ATAKI SOCIAL-ENGINEERING I LOW-TECH

WPROWADZENIE.

Według mitologii greckiej Grecy pokonali Trojan w Wojnie Trojańskiej za pomocą drewnianej statui. Po bezskutecznej wojnie trwającej dekadę Grecy wycofali się ze swojej twierdzy na plaży. Za bramami Troi zostawili wielkiego drewnianego konia. Statua zmieszała trojańskich żołnierzy, ale została wprowadzona do Troi. Wewnątrz posągu ukryło się kilku greckich żołnierzy. Gdy zapadła ciemność, żołnierze wyłonili się z posągu i otworzyli bramy Troi. Armia grecka wkroczyła do Troi i zaskoczyła żołnierzy i obywateli Troi. Po oszustwie Grecja szybko wygrała wojnę. Koń trojański zbudowany przez Greków był skuteczny, ponieważ wykorzystał oszustwo, aby osiągnąć pożądany rezultat: przeniknąć do ustalonej obrony wroga. Koń trojański osiągnął to, o czym inżynierowie bezpieczeństwa informują, o bezpieczeństwie informacji. Inżynieria społeczna może być zdefiniowana jako pozyskiwanie informacji lub zasobów od ofiar za pomocą przymusu lub oszustwa. Inżynieria społeczna odnosi się do kłamstwa, oszukiwania, oszukiwania, uwodzenia, wyłudzania, zastraszania, a nawet grożenia pracownikom, aby ujawnili poufne informacje, które następnie można wykorzystać do włamania się do systemów. Inżynieria społeczna opiera się na oszukiwaniu i naruszaniu społecznych norm uczciwości i uczciwości. Podczas ataku socjotechnicznego osoby atakujące nie polegają na technologii niszczenia, na przykład skanowaniu sieci, łamaniu haseł przy użyciu brutalnej siły lub wykorzystywaniu luk w zabezpieczeniach oprogramowania. Inżynierowie społeczni działają raczej w świecie społecznym, manipulując zaufaniem lub naiwnością ludzi. Inżynieria społeczna polega zatem na manipulowaniu naturą ludzką w celu wydobycia informacji lub dostępu poprzez oszukanie ofiary. Inżynieria społeczna związana jest z atakami o niskiej technologii, które często idą w parze. Ataki o niskiej technologii są podobne do ataków socjotechnicznych, ponieważ nie wykorzystują technologii. Są to fizyczne ataki dokonywane na majątek firmy lub osoby fizycznej. Nie wszystkie ataki socjotechniczne i technologiczne dostarczą atakującym wszystkie informacje, których szukają jednocześnie. Inżynierowie społeczni będą gromadzić małe informacje, które wydają się nieszkodliwe dla osób, które je ujawniają. Inżynierowie społeczni mogą gromadzić te fragmenty informacji w pozornie losowej kolejności, ale następnie łączyć je w dane wywiadowcze, które są wykorzystywane do przeprowadzania większych ataków, które mogą być dewastujące dla bezpieczeństwa informacji, zasobów, finansów, reputacji lub przewagi konkurencyjnej organizacji. Rzeczywiście cel ataku inżynierii społecznej może być tak różnorodny, jak zastosowana metoda ataku. Rezultat jest jednak ogólnie taki sam: utrata własności intelektualnej, pieniędzy, korzyści biznesowych, wiarygodności lub wszystkie powyższe. Ataki socjotechniczne były i będą skuteczne ze względu na najsłabsze ogniwo bezpieczeństwa w organizacji: ludzi. Są ważne, ponieważ wykorzystują ludzką naturę, która jest niezmienna, a zatem wiecznie wrażliwa. W tym rozdziale przedstawiono historię ataków socjotechnicznych i ataków opartych na niskich technologiach, ich metody, nauki społeczne i ich wpływ na biznes. Ponadto obejmuje polityki wykrywania i ograniczania ryzyka dla menedżerów i funkcjonariuszy ds. bezpieczeństwa informacji w celu obrony przed atakami socjotechnicznymi i technologicznymi oraz ich łagodzenia. Cel ataku socjotechnicznego może być tak różnorodny, jak metoda ataku. Niemniej jednak rezultat dla ofiar jest zasadniczo taki sam, utrata własności intelektualnej, pieniędzy lub biznesu, wiarygodności lub wszystkich zaległych. Tutaj przedstawiono historię ataków socjotechnicznych i ataków opartych na niskich technologiach, ich metody, nauki społeczne i ich wpływ na biznes. Ponadto obejmuje polityki wykrywania i ograniczania ryzyka dla menedżerów i pracowników ochrony informacji w celu obrony przed atakami socjotechnicznymi i technologicznymi.

TŁO I HISTORIA.

Inżynieria społeczna nie jest nową taktyką ani wynalazkiem współczesnych hakerów. Termin ten ma swoje fundamenty w historii politycznej, gdy osoba lub grupa manipuluje grupą ludzi, dużą lub małą, próbując przekonać lub manipulować postawami lub przekonaniami społecznymi. Często rządy lub partie polityczne angażują się w tę praktykę. Początki współczesnego terminu sięgają II wojny światowej, a naziści rzeczywiście wymyślili ten termin. Do dziś termin ten ma negatywną konotację ze względu na swoje korzenie w historii, zwłaszcza w kontrolowanych przez nazistów Niemczech.

Niektórzy badacze uważają także, że dziedzina inżynierii społecznej obejmuje wszystko, od reklamy i nowoczesnych mediów po polityczne grupy działania. Inżynieria społeczna jest dziś bardziej znana z zastosowania jej jako techniki penetracji bezpieczeństwa. Oszustwo było nieodłącznym elementem szpiegostwa na przestrzeni wieków. Sun Tzu napisał w V w. p.n.e.

* „Każda wojna jest podstępem".

Oszustwo - w szczególności podawanie fałszywych informacji szpiegom wroga - było integralną częścią Drugiej Wojny Punickiej między Rzymem a Kartaginą w III wieku p.n.e. Podczas Drugiej Wojny Światowej Alianci użyli „Operacji Bodyguard", aby oszukać moce Osi, aby uwierzyć, że inwazja D-Day nastąpi w innym czasie i miejscu niż jej prawdziwy harmonogram i cel. Oszustwo było integralną częścią konkurencji szpiegowskiej z kontrwywiadem między blokiem komunistycznym a Zachodem podczas zimnej wojny. Dobrze znanym przykładem inżynierii społecznej są eskapady Franka W. Abagnale'a, temat fikcyjnego filmu „Złap mnie, jeśli potrafisz". Abagnale był w stanie skutecznie podszywać się pod autorytety, w tym lekarza, pilota, adwokata i nauczyciela, mimo że był nastolatkiem. Używał także technik inżynierii społecznej, aby przekonywać i manipulować niewinnymi i dobrodusznymi osobami, aby pomóc mu w przeprowadzeniu wielu jego oszustw. Wiele technik Abagnale odniosło duży sukces i zostało dobrze zaprojektowanych. Dziś pomaga organizacjom rozpoznawać i bronić się przed takimi atakami poprzez swoje wystąpienia mówcze i doradztwo biznesowe. Jednym z najbardziej znanych inżynierów społecznych jest Kevin Mitnick. Chociaż Mitnick jest obecnie konsultantem, wykładowcą i autorem bezpieczeństwa komputerowego, jego obecną karierę poprzedziło wiele lat spędzonych jako haker komputerowy i inżynier społeczny. Od dawna zreformowany, Mitnick napisał kilka książek omawiających jego obserwacje i techniki jako hakera komputerowego. Mitnick utrzymuje, że inżynieria społeczna jest najpotężniejszym narzędziem w zestawie narzędzi hakera. Od kiedy inżynieria społeczna stała się popularną i, co ważniejsze, skuteczną techniką, jej częstotliwość stosowania wzrosła. Jednym z najbardziej widocznych przypomnień jest duża liczba ataków typu phishing i pharming. Na niektórych konwencjach hakerów kryminalnych socjotechnika stała się nawet sportem dla widzów. Podczas targów DEF CON 2012 w Las Vegas Shane MacDougall wygrał konkurs zdobywania flagi przez socjotechnikę, oszukując dyrektora Walmart w kanadyjskim sklepie, aby ujawnił każdą poufną informację wymienioną w celach konkursu. Darnell zapytał kierownika o całą logistykę fizyczną jego sklepu: wykonawcę usług porządkowych, dostawcę usług gastronomicznych w stołówce, cykl płac pracowników i harmonogramy zmian personelu. Dowiedział się, o której menedżerowie robią sobie przerwy i gdzie zwykle idą na lunch. Utrzymując stały szloch na temat nowego projektu i życia w Bentonville, Darnell zmusił kierownika do podania kilku kluczowych szczegółów na temat rodzaju używanego komputera. Darnell szybko ustalił markę i numery wersji systemu operacyjnego komputera, przeglądarki internetowej i oprogramowania antywirusowego. Inżynieria społeczna, gdy jest używana jako samodzielne narzędzie ataku, jest bardzo skuteczna. Ale to narzędzie może być używane jako część większego ataku, a nawet jako część ataku technicznego. Inżynieria społeczna jest powszechnie stosowana na początku większego, bardziej znaczącego ataku. Ważne jest, aby pamiętać, że niektóre ataki miały miejsce przez tygodnie, miesiące lub lata. Nie zawsze tak jest i tylko dlatego, że uniknięto konkretnej próby inżynierii społecznej, większy atak może nie zostać całkowicie złagodzony. Przykładem może być to, że początkowy atak nie powiódł się, ponieważ atakujący nie miał wystarczających lub dokładnych informacji do przeprowadzenia ataku. Atakujący może ponownie powrócić do inżynierii społecznej i strategii ataku o niskim poziomie technologii, aby zebrać informacje o innym, być może udanym, ataku technicznym. Chociaż organizacja może mieć najlepszą na świecie zaporę ogniową, system wykrywania włamań i narzędzia do zarządzania ryzykiem, osoba atakująca może skorzystać z inżynierii społecznej, aby obejść te zabezpieczenia techniczne. Atakujący nie zostanie zatrzymany przez najlepszą obronę techniczną, jeśli będzie w stanie wydobyć prawidłową nazwę użytkownika i hasło od niczego niepodejrzewającego pracownika. Gdy osoba atakująca uzyska te informacje, może być wystarczająca do przeprowadzenia masowego ataku na systemy informatyczne organizacji - być może nie zostanie wykryta. Przestępcy komputerowi byli w stanie zastosować czysto socjotechnikę i techniki ataku low-tech, nie polegając na żadnej poważnej

