Zapobieganie i łagodzenie

Poprzednie części podkreślały niebezpieczeństwo związane z inżynierią społeczną. Wyjaśniono wiele sztuczek i technik stosowanych w inżynierii społecznej, a także narzędzia użyte do przeprowadzenia ataku. Techniki te zostały przedstawione jako tak skuteczne i potężne, ale cele są tak słabe, że zastanawia się, czy istnieje jakakolwiek szansa na walkę z inżynierią społeczną. Rzeczywistość jest taka, że z powodu braku gotowości wielu osób do tego rodzaju ataku szanse na ataki inżynierii społecznej są niewielkie. Jest to główny powód, dla którego organizacje inwestują w odzyskiwanie danych po awarii i reagowanie na nie, ponieważ istnieje niebezpieczeństwo włamania się do ich użytkowników. Jednak sytuacja nie jest beznadziejna. Przygotowani pracownicy i osoby mogą łatwo zidentyfikować i udaremnić ataki inżynierii społecznej. Ta część skupi się na tym, w jaki sposób ataki socjotechniki mogą być chronione przed atakami socjalnymi i ograniczane przez nie. Omówi to w następujących tematach:

* Nauka rozpoznawania ataków inżynierii społecznej

* Łagodzenie ataków inżynierii społecznej

Nauka rozpoznawania ataków socjotechniki

Aby móc zapobiegać atakom inżynierii społecznej i łagodzić je, należy umieć je zidentyfikować. Niezbędne jest zrozumienie wzorców i postępu próby inżynierii społecznej. Używanie niektórych wyrażeń, mowy ciała i wyrażeń podczas rozmów powinno być w stanie wywołać alarm, jeśli mają one na celu spowodowanie, że użytkownik padnie ofiarą inżynierii społecznej. Ponieważ osoby atakujące spędzają czas na szkoleniu, jak zdobyć swoje cele, zadaniem tych obiektów jest stworzenie kultury świadomości bezpieczeństwa. Firmy powinny upewnić się, że ich pracownicy mają zaszczepioną kulturę. Pracownicy organizacji zachowują się nieufnie wobec bezpieczeństwa, ponieważ wiedzą, że jeśli dane zostaną skradzione przez hakerów, nie będą oni bezpośrednimi ofiarami. Istnieje również fałszywe przekonanie, że zadaniem działu IT jest wprowadzenie wszystkich środków bezpieczeństwa, aby zapobiec wszelkiego rodzaju włamaniom, nawet tym, w których zmusza się pracowników do udzielania poufnych informacji.

Poszczególni użytkownicy nie rozpoznają zagrożeń, z którymi ciągle się spotykają w mediach społecznościowych i rozwijają tę kulturę bezpieczeństwa dopiero, gdy padli ofiarą. Jeśli zostanie skradziony numer ubezpieczenia społecznego lub zhackowane konto e-mail, poważnie podchodzą do kwestii bezpieczeństwa.

Oto niektóre sposoby identyfikowania prób inżynierii społecznej na różnych platformach:

E-maile

E-maile od przyjaciela, efekt haczyka śnieżnego pojawia się, gdy hakerzy skutecznie zhackują twoje konto e-mail. Hakowanie może odbywać się poprzez profilowanie hasła lub wysłanie sklonowanej witryny logowania e-mail do ofiary. Gdy hakerzy uzyskają dostęp do wiadomości e-mail ofiary, mogą wykorzystać ją do wykorzystania swoich przyjaciół. W oparciu o raporty z inżynierii społecznej, poniżej wymieniono niektóre rodzaje wiadomości mających na celu wykorzystanie przyjaciół ofiary za pośrednictwem poczty elektronicznej:

* E-maile zawierające linki: inżynierowie społeczni są przekonani o sile przyjaźni i związanym z nią zaufaniu. Jeśli wyślą link do przyjaciela ofiary, zachęcając go do kliknięcia, ciekawość i zaufanie odegrają rolę w uzyskaniu nowego celu kliknięcia linku. Łącze może prowadzić do złośliwej witryny, która instaluje złośliwe oprogramowanie na swoim urządzeniu. To złośliwe oprogramowanie może ukraść zapisane dane logowania w przeglądarkach lub rozpocząć rejestrowanie kluczy naciśniętych na tym

komputerze w celu zebrania danych logowania. Skradzione informacje można wykorzystać do zaatakowania innych przyjaciół w ten sam sposób.

