oknie podręcznym wyskakujące okienko, w którym urządzenie zostało przeskanowane i wykryło złośliwe oprogramowanie. Osoba starsza będzie bardzo zaniepokojona tym odkryciem i będzie gotowa zrobić wszystko, aby się tym zająć. Dlatego seniorzy często klikają podane linki i wnoszą opłaty za usługę sprzątania, z której atakujący będzie je dalej zbierał. Istnieje również oszustwo prowadzone przez strony, które udają, że oferują bezpłatne pobieranie programów. Gdy dana osoba odwiedza witrynę, istnieją trzy lub cztery przyciski pobierania, z których większość jest złośliwych. Po kliknięciu poprosi starszą osobaę, aby wprowadzić swój numer telefonu, z którego będą pobierane opłaty za pobieranie. Naliczane są opłaty, wysyłany jest kod, ale pobieranie nigdy się nie kończy lub nie prowadzi do pobrania żądanego pliku.

Programy inwestycyjne: Osoby starsze osiągną pewne oszczędności na emeryturze, aby po przejściu na emeryturę mieć coś do wydania na inwestycje. Inżynierowie społeczni są zawsze blisko, aby zapewnić im idealne możliwości inwestycyjne. Te plany inwestycyjne będą brzmiały wyjątkowo dobrze tam, gdzie będą szalone zwroty i minimalne wymagania dotyczące zarządzania. Zwykle są to piramidy, w których celom nakazuje się dokonać znacznych inwestycji początkowych i po prostu czekać, aż pieniądze zaczną płynąć wstecz, ale nigdy tego nie robi. Schematy piramid są przedstawiane w taki sposób, aby wyglądały zachęcająco, a naturalną ludzką chciwością jest zdobywanie większej ilości zasobów, które wiążą osoby starsze w tej pułapce.

Oszustwa związane z hipoteką: inżynierowie społeczni wykorzystują najbardziej prawdopodobny scenariusz, że osoby powyżej pewnego wieku będą w większości mieszkały we własnych domach. Starsi ludzie najprawdopodobniej kupią swoje domy, a inżynierowie społeczni nie zawahają się skorzystać z tego. Mogą zacząć wysyłać spersonalizowane listy rzekomo urzędników państwowych, którzy chcą ponownie ocenić wartość domu i jego obciążeń podatkowych. Następnie zażądają opłaty, po której, po jej wypłaceniu, znikną.

Loterie: to skomplikowane oszustwo, które jest zwykle skierowane do osób starszych i jest zaskakująco skuteczne. Inżynier społeczny zadzwoni i wyjaśni im, że wygrali na loterii i że otrzymają czek z ogromnymi kwotami pieniędzy, które mogą zdeponować w swoich bankach. Jednak między celem a czekiem nakładane są pewne ograniczenia, a następnie wprowadza się pewne opłaty. Inżynier społeczny może powiedzieć, że rząd nałożył określony procent podatku, który musi zapłacić cel, lub można powiedzieć, że niektóre opłaty powinny być zapłacone, aby umożliwić bezpieczny transport czeku do celu. Z powodu emocji związanych z wygrywaniem ogromnych ilości pieniędzy, cel prawie nie pomyśli dwa razy o wysłaniu tych opłat. Inżynier społeczny może omijać cel przez znaczną ilość czasu i zarabiać dużo pieniędzy.

Oszustwo na wnuczka: Jest to nowy rodzaj oszustwa, którego celem są zamożni dziadkowie, o których uważa się, że mają dobre serca. Inżynier społeczny odbierze telefon, zadzwoni do celu i powie, aby zgadł, który dzwoni do niego wnuk. Po wielu przypuszczeniach inżynier społeczny udaje, że jest jedną z wymienionych osób i próbuje dogonić cel . Po krótkiej dyskusji inżynier społeczny wprowadza pewną sytuację, w której się znajduje i pilnie potrzebuje pieniędzy. Może to być rachunek medyczny, wypadek, eksmisja z powodu braku opłaty za czynsz lub potrzeba gotówki na naprawę samochodu na osieroconym pojeździe. Inżynier społeczny, aby zamaskować swoje ślady, mówi celowi, aby nie informował rodziców, że poprosili o takie pieniądze. Osoba starsza wyśle pieniądze, a inżynier społeczny będzie dzwonił za każdym razem pod pretekstem wnuka.