technologii, aby spowodować szkody na dużą skalę również w organizacji. Czynność tak prosta, jak usunięcie odrzuconych, potencjalnie szkodliwych informacji ze śmietnika i przesłanie ich do lokalnych mediów, może spowodować znaczne uszkodzenie wizerunku organizacji. Akt ten może być częścią większej kampanii lub operacji grupy osób poszukujących działań politycznych lub społecznych przeciwko organizacji. Przykładem tego jest ostatnio Home Box Office (HBO) z udziałem grupy obywateli, która rutynowo zbierała śmieci z okręgowych centrów wyborczych i urzędów miasta, aby zebrać dowody, które mogliby przedstawić mediom w celu udowodnienia oszustwa wyborcy. Dokumenty, które zostały niewłaściwie usunięte, miały niezwykle negatywne konsekwencje dla urzędników wyborczy

METODY INŻYNIERII SPOŁECZNEJ

Ataki socjotechniczne mogą przybierać różne formy, a doświadczeni inżynierowie społeczni mogą bardzo szybko zmieniać metody ataku, aby odnieść sukces. Podstawową zasadą większości ataków jest pretekstowanie, które jest zdefiniowane jako „zbieranie informacji… pod fałszywymi pozorami". Dwie odrębne metodologie stosowane są podczas ataków socjotechnicznych, podszywania się i uwodzenia. Podstawą większości ataków jest jedna z tych dwóch metod. Niektóre ataki o niskiej technologii, które nie wymagają kontaktu z ludźmi, są wyjątkami. Cele ataków socjotechnicznych również różnią się znacznie. W zależności od stopnia złożoności ataku lub od tego, ile wiedzy ma osoba atakująca, pomoże określić cel ataku. Jednak w wielu przypadkach atak socjotechniczny jest atakiem szansy, a ofiara zostanie losowo wybrana. W niektórych dobrze zaplanowanych atakach konkretny cel może zostać zidentyfikowany jako ofiara

PODSZYWANIE

Podszywanie się jest definiowane jako udawanie kogoś innego i jest to jedna z najpopularniejszych metod stosowanych przez inżynierów społecznych. Inżynierowie społeczni mogą wykorzystywać ataki z zakresu podszywania się pod inne osoby, aby atakować pracownika na dowolnym poziomie w docelowej organizacji. Mogą udawać prawdziwą, nazwaną osobę lub udawać, że pełnią określoną rolę lub autorytet. Dyrektorzy korporacyjni są wspólnym celem inżynierii społecznej. Pracownicy działu pomocy technicznej i administratorzy systemów są również częstymi celami podszywania się pod inne osoby. Większość organizacji posiada centra pomocy, które pomagają pracownikom w kwestiach związanych z technologiami informatycznymi. Pracownicy zazwyczaj postępują zgodnie z instrukcjami personelu działu pomocy technicznej tylko dlatego, że są postrzegani jako technologicznie dobrze poinformowani i godni zaufania. Inżynierowie społeczni rozumieją to zaufanie i wykorzystają je do kradzieży informacji. Atakujący podszywa się pod personel pomocy technicznej i nadużywa tego ślepego zaufania, aby gromadzić wszelkie informacje, których potrzebuje atakujący. Personel działu pomocy technicznej może być także ofiarą ataków socjotechnicznych, a inżynier społeczny podszywa się pod użytkownika potrzebującego pomocy technicznej. Atak na centrum pomocy AOL jest historycznym przykładem udanego ataku socjotechniki na personel centrum pomocy. Osoba atakująca udająca klienta była w stanie infiltrować środowisko AOL, zwalniając pracownika działu pomocy AOL. Zdarzały się również przypadki, w których inżynierowie społeczni podszywają się pod urzędników lub menedżerów korporacyjnych. W jednym przypadku gigant płac ADP opublikował informacje o personelu i rachunku maklerskim setkom tysięcy klientów. Atakujący podszywał się pod członka zarządu firmy, poprosił o informacje i je otrzymał. Ta sprawa podkreśla potrzebę kontroli i edukacji dla wszystkich poziomów pracowników. Ofiara w tym przypadku mogła obawiać się, że nie zadowoli silnego członka organizacji, i mogła obawiać się kary. Należy pamiętać, że osoby atakujące podszywają się również pod zwykłych pracowników organizacji, ubierając się, rozmawiając i wtapiając się w środowisko organizacji. Robiąc to, atakujący może uzyskać fizyczny dostęp do obiektu przez piggybacking lub tailgating. W jednym przypadku zgłoszonym przez studenta na kursie bezpieczeństwa w 1993 roku inżynier społeczny współpracujący ze skorumpowanym menedżerem był w stanie kierować nieużywanym biurkiem w dużej firmie przez kilka miesięcy, zanim ochroniarz poprosił o

identyfikację jego firmy. Przestępca natychmiast zniknął, ale nie wcześniej, niż sam się wcielając w stosunku do pracowników jako nowy pracownik, a nawet będąc niczego nie podejrzewającym zaproszonym na spotkania towarzyskie. Dla inżyniera społecznego nie ma granic podszywania się; mogą próbować uzyskać informacje poprzez fizyczny dostęp do organizacji przy użyciu dowolnej liczby podstępów, w tym podszywania się pod:

* Pracownicy tymczasowi (np. kontrahenci lub audytorzy)
* Pracownicy przedsiębiorstw użyteczności publicznej lub telekomunikacyjnych
* Personel ratunkowy
* Pracownicy dozorcy lub konserwatorzy
* Nowi pracownicy
* Personel dostawy

Fizyczny dostęp może znacznie zwiększyć wskaźnik skuteczności ataku w zależności od tego, czy organizacja ma odpowiednią kontrolę. Silnie zmotywowani inżynierowie społeczni mogą posunąć się nawet do znalezienia zatrudnienia w firmie lub w firmie będącej klientem firmy, aby mieć łatwiejszy dostęp do ofiary.

UWODZENIE

Słowo „uwieść" definiuje się jako „odejście od obowiązku, przyjętych zasad lub właściwego postępowania". Zasadniczo atak socjotechniczny z wykorzystaniem uwodzenia zajmie więcej czasu niż atak personifikacji. Atakujący, wykorzystując uwodzenie, zidentyfikuje cel i utworzy więź z tą osobą, poprzez ustawienia społecznościowe, online lub poprzez inny mechanizm. To podczas tego związku informacje ofiary są przekazywane napastnikowi. Na przykład inżynier społeczny, który chce uzyskać dostęp do budynku, może zaprzyjaźnić się ze strażnikiem tej organizacji. Po upływie pewnego czasu i rozwoju związku napastnik może poprosić o wycieczkę po obiekcie. Strażnik, chcąc zadowolić nowego przyjaciela, może zezwolić na wycieczkę. Inżynier społeczny, będąc już w środku, może sadzić tajne urządzenia nasłuchujące, szukać nazw użytkowników lub haseł oraz czytać dokumenty pozostawione na zewnątrz.