* E-maile zawierające treść do pobrania: możliwość celu do pobierania załączników e-mail i otwieranie ich znacznie się poprawia, jeśli uważają, że zostały wysłane przez osobę godną zaufania. Pliki PDF o nazwach kuszących zostaną pobrane i otwarte przez nieświadomych użytkowników, którzy uważają, że ich przyjaciele nie mogą im zaszkodzić. Można użyć innych typów plików. Spakowane filmy, dokumenty i pliki audio nadal mogą załatwić sprawę. Gdy cel otwiera te pliki, złośliwe oprogramowanie jest ładowane na ich komputer. W poprzednich częściach omawiano niektóre exploity Metasploit, które mają zdolność generowania szkodliwych plików, które są gotowe do wysłania pocztą e-mail.

* E-maile z prośbą o pilną pomoc: Pilność jest powszechnym wskaźnikiem inżynierii społecznej. Inżynierowie społeczni nigdy nie chcą, aby cel miał wystarczająco dużo czasu na przetworzenie nowych informacji, jeśli mogłoby to ujawnić ich atak. Dlatego, gdy tylko będzie to możliwe, zostanie wykorzystana pilność. Gdy inżynierowie mają kontrolę nad adresem e-mail, mogą go łatwo użyć do wyłudzenia pieniędzy od użytkowników poczty e-mail, którzy wcześniej kontaktowali się z ofiarą. Mogą poprosić o natychmiastowe przesłanie pieniędzy na określone konto, aby można było zapłacić rachunek lub zapłacić niektóre grzywny, aby przyjaciel został zwolniony lub zwolniony. Oszustwo zostaje odkryte dopiero po wysłaniu pieniędzy.

* E-maile z prośbą o darowizny: Współczucie jest słabością obecną i można ją wykorzystać u większości ludzi. Inżynierowie społeczni są ekspertami w tworzeniu pretekstów, które budzą sympatię ludzi, powodując, że oferują pomoc bez zastanowienia się. Dlatego wiadomości zmuszające do przekazania darowizn na rzecz nieznanych fundacji charytatywnych lub od nieznanych osób proszących o pieniądze na inne cele charytatywne mogą okazać się próbami inżynierii społecznej. Dlatego wszelkie prośby o darowizny, zwłaszcza jeśli są pilne, należy traktować ostrożnie.

Próby phishingu

Phisherzy są znani z wysyłania dużej ilości e-maili z prośbą o pieniądze od swoich celów lub niektóre poufne informacje. Ze względu na ich liczbę, tylko nieliczni potrafią sprawić, że ich cele wysyłają pieniądze lub informacje, o które proszą. Istnieje inny rodzaj wiadomości phishingowych, które zwykle odnoszą większe sukcesy. Są to wiadomości phishingowe dostosowane do rodzaju osób, które mają je otrzymywać. Są używane w typie ataku phishingowego zwanego phishingiem typu spear. Istnieje kilka cech, które mogą pomóc w identyfikacji wiadomości e-mail typu phishing. Są to:

* Wiadomości wyjaśniające problem: niektóre próby socjotechniki polegające na wyłudzaniu informacji zwykle próbują uwięzić swoje cele za pomocą wiadomości wymagających weryfikacji niektórych informacji. Podaje się link do celu wyjaśniającego mu, że muszą wypełnić pewne informacje w danym formularzu. Chociaż linki mogą prowadzić do stron, które wydają się wiarygodne, są to w większości klonowane witryny z dokładnym logo i treścią zaufanych witryn. Zazwyczaj strony te obejmują usługi płatności online, strony mediów społecznościowych i dostawców usług e-mail. Ponieważ wszystko jest profesjonalnie dobrze ułożone, cel ostatecznie przekazuje poufne informacje oszustom. Dopiero po podaniu tych danych logowania można zdać sobie sprawę, że tak naprawdę nie logują się na stronie internetowej. W tym momencie jest już za późno, aby odwrócić swoje działania. Niektórzy hakerzy przekierowują użytkowników do legalnych witryn po kradzieży danych logowania. Przeważnie użytkownicy są zmuszani do podawania poufnych informacji poprzez wykorzystanie niepożądanych konsekwencji, takich jak zawieszenie lub banowanie kont.