Życzliwi

Nie do pomyślenia jest to, że ktoś chciałby czerpać zyski z katastrofy, ale niestety inżynierowie społeczni są na tyle bez serca, aby to zrobić. W wielu przypadkach, takich jak zamachy bombowe i huragany, inżynierowie społeczni utworzą własne fundacje charytatywne. Będą reklamować to ludziom i zachęcać ich do wysyłania pieniędzy, aby można je było wykorzystać na pomoc ofiarom. Wydaje się, że to dobry powód, tyle że pieniądze nie trafiają do ofiar, a raczej w kierunku wzbogacenia kilku inżynierów społecznych. Do czasu odkrycia oszustwa i odradzenia ludzi i przekazywania darowizn, inżynierowie społeczni mogliby zarobić miliony dolarów. Było to szczególnie duże wyzwanie podczas trzęsienia ziemi o sile 7,0 stopnia na Haiti. Wiele fałszywych organizacji charytatywnych założono online i reklamowano ludziom. Dużo pieniędzy trafiło do kieszeni kilku osób, a nie zamierzonych ofiar:

Porady

Wskazówki dotyczące kierowania i ponownego rozpoznania są następujące:

* Nigdy nie udostępniaj ważnych informacji w mediach społecznościowych

* Nigdy nie używaj ważnych haseł

* Nigdy nie udostępniaj więcej niż druga osoba musi wiedzieć

* Wiedz co mówić, kiedy mówić i jak mówić

* Pamiętaj, że nie ma czegoś takiego jak moje konto w mediach społecznościowych

Podsumowanie

Inżynierowie społeczni szczególnie lubią ofiary, na które celują. Cele są wybierane po dokonaniu oceny tego, co można od nich ukraść i jak łatwo można to zrobić. Tu omówiono wiele celów, które są preferowane przez inżynierów społecznych ze względu na role, które pełnią, bogactwo, które posiadają, lub łatwość, z jaką mogą zostać oszukani. Po raz pierwszy przyjrzeliśmy się bankom i zwrócili uwagę na luki, które można wykorzystać. Podsumowując, podano przykład profesjonalnego rabusia

bankowego, który podkreśla sposoby, które wykorzystują do kradzieży danych z tych instytucji. Przeanalizowano również włamania występujące w starych organizacjach, które sprawiają, że są łatwym celem dla inżynierów społecznych. Szczególną uwagę zwrócono na trzy typy pracowników organizacyjnych, którzy są głównymi celami inżynierów społecznych - personelu IT, personelu działu finansów i kadry kierowniczej. Kolejnym celem, na który celują inżynierowie społeczni ze względu na łatwość, z jaką można ich oszukiwać, są osoby starsze. Dziesięć typowych sposobów ich wykorzystania przez inżynierów społecznych zostało przedyskutowanych. Wreszcie, kwestia wykorzystania życzliwych osób została omówiona na dobrym przykładzie z trzęsienia ziemi na Haiti. Ważne jest, aby pamiętać, że inżynierowie społeczni będą atakować o wiele więcej osób. Omawiane są wspólne cele, które zwykle wybierają inżynierowie społeczni. Omówiono najczęstsze cele inżynierów społecznych i wyjaśniono powody, dla których często są wybierani. Niektóre z nich, takie jak personel IT, są ukierunkowane ze względu na poziom dostępu i kontroli, jaką mają do poufnych danych organizacyjnych i komunikacji wewnętrznej. Kierownictwo było omawiane jako cele, ponieważ przedstawiają dwa zestawy celów w jednym, własne dane osobowe i dane swoich organizacji. Osoby starsze zostały omówione jako cele ze względu na łatwość, z jaką można je przekonać do podjęcia pewnych działań. Ważną uwagę do zapamiętania w tym rozdziale jest to, że istnieje wiele innych celów, w tym ciebie. Inżynier społeczny nie zawahałby się celować w organizację lub osobę odrębną od omawianych. Dlatego każdy powinien zachować najwyższą ostrożność, aby zapobiec wykorzystaniu. Następny rozdział poświęcony będzie wzbudzeniu. Ludzie będą chcieli mieszkać w bezpiecznej strefie, dlatego inżynierowie społeczni muszą dysponować sztuczkami, aby skłonić ich do niebezpiecznej ścieżki.