ZASTRASZENIE

Inżynierowie społeczni mogą wykorzystać strach, aby osiągnąć swoje cele. Na przykład w 2012 r. oszuści rozpowszechniali alarmujące wiadomości e-mail dotyczące ścigania FBI wśród niewinnych ofiar. Cyberprzestępcy wdrażają nową technikę wymuszenia, wykorzystując platformę złośliwego oprogramowania Citadel do dostarczania oprogramowania ransomware Reveton. Najnowsza wersja oprogramowania ransomware używa nazwy Internet Crime Complaint Center, aby odstraszyć ofiary od wysyłania pieniędzy do sprawców. Oprócz wzbudzania obaw przed oskarżeniem, ta wersja złośliwego oprogramowania twierdzi również, że aktywność użytkownika na komputerze jest rejestrowana za pomocą audio, wideo i innych urządzeń. Jak opisano we wcześniejszych alertach dotyczących tego złośliwego oprogramowania, zwabia on ofiarę na stronie internetowej drive-by download, w której ransomware jest instalowane na komputerze użytkownika. Po zainstalowaniu komputer zawiesza się i wyświetla się ekran z ostrzeżeniem, że użytkownik naruszył prawo federalne Stanów Zjednoczonych. Wiadomość zawiera ponadto oświadczenie, że organ ścigania ustalił, że komputer korzystający z adresu IP ofiary uzyskał dostęp do pornografii dziecięcej i innych nielegalnych treści. Aby odblokować komputer, użytkownik jest proszony o zapłacenie grzywny za pomocą usług kart przedpłaconych. Położenie geograficzne komputera użytkownika określa, jakie usługi płatnicze są oferowane. Oprócz oprogramowania ransomware złośliwe oprogramowanie Citadel nadal działa na zaatakowanym komputerze i może być wykorzystywane do popełniania oszustw związanych z bankowością internetową i kartami kredytowymi. Innym atakiem inżynierii społecznej wykorzystującym zastraszanie jest fałszywe oszustwo biurowe. Pracownik niskiego poziomu akceptuje ofertę bezpłatnego tonera do drukarki, środka do czyszczenia szkła lub papieru i otrzymuje pudełko materiałów, a następnie fakturę. Odrzucane są próby zwrotu niechcianych materiałów, które już nie są

wolne, a przestępcy stosują coraz silniejsze groźby w celu zastraszenia pracownika do przekazania faktury wraz z zapłatą. Pracownicy mogą zostać poinformowani, że ich pracodawca zostanie pozwany lub że skarga dotycząca ich zachowania zostanie wysłana do wyższych szczebli organizacji. Odmiana polega na wysłaniu prezentu do ofiary w nadziei, że przyjęcie go może być wykorzystane do zawstydzenia odbiorcy do spełnienia wymagań oszustów. Takie oszustwa często wystarczają, aby wygenerować miliony dolarów dochodu dla przestępców

ATAK LOW-TECH

Ataki z wykorzystaniem niskiej technologii są nieocenione dla atakującego w ramach rozpoznania, kradzieży informacji i badań dla łatwych celów. Czasami metody te mogą nawet nagrodzić atakującego bardzo dużą ilością użytecznych informacji w bardzo krótkim czasie. Metody ataku Low-tech mogą wydawać się proste lub nieprawdopodobne, ale opisane metody mogą być łatwo przeoczone przez menedżerów bezpieczeństwa. Nie są to miejskie legendy - były używane w przeszłości i są nadal używane.

NURKOWANIE W ŚMIETNIKU

W kontekście inżynierii społecznej nurkowanie Dumpster Diving jest czynnością inżyniera socjalnego polegającą na przeszukiwaniu śmieci organizacji w celu znalezienia dokumentów, sprzętu, oprogramowania lub czegokolwiek, co może być wartościowe dla osiągnięcia celów atakującego. Nawet przy coraz szerszym wykorzystaniu niszczenia poufnych dokumentów nurkowanie w kontenerach jest popularną techniką socjotechniki, ponieważ jest łatwe i często skuteczne. Oracle zatrudniło detektywów, aby kupili śmieci Microsoftu podczas procesu antymonopolowego Microsoftu. (Dedektywom się nie udało). Inżynierowie społeczni nie muszą nikogo oszukiwać, aby wykonać atak. W wielu przypadkach wyrzucone materiały mogą znajdować się w otwartych pojemnikach przez tygodnie. Nurkowanie w kontenerach odbywa się najczęściej w nocy, gdy nikogo nie ma w pobliżu, ponieważ ryzyko złapania jest mniejsze. Aby nie zwracać na siebie uwagi, nurkowie wywrotki znani są z ubierania się w ciemne ubrania, a nawet w mundury porządkowych. Wszystkie organizacje muszą zrozumieć prawne konsekwencje nurkowania w śmietniku. Lokalne i stanowe przepisy mogą się znacznie różnić i być mętne; jednak brak organizacji lub osoba fizyczna powinna mieć realistyczne oczekiwania dotyczące prywatności w odniesieniu do materiałów w pojemnikach na śmieci. Atakujący może nawet legalnie usunąć i przejąć na własność wszystko, co pozostało w pojemniku na śmieci, jeśli jest ono umieszczone poza granicami własności prywatnej. Informacje poufne muszą zostać zniszczone, a nie po prostu odrzucone. Niefortunny przykład udostępniania poufnych danych w śmieciach wyszedł na jaw w listopadzie 2012 r., kiedy odkryto, że paski konfetti rzucone w tłum podczas parady Dziękczynienia Macy mają nienaruszone, czytelne poufne dane: Wśród łatwo identyfikowalnych danych z policji hrabstwa Nassau Departament były szczegóły trasy Mitta Romneya do i z ostatniej debaty prezydenckiej na Uniwersytecie Hofstra. WPIX-TV twierdzi, że konfetti zebrane przez widzów w pobliżu 65th Street i Central Park West zawierały również akta aresztowań, raporty o incydentach i dane osobowe oraz zidentyfikowanych tajnych funkcjonariuszy. „Są numery telefonów, adresy, więcej numerów ubezpieczenia społecznego, numery rejestracyjne" - powiedział Ethan Finkelstein z Manhattanu, który zebrał niektóre konfetti z przyjaciółmi. „A potem znajdujemy wszystkie raporty z incydentów z policji.

KRADZIEŻ

Odwieczna zbrodnia kradzieży to kolejna popularna technika inżynierii społecznej. Inżynierowie społeczni mogą zbierać wszystko, co mogą dostać, dosłownie, i wykorzystywać uzyskane informacje do przeprowadzania innych ataków. Cele kradzieży obejmują między innymi materiały drukowane, dyski CD-ROM, dyski flash USB, nośniki kopii zapasowych, tablety, urządzenia inteligentne i laptopy. Złodzieje mogą zdobywać przedmioty w towarzystwie lub poza lokalem. Będąc na terenie firmy, mogą

szukać przedmiotów, które mogą złapać i szybko ukryć. Atakujący może przynieść puste torby na laptopa, plecaki, a nawet duże portfele, aby pomóc w ich wysiłkach. Większość pracowników jest bardziej świadoma technik kradzieży poza organizacją, takich jak taksówki, lotniska i inne miejsca publiczne. Pracownicy mogą nie zdawać sobie sprawy z tego, że inżynier społeczny lub inny przestępca może być również osobą z wewnątrz.

WYKORZYSTANIE USTAWIEŃ SPOŁECZNOŚCIOWYCH

Inżynierowie społeczni mogą wykorzystywać ustawienia społecznościowe do uzyskiwania informacji, ponieważ ludzie relaksują się w otoczeniu społecznościowym i mogą wierzyć, że praktyki bezpieczeństwa informacji dotyczą tylko miejsca pracy. Inżynier społeczny może wykorzystać otoczenie społeczne, takie jak bar, aby skorzystać z picia pracowników w celu uzyskania informacji. Atakujący może aktywnie zaangażować się w cel lub biernie podsłuchiwać rozmowę. Chociaż ten rodzaj ataku może wydawać się zbyt daleko idący, istnieje wiele sytuacji, w których atakujący może być we właściwym miejscu we właściwym czasie, aby zdobyć wiedzę, którą można później wykorzystać jako część większego ataku. Ludzie w otoczeniu społecznym rzadziej mają zapewnioną obronę i bezpieczeństwo. Restauracje, funkcje firmowe, improwizowane spotkania poza budynkiem firmy lub głośne rozmowy telefoniczne to wszystkie obszary lub sytuacje, w których może wystąpić podsłuch. Wiele razy pracownicy będą pracować w pociągach podmiejskich lub prowadzić działalność w innych miejscach publicznych. Inżynier społeczny może wykorzystać mobilną siłę roboczą organizacji w celu uzyskania informacji. Pracownicy powinni być świadomi tego, kto jest wokół nich podczas wykonywania jakichkolwiek zadań związanych z pracą.