* Wiadomości powiadamiające o dużej wygranej finansowej: powszechną taktyką użytkowników phishingu jest mówienie im, że zarobili dużo pieniędzy lub że mają szansę bez wysiłku zdobyć ogromne

sumy pieniędzy. Oszustwa te są tak stare jak Internet, a pochodzą z oszustw księcia nigeryjskiego, które pojawiły się, gdy pojawiły się wiadomości e-mail. Inne rodzaje tego oszustwa to oszuści, którzy rzekomo są bankami, które chcą przelać na konto pieniądze przechowywane przez zmarłego krewnego, twierdzą, że dana firma daje komuś ogromną nagrodę finansową za to, że jest milionowym klientem, pieniądze wygrane z loterii lub nawet zwroty z usługi Internal Revenue Service (IRS). Tego rodzaju oszustwa podążają prawie tymi samymi sztuczkami. Podają celowi informacje o swoich rachunkach bankowych, aby przelać pieniądze. Następnie proszą o podanie bardziej poufnych danych, aby pomóc w przetwarzaniu przelewu. Mogą poprosić o potwierdzenie tożsamości poprzez podanie numeru ubezpieczenia społecznego. W pewnym momencie mogą nawet zacząć prosić o przesłanie pieniędzy, aby usunąć wąskie gardła stojące na drodze do uwolnienia pieniędzy. Ponieważ są bardzo przekonujący, atakujący często otrzymują informacje lub pieniądze, których żądają od celów. Obietnica ogromnej nagrody finansowej jest wystarczająco silna, aby skłonić ludzi do fałszywej przyczyny ścigania pieniędzy, nawet jeśli oznacza to podanie pewnych prywatnych informacji lub rozstanie się z pewną kwotą w celu pokrycia pewnych opłat w celu ułatwienia transferu.

* Wiadomości z prośbą o pomoc: Hojność i życzliwość są często wykorzystywane przez socjotechnikę. Dlatego prośby od nieznanych osób, które proszą o pomoc finansową z powodu katastrofy, której doświadczają, lub wydarzenia charytatywnego, które będą miały miejsce, należy rozpatrywać z dużą ostrożnością. Chociaż hojność nie jest niczym złym, jest to cecha ludzka, którą można niestety wykorzystać. Najlepiej jest poszukać szczegółów każdej organizacji charytatywnej, w której mówi się, aby wnieść wkład. Oszuści wykorzystują w czasie katastrofy wysyłanie wiadomości e-mail typu phishing z prośbą o przekazanie darowizn na niektóre konta bankowe, aby pomóc ofiarom katastrofy.

Jednocześnie legalne organizacje charytatywne będą również docierać do osób proszących o darowizny. Dlatego może być trudne rozróżnienie między uzasadnionymi a fałszywymi prośbami o datki charytatywne.

Przynęty

Inżynierowie społeczni potrafią wabić swoje cele. Są skuteczni w znajdowaniu czegoś, co może zwichnąć ich cele. Znajdują coś, czego chcą cele i chętnie przyjmą przynętę. Jest to powszechna metoda ataku na witryny peer-to-peer, szczególnie tam, gdzie ludzie pobierają pirackie treści. Za nielegalnie pobranymi treściami chronionymi prawem autorskim kryje się złośliwe oprogramowanie, które infekuje komputery użytkowników, bez ich zauważania. Szacuje się, że w 2015 r. Zzłośliwe oprogramowanie zarażało 12 milionów komputerów miesięcznie. Torrenty są powszechnym sposobem bezpłatnego pobierania treści premium i programów, naruszając w ten sposób prawa dotyczące własności, takiej jak filmy, gry i programy. Szacuje się, że z około 1000 stron torrentowych jedna trzecia będzie pobierać złośliwe oprogramowanie przez nieświadomych użytkowników. Pliki zawierające złośliwe oprogramowanie to pliki o wysokim popycie. Pojawiły się doniesienia, że kiedy EA Sports wypuszcza nową wersję gry FIFA, hakerzy zalewają strony torrentów fałszywymi linkami do pobrania, dzięki czemu użytkownicy mogą pobierać gigabajty złośliwego oprogramowania na swoje komputery. Pliki o dużym natężeniu ruchu związanego z wyszukiwaniem są często używane i nękane złośliwym oprogramowaniem, ponieważ osoby atakujące wiedzą, że będą ludzie próbujący je pobrać. Niektóre z tego złośliwego oprogramowania są wykorzystywane do kradzieży danych z komputerów, podczas gdy inne otwierają połączenie zaplecza, umożliwiając hakerom pobranie więcej złośliwego oprogramowania na komputery ofiary. Dane ofiar można sprzedawać na czarnym rynku, a ich komputer można zaciągnąć do armii botnetów. Z tego rodzaju ataku mówi się, że cyberprzestępcy zarabiają ponad 70 milionów dolarów rocznie na swoich ofiarach.

Odpowiadanie na niezadane pytania

Czasami inżynierowie społeczni wymuszą utworzenie określonego pretekstu, aby skorzystać z możliwości użytkownika. Jednym z tych sposobów jest wycofanie się z obsługi klienta dużej firmy, która ma miliony użytkowników, którzy odpowiadają na zadane pytanie. Mogą udawać, że pochodzą z Gmaila, PayPala lub IRS, między innymi organizacji, które generalnie mają duży ruch i prawie każdy ma przy nich konto. Gdy kierują reklamy do użytkownika, udają, że oferują możliwość uzyskania bezpłatnej usługi lub produktu. Skrypt do ataku jest podobny do omawianego w poprzednim ataku. Cyberprzestępcy powiedzą celowi, aby się uwierzytelnił, logując się do systemu za pomocą określonego linku. Poczynią niezbędne przygotowania, aby link prowadził do strony o podobnym wyglądzie i działaniu jak prawdziwa strona internetowa. Jeśli jest to PayPal, wszystko zostanie ułożone tak, jak na oficjalnej stronie PayPal.

Tworzenie nieufności

Aby pojawiać się jako bohaterowie i rozwiązywacze problemów, inżynierowie społeczni mogą planować wzbudzić nieufność i prawdopodobnie siać spustoszenie, aby jeden z nich mógł pojawić się jako bohater. Nieufność może powstać między celem a przedstawicielem firmy, instytucją bankową, a nawet firmą ubezpieczeniową. W życiu celu istnieje wiele ścieżek, w których chaos można opanować na scenie. Kiedy pojawi się nieufność i prawdopodobnie chaos, inżynier społeczny wkroczy i spróbuje rozwiązać problem. Będą grać razem, oraz na koniec, cel będzie miał zaufanie do inżyniera społecznego jako bardzo zaradnej osoby zdolnej do zakończenia konfliktów. Kiedy cel zaczyna ufać inżynierowi społecznemu, zaczynają się wymuszenia i manipulacje. Mogą poprosić o podanie danych logowania, aby kontynuować realizacji sprawy. Mogą również poprosić o pomoc finansową, która pomoże im poradzić sobie z niefortunną sytuacją, z którą mają do czynienia w życiu prywatnym. Z wrażeniem, że inżynier społeczny jest osobą godną zaufania, cel może po prostu się spełnić.

Inne znaki

Rozważ inne znaki w następujący sposób:

Słaba gramatyka: niektórzy inżynierowie społeczni pochodzą z krajów, które nie komunikują się w języku danego kraju jako głównym języku. Dlatego mają trudności z językiem, co widać w e-mailach, które piszą, a nawet w ich głosach. Jeśli ktoś otrzyma wiadomość e-mail z prośbą o pomoc, oferującą ogromne korzyści finansowe lub z prośbą o informacje zawierające błędy gramatyczne, istnieje duże prawdopodobieństwo, że jest to próba inżynierii społecznej.

Postawa: Niektórzy inżynierowie społeczni twierdzą, że są przedstawicielami niektórych renomowanych organizacji i instytucji. Personel obsługi klienta powinien być uprzejmy wobec klientów i odpowiadać na pytania, które mogą mieć. Jeśli podczas monitorowania poufnego połączenia rzekomy agent obsługi klienta wykaże oznaki niegrzeczności lub agresji, istnieje prawdopodobieństwo, że jest inżynierem społecznym. Gniewają się na ludzi, którzy próbują odkryć swoje sztuczki lub kwestionują niektóre z rzeczy, które oczekują, że zostaną zrobione. Jeśli klient odmawia odczytania żądanego hasła PayPal, a osoba żądająca takich informacji zaczyna być agresywna, oznacza to, że inżynier społeczny wścieka się na cel.