WYKORZYSTANIE CIEKAWOŚCI LUB NAIWNOŚCI

Inżynierowie społeczni mogą oszukać ofiarę, aby nieświadomie pomogła w ataku, wzbudzając ciekawość użytkownika. Na przykład osoba atakująca może zostawić intrygująco oznaczoną płytę CD-ROM w pokoju wypoczynkowym, mając nadzieję, że ofiara jest ciekawa zawartości. Gdy ofiara umieści płytę CD-ROM w swoim komputerze, złośliwy program, taki jak wirus, może automatycznie uruchomić się i rozprzestrzeniać. Ta technika została również wykonana przy użyciu napędów USB, iPodów i uszkodzonych płyt CD z muzyką

EKSPLORACJA DANYCH

Wyszukiwarki mogą skatalogować zaskakującą ilość informacji wrażliwych i poufnych. Inżynierowie społecznościowi mogą tworzyć specjalne wyszukiwania, korzystać z interfejsów programowania aplikacji w wyszukiwarkach (API) oraz korzystać z zaawansowanych możliwości wyszukiwania wielu wyszukiwarek w celu wyszukiwania informacji o firmie. Kolejnym wektorem ataku jest funkcja buforowania wielu wyszukiwarek. Wyszukiwarka może buforować stronę WWW zawierającą poufne informacje. Jeśli organizacja zażąda usunięcia pamięci podręcznej, nadal występuje opóźnienie przed zaktualizowaniem pamięci podręcznej wyszukiwarki, w którym to czasie ujawniane są informacje organizacji. Inżynierowie społeczni mogą również wykorzystywać dane o osobach lub organizacjach zebrane z mediów społecznościowych. Atakujący mogą wydobywać te dane na potrzeby trendów behawioralnych ofiar. Mogli zdobyć więcej informacji o ofiarach niż dane z mediów społecznościowych. Dokumenty opublikowane przez firmę są kolejnym źródłem niezamierzonego ujawnienia informacji. W technice znanej jako szlifowanie danych inżynierowie społeczni mogą używać oprogramowania metadatareader do wydobywania informacji, takich jak nazwisko autora, organizacja, nazwa komputera, nazwa sieci, adres e-mail, identyfikator użytkownika (ID) i komentarze z dokumentów Microsoft Office. Te potencjalnie szkodliwe informacje są zawarte w większości typów dokumentów.

PIGGYBACKING LUB TAILGATING

Powszechną i bardzo skuteczną metodą inżynierii społecznej jest piggybacking lub tailgating. Ta metoda umożliwia atakującemu dostęp do obiektu bez pokazywania odpowiednich poświadczeń. Ofiara w tych przypadkach jest uprzejma i trzyma drzwi napastnikowi, który wchodzi do obiektu, korzystając z poświadczeń ofiary. Wewnątrz obiektu atakujący może swobodnie wędrować po budynku w poszukiwaniu informacji. W razie zapytania osoby atakujące mogą skorzystać z wymówki, by zapomnieć o swoich danych uwierzytelniających lub zostać nowymi pracownikami. Zasadniczo, jeśli zamierza się zastosować piggybacking, inżynierowie społeczni będą się ubierać i działać zgodnie z innymi członkami organizacji, aby mogli wtopić się w placówkę. Jeśli obiekt jest zabezpieczony wieloma warstwami bezpieczeństwa fizycznego, osoby atakujące mogą próbować wykorzystać socjotechnikę do naruszenia pierwszych kilku warstw, a następnie zastosować inne metody ataku

METODY SIECIOWE I GŁOSOWE

Internet wystartował, podobnie jak ataki socjotechniczne. Ataki te różnią się od tradycyjnych ataków socjotechnicznych ze względu na minimalną interakcję człowieka lub brak interakcji. Nadal jednak podstawą ataków jest ufna natura ludzi. Irytujący atak nigeryjski 419 jest atakiem kombinowanym, wykorzystującym zarówno wiadomości e-mail, jak i interakcję człowieka. Metody stosowane w tych atakach to phishing, pharming, szpieg, złośliwe oprogramowanie i vishing

WYŁUDZANIE INFORMACJI

Wyłudzanie informacji jest jednym z najczęściej używanych i udanych ataków socjotechnicznych. Jest to zdefiniowane jako „czynność wysłania wiadomości e-mail do użytkownika, który fałszywie twierdzi, że jest uznanym za legalne przedsiębiorstwo, w celu oszukania użytkownika w celu przekazania prywatnych informacji". Phishing, podobnie jak wszystkie ataki socjotechniczne, opiera się na zaufaniu ludzi. Naiwność o korzystaniu z Internetu również odgrywa rolę w powodzeniu tego ataku. Ciekawym nowym problemem jest to, że fałszywe przedstawianie jako źródła wiadomości e-mail typu phishing było drugim najczęstszym rodzajem ataku zgłaszanego przez respondentów (39 procent) w ankiecie Computer Security Institute „2010⁄2011 Computer Crime and Security Survey". Coraz większą popularność zyskują także nowsze, bardziej ukierunkowane ataki phishingowe zwane phishingiem włóczniowym. Wyłudzanie informacji typu spear jest wykorzystywane w niebezpiecznym typie zagrożeń znanych jako Advanced Persistent Threats (APT). Phishing spear został wykorzystany w części naruszenia bezpieczeństwa firmy RSA w 2011 roku.

SPIM

Wiele osób i firm polega na komunikacji synchronicznej które oferuje komunikator internetowy (IM). Inżynierowie społeczni zauważyli wzrost wykorzystania oprogramowania komunikatorów internetowych i opracowali Spim. Spim to „natychmiastowy spam lub spam IM". Atak szpiegowski jest bardzo podobny do ataku phishingowego, z tym że wektor to oprogramowanie do wiadomości błyskawicznych zamiast wiadomości e-mail. Na przykład osoba atakująca opracuje fałszywą witrynę internetową, która przypomina legalną, i wyśle link do wielu kont czatu. Ofiary odwiedzą stronę internetową i zalogują się, ujawniając swoje dane uwierzytelniające atakującemu. Oszukańcza witryna może zawierać złośliwe oprogramowanie, które infekuje komputer ofiary. Co zaskakujące, pomimo coraz częstszego korzystania z oprogramowania do przesyłania wiadomości błyskawiczne tempo wzrostu jest powolne

PHARMING

W atakach pharming osoby atakujące próbują zmusić ofiary do odwiedzenia sfałszowanych stron internetowych w celu ujawnienia poufnych danych osobowych. Atakujący osiągają to poprzez manipulowanie lokalnym lub globalnym katalogiem DNS ofiary. Ataki typu „pharming" mogą oszukać

użytkowników łatwiej niż inne ataki typu „low-tech”, ponieważ użytkownik może nie otrzymać żadnej wskazówki, że atak jest w toku. Użytkownicy mogą jak zwykle wpisać adresy URL swoich stron internetowych z bankowością lub kartami kredytowymi w swoich przeglądarkach i zwykle nie zauważają, że faktycznie odwiedzają fałszywe strony. W 1997 roku Dan Parisi zarejestrował domenę whitehouse.com i złapał ludzi, którzy omyłkowo szukają whitehouse.gov do oglądania pornografii - wczesnej formy pharmingu. Podczas ataku pharmingu w 2005 r. użytkownicy usługi poczty internetowej Hushmail zostali przekierowani na fałszywą stronę, na której zebrano ich informacje. Hushmail odniósł negatywny rozgłos z powodu tego ataku i był zmuszony codziennie informować swoich użytkowników o dochodzeniu w sprawie ataku

ZŁOŚLIWE OPROGRAMOWANIE

Złośliwe oprogramowanie to programy lub pliki, które są szkodliwe lub niebezpieczne dla użytkownika końcowego. Inżynierowie społeczni często używają trojanów i wirusów. Chociaż same programy nie stanowią czysto socjotechnicznego ataku, podstawa ataku nadal polega na manipulowaniu zaufaniem ofiary. Na przykład inżynier społeczny może wysłać ofierze wiadomość e-mail zawierającą link do szkodliwej witryny internetowej. Jeśli użytkownik odwiedzi złośliwą witrynę internetową, trojan zostanie zainstalowany na komputerze ofiary, a złośliwy program zacznie gromadzić informacje o ofierze. Inny przykład dotyczy dysku USB załadowanego automatycznie uruchamiającym się złośliwym oprogramowaniem. Ofiara ciekawa zawartości podłączy dysk do komputera i wykona złośliwy kod. Można użyć dowolnej liczby wektorów, w tym dokumentów, wiadomości e-mail, stron internetowych, płyt CD i napędy USB. Założenie jest takie samo dla wszystkich rodzajów tych ataków: niczego niepodejrzewający użytkownicy, ciekawi treści, niechcący zainstalują te niebezpieczne programy. Infekcje złośliwym oprogramowaniem były najczęstszym rodzajem ataku zgłoszonym przez respondentów (67 procent) w ankiecie Computer Security Institute „2010⁄2011 Computer Crime and Security Survey”, a boty i zombie zgłoszono o 29 procent. Złośliwe oprogramowanie zaczęło ostatnio wykorzystywać rodzaj ataku socjotechnicznego, w którym zaufanie pokładane w ważnym certyfikacie jest wykorzystywane w połączeniu ze znaną od dawna luką zwaną wstępnym ładowaniem biblioteki Data Link Library (DLL). W tym ataku przygotowywany jest pakiet zawierający prawidłową, zaufaną aplikację z prawidłowym podpisem. Jednak w tym pakiecie znajduje się złośliwa biblioteka DLL. Większość użytkowników, którzy wiedzą, jak szukać ważnego certyfikatu, rzeczywiście znajdzie go w aplikacji i dlatego zaufa całemu pakietowi. Ofiara uruchamia prawidłową, zaufaną aplikację, a ze względu na lukę wczytywania wstępnego złośliwa biblioteka DLL jest ładowana z katalogu lokalnego przed ważną Biblioteką DLL jest ładowana ze zwykłej ścieżki.