* Nieformalne wnioski: inżynierowie społeczni czasami przedstawiają się jako pochodzący z dużych firm. Są jednak sprawcami bardzo nieformalnych próśb. Agent obsługi klienta PayPal nie może w żadnym wypadku poprosić klienta o odczytanie hasła, którego użył ostatnio do zalogowania się na swoje konto. Agenci PayPal nie będą również żądać od użytkowników przesyłania danych logowania za pośrednictwem kanałów takich jak Facebook. Dyrektor generalny nie zacznie prosić księgowych o przesłanie pieniędzy na swoje konto osobiste, które zostaną później zwrócone. Nieformalne wnioski to

wskaźniki, że nie są one składane przez uprawnione podmioty. Niezwykłe komplementy: inżynierowie społeczni zwykle chcą zachęcić cel do spełnić niektóre podane prośby.

* Inżynieria społeczna: Na przykład była prośba do celu o podanie danych logowania na stronie takiej jak Facebook. Po przekazaniu wiadomości e-mail inżynier społeczny może być zbyt niespokojny i zacząć komplementować cel oraz zachęcać go do przesłania pozostałej informacji. Ponadto, istnieją słabi inżynierowie społeczni, którzy wydają się nie mieć racji w procesie budowania relacji. Dlatego trzymają komplementując cel w nadziei na zbliżenie się do zamierzonej ofiary. Inżynierowie społeczni mogą udzielać komplementów w stosunku do bardzo trywialnych zadań.

* Nie posiadaj ważnego numeru zwrotnego: inżynierowie społeczni używają różnych numerów, jeśli ich ataki mają być wykonywane głosem. Dlatego, gdy kontaktują się z celem, mogą nie być ponownie osiągalni pod tym samym numerem. Częstym czynnikiem odstraszającym dla inżynierii społecznej było anulowanie połączenia telefonicznego, a następnie oddzwanianie za pośrednictwem oficjalnie znanych kanałów.

* Pośpiech: Niektórzy inżynierowie społeczni są zawsze w ruchu, próbując znaleźć nowe cele. Dlatego cenią sobie czas. W innych przypadkach inżynierowie społeczni chcą, aby defraudacja nastąpiła szybko, zanim cel zacznie podejrzewać. Dlatego jedną ze znanych taktyk stosowanych przez inżynierów społecznych jest pośpiech. Zawsze chcą, aby rzeczy były podejmowane nieco szybciej, aby atakujący mógł również szybko się poruszać.

Łagodzenie ataków inżynierii społecznej

Rozmowy telefoniczne

Rozmowy telefoniczne szybko stały się powszechnymi metodami inżynierii społecznej. Inżynierowie społeczni polegają na technikach fałszowania identyfikatora dzwoniącego i natychmiastowości telefonu, aby cele były zgodne z żądaniami bez przestrzeni do myślenia. Organizacje odczuwają wpływ telefonicznych ataków socjotechnicznych, w których pracownicy IT otrzymują żądania od dzwoniących osób, które podają się za pracowników organizacji, którzy zapomnieli hasła. Podobnie jak w wielu organizacjach, technicy zresetują hasło i powiedzą dzwoniącemu nowe hasło, nawet bez sprawdzenia, czy dzwoniący jest tym, za kogo się podaje. Inżynierowie społeczni również losowo atakują członków społeczeństwa, którzy twierdzą, że pochodzą z wiarygodnych organizacji, takich jak IRS, i proszą o poufne informacje. Aby zmniejszyć ryzyko inżynierii społecznej poprzez rozmowy telefoniczne, należy przestrzegać następujących wskazówek:

* Weryfikuj osoby dzwoniące: Prostą strategią ograniczania ryzyka jest weryfikacja osób dzwoniących przy użyciu informacji, które by wiedziały, gdyby były legalne. W przypadku połączeń od osób, które rzekomo pochodzą z urzędu skarbowego, można zapytać o kwoty złożone w poprzednim zeznaniu. W przypadku banków można poprosić dzwoniącego o zweryfikowanie ostatniej kwoty obciążającej konto. Są szanse, że uprawnieni dzwoniący będą mieli dostęp do systemów organizacji, o których mówią, że pracują i nie będą mieli problemu z odzyskaniem takich informacji. Inżynierowie społeczni będą wyschnięci w obliczu takich pytań i spróbują ich uniknąć.

* Porzucanie połączenia i oddzwanianie za pomocą legalnego numeru: Prosta poprawka, z której korzysta wiele osób, aby poradzić sobie z denerwującymi IRS i oszustami bankowymi dzwoniącymi i twierdzącymi, że pochodzą z dużych wiarygodnych organizacji, przerywa połączenia i dzwoni bezpośrednio do tych dużych wiarygodnych organizacji. Jeśli cel to zrobi, zostanie poinformowany, czy istnieje problem, który spowodował wykonanie połączenia. Inżynierowie społeczni ponownie zostaną

ujawnieni, ponieważ organizacje, dla których twierdzą, że pracują, odrzucą ich roszczenia. Ta sztuczka pozwoliła ludziom zaoszczędzić dużo pieniędzy i stresu.

* Zgłaszanie podejrzanych połączeń: gdy ktoś może ujawnić inżyniera społecznościowego próbującego oszukać za pośrednictwem połączeń telefonicznych, osoby takie powinny zostać zgłoszone odpowiednim władzom. Doprowadzi to do sprawdzenia numeru, aby dowiedzieć się, zarejestrowana osoba lub ostatnia lokalizacja, z której został użyty. Pomaga władzom rozprawić się z siecią socjotechniczną, która często wiąże się z oszustwami telefonicznymi. Sieć inżynierów społecznych IRS została niedawno aresztowana w Indiach i mówiono, że zgromadzili miliony dolarów od Amerykanów. Dlatego zgłaszanie podejrzanych połączeń pomaga upewnić się, że złośliwi rozmówcy nie odniosą sukcesu w oszukiwaniu i wyłudzaniu ludzi.

E-maile

Powszechnym sposobem inżynierii społecznej jest używanie wiadomości e-mail, ponieważ inżynier społeczny może dotrzeć do wielu osób przy użyciu ograniczonych zasobów. Najbardziej niebezpieczne ataki to te, które obejmują wiadomości e-mail ze złośliwymi załącznikami i linkami, które prowadzą do zainfekowania przeglądarki złośliwym oprogramowaniem, które kradnie dane lub przejmuje kontrolę nad urządzeniem. Inne rodzaje e-maili socjotechnicznych zawierają linki do sklonowanych witryn, w których użytkownicy tracą swoje dane uwierzytelniające, gdy próbują się zalogować. Tego rodzaju wiadomości e-mail są nadal powszechnie używane, a ludzie nadal padają ofiarą. Istnieją pewne zabezpieczenia, które ludzie powinni stosować, aby uniknąć bycia ofiarami tego rodzaju ataków socjotechniki, a niektóre z nich są następujące:

* Unikaj ujawniania danych osobowych lub poświadczeń w wiadomościach e-mail: W większości przypadków banki, rządy, firmy ubezpieczeniowe i wiele innych renomowanych instytucji nigdy nie zażądają od użytkownika przesłania prywatnych informacji za pośrednictwem adresów e-mail i nie będą też prosić o przesłanie poświadczeń na adres ich konta online. Gdy dostaje się takie żądania za pośrednictwem wiadomości e-mail, najlepiej traktować je jako próby ataku i zignorować lub usunąć.

* Unikaj pobierania załączników od nieznanych nadawców: zawsze istnieje ryzyko pobrania złośliwego oprogramowania z załączników e-mail, dlatego użytkownicy powinni zachować przy tym dużą ostrożność. Powinny być bardzo zaniepokojone przy pobieraniu załączników od nieznanych nadawców, szczególnie gdy e-maile zachęcają do otwierania.

* Unikaj klikania linków lub podawania danych osobowych w połączonych adresach internetowych: Linki prowadzące do stron internetowych, które proszą użytkowników o zalogowanie się do swojego konta bankowego, służbowego, e-mailowego i mediów społecznościowych, powinny być traktowane podejrzliwie, szczególnie jeśli pochodzą z kont wątpliwych. Sklonowanych witryn lub złośliwych witryn jest mnóstwo, dlatego użytkownicy powinni zawsze zachować ostrożność w stosunku do otrzymywanych wiadomości e-mail, nawet jeśli twierdzą, że pochodzą z prawdziwych witryn.