VISHING

Atakujący, którzy wabią ofiary za pomocą wiadomości e-mail i telefonu lub po prostu telefonu, dokonują ataku vishingu. Inżynierowie społeczni mogą wysłać wiadomość e-mail lub zadzwonić do ofiary w organizacji w sprawie problemu i poprosić o oddzwonienie. Podany numer jest obsadzony przez wspólników lub odebrany przez uzasadniony zautomatyzowany system. Ofiary są proszone o ujawnienie potencjalnie szkodliwych informacji o sobie w przypadku kradzieży tożsamości lub o swojej firmie. W innym przykładzie osoba atakująca może wykorzystać zautomatyzowane systemy odpowiadania na telefon, które pozwalają dzwoniącemu na wprowadzenie pierwszych kilku liter nazwiska kontaktu w celu dotarcia do jego numeru wewnętrznego. Atakujący może wypróbować wiele rozszerzeń i natknąć się na niektóre, które ujawniają szczegóły dotyczące pozycji osoby, tytułu lub statusu biura (np. „Jestem na urlopie do 4 kwietnia”). Inżynier społeczny może wykorzystać te informacje i zadzwonić do innych pracowników w celu uzyskania dodatkowych informacji lub dostępu. Należy również zauważyć, że wraz z rozprzestrzenianiem się protokołu Voice over Internet Protocol (IP) (VoIP) istnieje obecnie funkcja Voice Phishing, która propaguje atak typu phishing-phishing. Ponieważ połączenie jest kierowane przez IP, numer połączenia można łatwo zmienić. To jest analogiczny do działania witryn phishingowych. Ponieważ jest to przede wszystkim oparty na głosach

atak socjotechniczny, uważa się go za atak głosowy zamiast ataku internetowego. VoIP umiędzynarodowiło również występowanie takich oszustw. Podczas incydentu w 2013 r. przestępcy, którzy prawdopodobnie przebywali w Afryce, reklamowali nieistniejące bezpłatne kocięta na tysiącach stron w sieci, używali VoIP do kontaktowania się z ofiarami w celu oszukiwania miłośników kotów o dobrych intencjach, aby płacili za wyimaginowane przesyłki fikcyjne koty

MEDIA SPOŁECZNOŚCIOWE

Media społecznościowe zyskały na popularności w ostatnich latach, podobnie jak szanse inżyniera społecznego na prześladowanie tak częstych tych rynków zbytu. Przydatne informacje można łatwo zebrać, przeszukując stronę społecznościową ofiary lub strony krewnych, które umieszczają ofiarę na swoich stronach. Zebrane dane mogą obejmować takie rzeczy jak:

* Terminy wydarzeń
* Przyjaciele / krewni / współpracownicy
* Zdjęcia
* Informacje kontaktowe
* Lokalizacje odwiedzane

Oprócz ścisłego zbierania danych, inżynier społeczny może użyć personifikacji, aby zaprzyjaźnić się z osobą, dzięki czemu można zobaczyć szczegóły ukryte przed widokiem publicznym. Może to pozwolić atakującemu na skuteczniejsze ukierunkowanie ataku na jego potrzeby. Szczególnie niepokojąca jest sieć LinkedIn, która do końca 2012 r. Osiągnęła 187 milionów członków na całym świecie; 57 procent znajdowało się w Stanach Zjednoczonych, a 63 procent w innych krajach. LinkedIn umożliwia śledzenie tytułów pracy, historii pracy, zaplecza technicznego, edukacji i powiązań z innymi osobami w danej organizacji - idealna informacja dla inżynierów społecznych do dowodzenia. Chociaż dane mają być trzymane z dala od osób, które nie są ze sobą powiązane, niektórzy użytkownicy LinkedIn rutynowo akceptują prośby o połączenie od każdego, kto wysyła im zaproszenie - nawet jeśli Umowa użytkownika LinkedIn wyraźnie stanowi, że członkowie nie mogą „Zapraszać osób, których nie łączysz i wiedzieć, jak dołączyć do swojej sieci. Przestępcy wykazali zainteresowanie kontaktami LinkedIn, sprzedając katalogi informacji zebranych w tej sieci.

ODWROTNA INŻYNIERIA SPOŁECZNA

Odwrotna inżynieria społeczna to skuteczny atak zwykle wykonywany przez doświadczonego inżyniera społecznego. Odwrotny atak inżynierii społecznej składa się z trzech odrębnych części. Po pierwsze, inżynier społeczny stworzy problem, na przykład problem z identyfikatorem użytkownika. Po drugie, inżynier społeczny opublikuje informację, że są jedyną osobą zdolną do rozwiązania problemu. W końcowej części ataku inżynier społeczny pomoże ofierze i „naprawi" problem. Inżynier społeczny zbierze informacje podczas trzeciego segmentu ataku. Wskaźnik skuteczności odwrotnych ataków socjotechnicznych jest zwykle wysoki, ponieważ ofiara jest usatysfakcjonowana, że sfabrykowany problem został rozwiązany. Na przykład atakujący może zmienić nazwę pliku (problem). Ofiara szuka pliku i nie może go znaleźć. Atakujący ogłosi, że był w stanie odzyskać utracone informacje, ale będzie potrzebował identyfikatora użytkownika i hasła, aby uzyskać dostęp do systemu (reklama). Ofiara, zdenerwowana myślą o utracie ważnego dokumentu, ujawni informacje. Wreszcie atakujący „znajdzie" brakujący plik (poprawkę). Ofiara, ciesząc się ze zwrotu pliku, zapomni o udostępnieniu poświadczeń dostępu do systemu.

PSYCHOLOGIA INŻYNIERII SPOŁECZNEJ

Znany ekspert ds. bezpieczeństwa Bruce Schneier stwierdził, że ekonomia behawioralna, psychologia podejmowania decyzji, psychologia ryzyka i neurobiologia mogą pomóc wyjaśnić, dlaczego nasze

poczucie bezpieczeństwa odbiega od rzeczywistości. Ta sekcja koncentruje się na jednym z tych aspektów - psychologii - i analizuje naukę leżącą u podstaw sukcesu inżynierii społecznej. Wykorzystame pewne ugruntowane zasady psychologii i psychologii społecznej do analizy inżynierii społecznej z dwóch punktów widzenia, psychologicznej perspektywy ofiary i socjopsychologicznej perspektywy inżyniera społecznego i ofiary. Kolejna sekcja wyjaśnia, że nie ma jednego stereotypu socjotechnika. Pojęcia użyte w tej sekcji można znaleźć w podręcznikach psychologii licencjackiej i psychologii społecznej, dlatego odniesienia do akademii zostały zminimalizowane. Inżynieria społeczna odnosi sukces z uwagi na ludzką naturę: W tej części przykłady ataków socjotechnicznych ilustrują naukowe terminy używane do scharakteryzowania inżynierii społecznej.