Ataki osobiste

Inżynieria społeczna może być także atakiem osobistym, w którym inżynier społeczny bezpośrednio manipuluje celem, aby spełnić niektóre żądania. Mogą zbliżać się do ludzi w miejscach pracy, restauracjach, barach, podczas imprez firmowych i tak dalej. Prawdopodobnie przeprowadzili badania dotyczące celu i będą dokładnie wiedzieć, o co zapytać. Aby ograniczyć ataki osobiste, należy wykonać następujące czynności:

* Bezpieczeństwo fizyczne: Strażnicy powinni zawsze potwierdzać wizyty gości w organizacjach. Nigdy nie mogą narażać bezpieczeństwa organizacji z powodu przekonujących argumentów odwiedzających, do których zostali wezwani w trybie pilnym.

* Uważność: pracownicy powinni zgłaszać nieznane osoby wchodzące do wrażliwych pokoi lub biur w organizacji. Pracownicy powinni również unikać uprzejmości polegającej na wykorzystywaniu przepustek do wpuszczania nieznajomych do zabezpieczonych części miejsca pracy.

* Ostrożność: pracownicy powinni unikać pozostawiania poufnych dokumentów na biurkach. Powinni także unikać pozostawiania karteczek z poświadczeniami umieszczonymi na biurkach lub monitorach. Pracownicy powinni również blokować ekrany podczas opuszczania biurka. Zawsze istnieje ryzyko, że nieznajomy może manewrować wokół fizycznych mechanizmów kontroli i dostać się do pomieszczeń organizacji.

Audyt inżynierii społecznej

Najlepszym sposobem na ograniczenie obecnego ryzyka inżynierii społecznej w korporacjach jest przeprowadzenie audytu inżynierii społecznej. Audyt ujawnia podatności w organizacji dotyczące jej pracowników i ich podatność na próby inżynierii społecznej. Zauważono, że dyrektorzy IT i organizacje społeczeństwa obywatelskiego przeprowadzają na nich audyty organizacje ze względu na rosnącą liczbę hacków ułatwiających przez socjotechnikę. W związku z tym głównym problemem dla organizacji stało się zapewnienie, że słabości w ich praktykach użytkowników są rozumiane i ograniczane poprzez ćwiczenia użytkowników. Szkolenie użytkowników jest znacznie bardziej skuteczne, gdy znane są wady, które należy usunąć.

Audyty inżynierii społecznej sprawdzają również istniejące mechanizmy kontroli, takie jak polityki bezpieczeństwa w organizacji, oraz zgodność pracowników z nimi. Ataki inżynierii społecznej w organizacjach są głównie wynikiem naruszenia bezpieczeństwa wewnętrznego przez pracowników, którzy z natury narażają organizacje na niebezpieczeństwo. Te naruszenia bezpieczeństwa są dość powszechne i obejmują one od klikania przez pracowników linków wysłanych do nich pocztą e-mail po pracowników wysyłających pieniądze z kont firmowych do oszustów. Niektóre działania kontrolne z zakresu inżynierii społecznej, które należy przeprowadzić w organizacjach, obejmują :

* Testy świadomości bezpieczeństwa

* Testy odpowiedzi użytkowników na próby phishingu

* Odpowiedź użytkowników na dziwne żądania osób postronnych

* Odpowiedzi użytkowników na próby wejścia obcych osób do zabezpieczonych obszarów

* Testy hojności użytkowników w udzielaniu poufnych informacji o organizacji lub innych pracownikach

Podsumowanie

Omówiono sposoby zapobiegania atakom inżynierii społecznej i ich łagodzenia. Najpierw zbadano, w jaki sposób można zidentyfikować możliwe scenariusze inżynierii społecznej. Omówiono sposoby, w jakie można stwierdzić, że wiadomość e-mail ma na celu próbę manipulowania nimi. Ponieważ większość prób socjotechniki będzie podejmowana za pośrednictwem wiadomości e-mail, omówiono kwestie, które należy wziąć pod uwagę przy ocenie, czy wiadomość e-mail jest wysyłana od inżynierów społecznościowych. Omówiono również ogólne możliwe do zidentyfikowania wzorce phishingu. Podkreślono również inne znaki w ogólnej komunikacji, takie jak gramatyka, które mogą sugerować możliwe ataki socjotechniki. W rozdziale omówiono następnie, w jaki sposób użytkownicy mogą

złagodzić próby socjotechniki zorganizowane na telefony, e-maile, a także osobiście. Jako rozwiązanie dla prób inżynierii społecznej na korporacjach, rozdział omawia audyty inżynierii społecznej. Podkreślono obszary, na które audyty powinny być ukierunkowane, ponieważ są one powszechnie wykorzystywane przez inżynierów społecznych.