PSYCHOLOGIA

Błąd poznawczy jest definiowany jako błąd psychiczny spowodowany uproszczonymi ludzkimi strategiami przetwarzania informacji. Ludzie stają się ofiarami ataków socjotechnicznych z powodu tendencji poznawczych, zwanych również „heurystyką" lub praktycznymi regułami, które są nieodłączne dla wszystkich ludzi. Te tendencje poznawcze są przede wszystkim przydatne. Psycholog Robert Cialdini pisze:
Nie możemy oczekiwać, że rozpoznamy i przeanalizujemy wszystkie aspekty w każdej osobie, wydarzeniu i sytuacji, które napotkamy nawet w jeden dzień. Nie mamy na to czasu, energii ani zdolności. Zamiast tego musimy bardzo często używać naszych stereotypów, naszych praktycznych zasad, aby klasyfikować rzeczy według kilku kluczowych funkcji, a następnie reagować bezmyślnie, gdy pojawi się jedna z tych funkcji wyzwalacza.
Chociaż uprzedzenia poznawcze występują u wszystkich, powszechna obecność uprzedzeń poznawczych nie oznacza, że nie można im przeciwdziałać. Poniżej przedstawiono niektóre uprzedzenia poznawcze, które mogą wyjaśnić, dlaczego ludzie padają ofiarą ataków inżynierii społecznej:

* Wspomagające wybór nastawienie. Ludzie zwykle pamiętają wybraną przez siebie opcję, która miała więcej pozytywnych aspektów niż negatywnych. Operatorzy działu informatycznego (IT) mogą podawać nazwiska pracowników, rozszerzenia lub oba te elementy bez weryfikacji tożsamości dzwoniących. Operatorzy działu pomocy technicznej pamiętają tę praktykę jako dobrą, ponieważ większość dzwoniących jest autentyczna, a dzwoniący dziękują im za udzielenie informacji. Inżynierowie społeczni mogą udawać prawdziwych dzwoniących, aby wykorzystać preferencje operatorów pomocy technicznej. Zgodnie z artykułem na temat witryny poświęconej analizie zabezpieczeń SecurityFocus, demonstracja tego ataku przeprowadzona przez Computer Security Instytut faktycznie się udało.
* Błąd uprzedzenia. Ludzie gromadzą i interpretują dowody w sposób, który potwierdza ich koncepcje. Jeśli organizacja ma umowę ze służbą powierniczą, a pracownicy widzą, że wszyscy opiekunowie noszą ten sam mundur, to inżynier socjalny w tym mundurze może nie zostać wezwany do zidentyfikowania się z powodu uprzedzeń potwierdzających pracowników. W filmie Ocean's Eleven znajduje się wiele scen, w których właściciel i pracownicy trzech kasyn w Las Vegas wcielają się w niesamowitych bohaterów ubranych tak, by wtapiać się w role i otoczenie.
* Efekt ekspozycji. Ludzie lubią rzeczy, które są im znane. Inżynier społeczny może zadzwonić do ofiar i wyjaśnić, że przeprowadzają ankietę w popularnej lokalnej restauracji i zapytać o organizację, w której ofiara jest zatrudniona. Ofiary czują się swobodnie, udzielając tych informacji, ponieważ znają restaurację. Według Elodie Grandjean, badaczki szkodliwego oprogramowania, niektóre motywy e-maili, adresów URL lub wiadomości błyskawicznych wykorzystywane w socjotechnice
ataki obejmują:
1. Linki i obrazy pornograficzne
2. Używanie żeńskiego imienia w polu nadawcy
3. Plany polityczne, w tym prośby o wkład w imieniu popularnego kandydata

4. Fałszywe wiadomości e-mail dla banków, internetowych usług płatniczych i innych usług finansowych. Żądają potwierdzenia lub aktualizacji danych logowania lub danych karty kredytowej.
5. Groźne wiadomości e-mail, informacje o sankcjach więziennych lub procedurach dotyczących przysięgłych
6. Bezpłatne gry i wygaszacze ekranu zawierające trojana lub bezpłatne narzędzia antyszpiegowskie, które same często są nieuczciwymi programami
7. Duże wydarzenia, takie jak sport, ekstremalna katastrofa pogodowa lub pilne wiadomości
8. Nazwiska gwiazd i relacje z ich przygód i złego zachowania
9. Potencjalnie zaufane lub tajne relacje, takie jak przynależność do 12-punktowego programu
10. Portale społecznościowe, fałszywi przyjaciele, szkolni koledzy lub krewni i tajni kochankowie
* Zakotwiczenie. Przy podejmowaniu decyzji ludzie zwykle koncentrują się na jednej cechy. Jeśli inżynier społeczny ma uspokajający głos, ofiara może skupić się na tym atrybucie w porównaniu do zadawanych pytań. Ekspert ds. bezpieczeństwa Winn Schwartau opisuje udany atak socjotechniczny, w którym niektórzy pracownicy nowojorskiej firmy świadczącej usługi finansowe zakochali się w fałszywym liście napisanym na papierze firmowym, podającym się za dział bezpieczeństwa informacji; 28 procent z 1200 pracowników odpisało na swoje dane osobowe. Pracownicy, ze szkodą dla niego, zbytnio skupili się na papierze firmowym i zignorowali inne aspekty żądania, takie jak jego podejrzliwość, powaga i nagłość.

PSYCHOLOGIA SPOŁECZNA.

Psychologowie społeczni definiują schemat jako nieodłączny obraz rzeczywistości wykorzystywany przez ludzi do osądzania i podejmowania decyzji. Z perspektywy psychologii społecznej inżynierowie społeczni wykorzystują fakt, że schemat większości ludzi zawiera zasady dotyczące zaufania innym ludziom i ich intencjom. Ludzi od samego początku uczy się, że bycie miłym dla innych jest dobrą rzeczą. W kontekście bezpieczeństwa informacji skłonność ludzi do ślepego zaufania innym może przeliterować katastrofę. Poniżej znajduje się lista typowych błędów popełnianych przez ludzi oraz przykłady wykorzystania przez inżynierów społecznych tych błędów do ataku na organizację.
* Podstawowy błąd atrybucji: w tym powszechnym błędzie ludzie zakładają, że zachowania innych odzwierciedlają stabilne, wewnętrzne cechy. Ktoś, kto popełni podstawowy błąd przypisania, może zobaczyć kolegę w złym humorze i pomyśleć: „Zawsze jest humorzasty". W rzeczywistości kolega może być ogólnie miły, ale w tym czasie odczuwa ból głowy. Inżynierowie społeczni będą działać przyjemnie i czarująco aby skłonić ofiary do popełnienia podstawowego błędu przypisania, być pod wrażeniem, że osoby atakujące są ogólnie miłymi ludźmi i tym samym im pomóc.
* Efekt Wagi: biorąc pod uwagę grupę osób, ludzie mają tendencję do zgadywania, że najbardziej lub najmniej wpływowa osoba to ta, która najbardziej się wyróżnia. Na przykład z grupy dziesięciu osób, z których dziewięć ma sześć stóp wzrostu, a wysokość pięciu stóp, jeśli zostanie poproszony o zgadnięcie, kto jest najinteligentniejszą osobą w grupie, obserwator może powiedzieć, że jest to pięciostopowa osoba. Inżynierowie społeczni próbują wtopić się w środowisko ofiary, aby skorzystać z efektu wagi. Są doskonale świadomi żargonu firmy, wydarzeń i regionalnych akcentów.
* Zgodność, zgodność i posłuszeństwo: Ludzie reagują na presję społeczną związaną z zgodnością, zgodnością i posłuszeństwem, dostosowując swoje zachowania. Inżynier społeczny, podszywający się pod kierownika wysokiego szczebla, domagającego się wstępu na teren firmy, może przekonać nowego ochroniarza o ciężarze przejętej władzy. Obietnica nagrody lub groźby kary ze strony autorytetu może dodatkowo wpłynąć na decyzję pracownika ochrony dotyczącą wykonania prośby atakującego.

PROFIL INŻYNIERA SPOŁECZNEGO

Profil inżyniera społecznego nie jest stereotypowym hakerem komputerowym często przedstawianym w filmach lub telewizji. Inżynierowie społeczni najprawdopodobniej nie będą samotnymi nastolatkami spędzającymi cały czas ze swoimi komputerami w ciemnej piwnicy. Inżynier społeczny jest często towarzyski, pewny siebie, doskonałym komunikatorem i dobrze wykształcony. Inżynierowie społeczni

mogą wykorzystywać własną osobowość lub przyjmować osobowość, która znacznie różni się od ich normalnej osobowości - często osobowości, którą rozwinęli w ciągu miesięcy, a nawet lat. Aby osiągnąć swoje cele, wtopią się w środowisko. Inżynierowie społeczni starają się być niezauważalni, niczym niezwykłym. Będą się ubierać zgodnie z zasadami ubioru środowiska, w którym działają. Co ciekawe, inżynierowie społeczni mogą być świetnymi aktorami, zdolnymi do myślenia na własnych nogach i szybkiego dostosowywania się do zmieniających się warunków. Pewność siebie atakującego często maskuje nerwowość lub napięcie podczas próby socjotechniki, co może prowadzić do nieuzasadnionej wiarygodności. Inżynierowie społeczni mogą również wykazywać ciemną stronę. Atakujący mogą nie brać pod uwagę konsekwencji swoich działań wobec ofiary. Mimo że napastnicy mogą wydawać się bardzo uprzejmi lub sympatyczni wobec swoich ofiar, w rzeczywistości bardzo nie dbają o ofiarę lub ludzi wykorzystywanych do osiągnięcia celu. Ofiara i inni są po prostu środkiem do osiągnięcia celu; są tylko częścią narzędzia ataku socjotechnicznego. Motywacje inżyniera społecznego mogą się znacznie różnić i wahać od osobistych korzyści finansowych po zemstę. Może być również znaczna presja zewnętrzna na napastnika ze strony znajomych lub syndykatów przestępczości zorganizowanej.

NIEBEZPIECZEŃSTWA INŻYNIERII SPOŁECZNEJ I JEJ WPŁYW NA DZIAŁALNOŚĆ BIZNESOWĄ.

Ostateczne cele atakującego mogą ograniczać się do kradzieży, ale mogą również obejmować zakłócenie działalności lub nawet zniszczenie firmy. Organizacja musi ocenić potencjalny wpływ nawet pozornie drobnej próby socjotechniki.

KONSEKWENCJE

Konsekwencje udanego ataku socjotechnicznego są prawie niezliczone. Coś, co można wymyślić jako wektor ataku, prawdopodobnie zostało gdzieś atakowane. Podobnie jak w przypadku planowania odzyskiwania po awarii, gdy próbujesz oszacować i zrozumieć wpływ ataków socjotechnicznych, wszystkie możliwości należy położyć na stole. Coś tak pozornie drobnego jak wewnętrzna notatka, która nie została odpowiednio zniszczona, może potencjalnie doprowadzić do bankructwa organizacji. W rezultacie prosty atak socjotechniczny może prowadzić do bardziej złożonego ataku, który przekształca się w poważną awarię bezpieczeństwa informacji opartą na informacjach zawartych w jednej źle umieszczonej notatce. Zagrożenie jest szczególnie wysokie w przypadku spółek giełdowych, które mogą stracić wartość z powodu utraty zaufania ze strony inwestorów. Wiele firm w ciągu ostatnich kilku lat znalazło się pod presją finansową z powodu naruszenia bezpieczeństwa lub wygaśnięcia bezpieczeństwa, które zwróciło znaczną uwagę ze strony naciśnij. Inżynieria społeczna była prawdopodobnie częścią tych incydentów bezpieczeństwa. Wiele organizacji jest prawnie zobowiązanych do posiadania zabezpieczeń, jeśli chodzi o bezpieczeństwo danych; coraz więcej z tych wymagań wymaga kontroli bezpieczeństwa, które pomogą organizacji w obronie przed atakami socjotechnicznymi i technologicznymi. Kolejną poważną konsekwencją udanego ataku socjotechnicznego jest niepewność i trudność w zbadaniu takiego ataku. Organizacje nigdy nie mogą w pełni odkryć, w jakim stopniu inżynier społeczny był w stanie infiltrować organizację. Istnieje tak wiele różnych wektorów i możliwości wtargnięcia, że może nie być możliwe pełne zrozumienie, co lub kto został naruszony podczas ataku. Szczególnie niebezpieczna i frustrująca jest sytuacja, w której osoba atakująca ma do czynienia z osobą wewnętrzną lub wspólnikiem w organizacji. Niektóre organizacje nigdy nie zidentyfikowały tych osób w organizacji. Ta niepewność jest trudna do odzyskania i obrony przed nią w przyszłości. Jest to także inna sytuacja, w której spółka może mieć poważne problemy z wiarygodnością i utratą zaufania ze strony akcjonariuszy po atakować, jeśli takie szczegóły zostaną ujawnione. Ta dokładna sytuacja doprowadziła również do przeciągnięcia liny między organami regulacyjnymi a organizacjami w sprawie przepisów dotyczących ujawniania informacji. Przepisy te różnią się znacznie w zależności od kraju i kraju. Firmy walczą o ochronę przed ujawnieniem obszernych informacji z samego powodu ochrony wizerunku firmy i wartości finansowej.

STUDIUM PRZYPADKU : PRZYKŁAD Z BIZNESU

Istnieje wiele dobrze znanych przykładów z rzeczywistych scenariuszy z organizacji, które mogą wykazać skuteczność inżynierii społecznej. Oto kilka dobrze znanych przykładów, które nie zawiodłyby zaangażowanych stron. Ataki socjotechniczne są prawdziwe - nie są to tylko teorie bezpieczeństwa komputerowego

Przypadek 1: Jednym z bardzo dobrze znanych ataków socjotechnicznych w świecie biznesu jest dopuszczenie. W tego rodzaju inżynierii społecznej atakujący będzie zależał od uprzejmości danej osoby. Większość ludzi pamięta z wczesnych lat szkolnych, że uczy się, jak otworzyć drzwi dla kogoś, kto stoi za nim lub nią. Ta uprzejmość jest często przedłużana w miejscu pracy, w tym w bezpiecznych obszarach, takich jak centrum danych. Potencjalny atakujący może próbować wejść do centrum danych bez odpowiednich poświadczeń, podążając za kimś w przeciwnym razie kto wchodzi do centrum danych z odpowiednią identyfikacją i autoryzacją. Upoważniona osoba najprawdopodobniej okaże uprzejmość i otworzy drzwi dla piggybackera, nawet jeśli tożsamość tej osoby nie jest znana. Trzymanie czegoś niewinnego często budzi zaufanie.

Wynik: w tym przykładzie atakujący, który nie jest autoryzowany, uzyskał dostęp do bezpiecznego obiektu, opierając się na poczuciu uprzejmości innej osoby. Może być bardzo trudno wymagać od pracowników powstrzymania się od korzystania z uprzejmości, ale musi istnieć polityka, która dokładnie tego wymaga. Od wszystkich osób wchodzących do bezpiecznego obiektu należy wymagać pełnego korzystania z mechanizmów identyfikacji i autoryzacji za każdym razem.

Przypadek 2: Kolejny przykład, który został przeprowadzony w różnych odmianach, obejmuje atakującego wykorzystującego kilka technik inżynierii społecznej, aby skorzystać z kilku zbieżnych zdarzeń w celu wykorzystania danych, informacji lub sprzętu z organizacji. Atakujący często wykonuje kilka połączeń telefonicznych lub wysyła kilka e-maili, aby znaleźć konkretną datę, kiedy urzędnik firmy, być może dyrektor finansowy lub dyrektor ds. technologii, jest poza biurem. Atakujący wtedy pokazuje się w organizacji, twierdząc, że urzędnik firmy upoważnił napastnika do zabrania określonego komputera z siedziby firmy. Zazwyczaj atakujący próbuje wykazać się pilnością i wykazać się pewnością siebie. Wiele razy pracownik zagłębiał się w żądania atakującego bez sprawdzania historii, a teraz firma zabrała bardzo ważny komputer. (Bardzo często używanym akcentem w tej sprawie, i który staje się coraz bardziej powszechny, jest zdalne instalowanie złośliwego oprogramowania backdoor lub keylogger na komputerze zamiast fizycznie go usuwać).

Wynik: W tym przypadku organizacja straciła kontrolę i własność komputera i / lub jego danych. Jeśli komputer nie ma solidnych zabezpieczeń, takich jak mechanizmy szyfrowania danych, dane i komputer można wykorzystać do dowolnej liczby destrukcyjnych działań. Jeśli informacje o incydencie zostaną upublicznione, można wyrządzić wielką szkodę reputacji organizacji. Dane zebrane z komputera mogą być również sprzedawane konkurentom lub wykorzystywane w ramach programu szantażowania.

WSKAŹNIK SUKCESU

Chociaż istnieje niewiele dokładnych statystyk dotyczących powodzenia inżynierii społecznej, jak ma to miejsce w wielu obszarach bezpieczeństwa informacji, większość ekspertów uważa, że wskaźnik ten jest wysoki. Jeśli historia ma coś, czego może nauczyć społeczność bezpieczeństwa na przykładach, inżynieria społeczna nadal będzie potężnym i skutecznym narzędziem dla przestępców. Niewiele organizacji jest odpornych na socjotechnikę, niezależnie od branży lub produktu. Jeśli nawet dobrze wyszkolony personel wojskowy jest podatny na zagrożenia, każda organizacja musi poważnie potraktować wskaźnik sukcesu. Wysoki wskaźnik sukcesu musi również podkreślać znaczenie ciągłego kształcenia pracowników i ponownej oceny wysiłków organizacji w zakresie zwalczania inżynierii społecznej i ochrony wszystkich zasobów danych. Jest to obszar, w którym wiele organizacji każdej wielkości, nadal przydziel zbyt mało zasobów. Częstotliwość prób socjotechniki dyktuje również potrzebę właściwego, wydajnego i szybkiego zgłaszania podejrzanych działań skierowanych do osób lub organizacji. Bardzo trudno jest bronić się przed próbami inżynierii społecznej, jeśli organizacja nie wie, że jest atakowana lub nie wie, gdzie i jak zgłosić incydent. Prawdopodobieństwo udanego ataku można znacznie zmniejszyć dzięki odpowiednio przeszkolonym, wspieranym i zmotywowanym pracownikom.

MAŁE FIRMY A DUŻE ORGANIZACJE

Wpływ i zagrożenia związane z atakami socjotechnicznymi i technologicznymi różnią się znacznie między małymi firmami i dużymi korporacjami. Jak omówiono powyżej, konsekwencje mogą być potencjalnie poważne, aż do upadku organizacji. Małe firmy są często znacznie mniej przygotowane pod względem operacyjnym i finansowym i znacznie mniej przygotowane do przetrwania poważnego naruszenia bezpieczeństwa. Z drugiej strony, i być może szokujące dla wielu, małe firmy mogą mieć przewagę nad dużymi organizacjami z powodu znacznie mniejszej siły roboczej i załamanej struktury zarządzania. O wiele łatwiej jest komunikować się i angażować wszystkich w małej firmie, gdy atak jest podejmowany lub przeprowadzany. Małe firmy mają również przewagę znacznie mniejszej siły roboczej do szkolenia; skutkuje to znacznie lepiej przygotowanymi pracownikami. Pracownicy małych firm prawdopodobnie częściej identyfikują osoby, które nie należą do organizacji lub nie powinny prosić o dostęp do wrażliwych obszarów lub danych. Mogą również częściej odmawiać dostępu lub przesłuchiwać osoby, których historia nie wydaje się prawdopodobna lub jest podejrzana. Duże organizacje mogą pogrążyć się w biurokracji, nieefektywnym zarządzaniu lub zbyt skomplikowanych procedurach raportowania. Osoba atakująca może wykonać cały plan, zanim zespół bezpieczeństwa w dużej firmie zostanie powiadomiony o próbie socjotechniki. Wiele razy jednostka jest mniej skłonna podważać wiarygodność nieznajomego w dużej organizacji. Jest to szczególnie ważne, gdy są pracownicy, którzy uważają, że mogą zostać ukarani za przesłuchanie kogoś wyższego stopnia lub uniemożliwienie komuś wykonania jego pracy. Pracownik może raczej pozwolić, by napastnik przeszedł bezsprzecznie, niż ryzykować ewentualne negatywne konsekwencje lub kontrolę. Podsumowując, wszystkie organizacje muszą wypatrywać tego typu ataku. Przestępcy nie zawsze wybierają łatwe lub oczywiste cele. Każda firma, mała lub duża, konglomerat rodzinny lub korporacyjny, może być celem ataku wykorzystującego socjotechnikę.

TRENDY

Chociaż ważne jest, aby każdy menedżer ds. bezpieczeństwa informacji zawsze sceptycznie przyglądał się statystykom, równie ważne jest, aby śledzić trendy dotyczące zagrożeń bezpieczeństwa. Inżynieria społeczna nie jest wyjątkiem. Każda ankieta lub sondaż może być trudny do zebrania faktów na temat liczby prób podjętych w danym roku lub liczby udanych. Wiele prób socjotechniki prawdopodobnie nigdy nie jest wykrywanych, a jeszcze mniej jest zgłaszanych lub przyjmowanych do ankiet. Jeśli chodzi o tak potężny i skuteczny mechanizm ataku, załóż najgorsze: jest coraz częściej wykorzystywany przez przestępców, nawet gdy organizacje wiedzą o tego rodzaju atakach, a nawet szkolą pracowników, aby się przed nim bronili. Przestępcy tworzą nowe formy i taktyki każdego dnia, a ludzie prawdopodobnie nadal będą się w nich zakochiwać

WYKRYCIE.

Wykrywanie ataków socjotechnicznych i ataków o niskiej technologii może być trudne. Charakter większości rodzajów ataków socjotechnicznych polega na wykorzystaniu chęci zaufania i pomocy ludzi, co pozwala sprawcy na obejście kontroli technicznych. W wielu przypadkach wykrywanie zależy od zdolności ludzi do rozpoznania potencjalnego ataku, w tym podejrzanej aktywności i odpowiedniej reakcji. Dalsze komplikowanie wykrywania to potencjał, że atak socjotechniczny może nie być pojedynczym zdarzeniem, ale wieloma mniejszymi wydarzeniami, których kulminacją jest atakujący uzyskujący dostęp do ograniczonych zasobów, ukrywający nikczemne działania lub kradnący zastrzeżone informacje. Stosowanie powolnych lub wieloetapowych ataków socjotechnicznych jest jeszcze trudniejsze do wykrycia i potencjalnie bardziej szkodliwe. Niedawno szeroko zgłaszano udane ataki socjotechniczne poprzez ukierunkowane kampanie e-mailowe skierowane do personelu wyższego szczebla. Jeden ekspert od testów penetracyjnych ocenia, że taktyki socjotechniki stanowią mniej niż 20 procent czasu spędzonego na ataku; resztę czasu poświęca się na techniczne

wykorzystanie informacji zebranych pierwotnie w drodze oszustwa. Istnieją trzy główne sposoby wykrywania ataków socjotechnicznych: ludzie, kontrole kontroli i technologia.

LUDZIE

Ponieważ ludzie są wektorem ataku, generalnie są pierwszą linią obrony. Organizacje muszą zapewnić pracownikom zasoby i ciągłą edukację, aby pomóc w rozpoznaniu potencjalnego ataku na podstawie uzasadnionego żądania. Wszystkie obszary organizacji wymagają szkolenia. Inżynierowie społeczni korzystają ze wszystkich dostępnych zasobów; nie ma departamentu ani osoby, która byłaby odporna na potencjalny atak. Ponadto organizacje muszą dostarczyć informacje o tym, co robić podczas ataku i bezpośrednio po nim. Na przykład podczas ataku telefonicznego należy przeszkolić pracowników w zakresie zapamiętywania jak największej liczby szczegółów. Elementy, które pracownik powinien zapamiętać, obejmują:

* Czy napastnik był mężczyzną czy kobietą?
* Czy wyświetlono identyfikator dzwoniącego?
* Czy w tle był hałas?
* Czy on lub ona ma akcent?
* Jakie pytania zostały zadane?
* Jakie odpowiedzi zostały udzielone?

Pracownicy powinni także zdawać sobie sprawę z tego, że ludzie zadają wiele pytań, z których niektóre mogą nie mieć sensu. Ponadto dzwoniący lub e-maile z prośbą o podanie nazwiska kierownika lub personelu IT powinni poprosić o telefon do działu bezpieczeństwa IT lub działu dochodzeń. Kultura organizacyjna jest również kolejnym kluczowym elementem, który pomaga bronić się przed atakami inżynierii społecznej. Kultura musi podkreślać i nagradzać właściwą weryfikację przed udzieleniem informacji. Wyższe kierownictwo może wspierać silną kulturę, wychwalając pracowników, którzy proszą ich o wykazanie się autentycznością, a nie wyrażaniem podrażniena, że ktokolwiek miałby na to odwagę. Wszystkie firmy, w tym firmy ochroniarskie, muszą przestrzegać tej mantry. Niestety, zbyt często VIP-y lub starsi liderzy nie muszą przestrzegać tego samego procesu weryfikacji, aby zmienić hasło lub otrzymać informacje. Wreszcie pracownicy powinni zdawać sobie sprawę z własnych zasad i praktyk biznesowych. Na przykład wszyscy pracownicy powinni zrozumieć, dlaczego dzwoniący prosi o zmianę hasła przez telefon lub wiadomość tekstową. Organizacje muszą również przekazywać swoim współpracownikom jasne informacje na temat tego, co należy zrobić w obliczu możliwej inżynierii społecznej. Na przykład, kogo należy powiadomić podczas faktycznego zdarzenia, bezpośrednio po nim lub obu (w zależności od tego, kiedy pracownik rozpozna atak). Aby pomóc w procesie powiadamiania, organizacja może utworzyć system informacji o zdarzeniach i rozpowszechniać informacje w całej organizacji, aby pracownik mógł natychmiast i łatwo określić, z kim należy się skontaktować w celu uzyskania pomocy.

KONTROLA AUDYTU I REJESTROWANIE ZDARZEŃ

Do wykrywania ataków socjotechnicznych można używać inspekcji i rejestrowania wiadomości e-mail, treści internetowych, loginów systemowych i zmian systemowych organizacji. Jeśli przegląd wydarzeń nie nastąpi w czasie rzeczywistym, nastąpi opóźnienie od momentu ataku i Identifikacji incydentu. W przypadkach, gdy powiadomienie nie odbywa się w czasie rzeczywistym, eksperci medycyny sądowej mogą wykorzystać informacje z audytu, aby pomóc w zestawieniu ataków i ustaleniu pierwotnej przyczyny. Zespoły uświadamiające mogą również wykorzystywać wyniki dziennika, aby pomóc w opracowaniu dodatkowego szkolenia dla grup docelowych. Podczas audytu w czasie rzeczywistym organizacje mogą natychmiast wprowadzić swoje plany zarządzania incydentami, aby ograniczyć potencjalne szkody. Nowoczesne narzędzia anty-malware i antyphishingowe mogą zapewnić nie tylko ochronę przed takimi atakami, ale mogą również przechowywać szczegółowe dane do analizy.

TECHNOLOGIA WYKRYWANIA

Organizacje mogą wdrażać technologię aby pomóc ograniczyć ataki socjotechniczne. Oprogramowanie do filtrowania treści może ograniczać ruch e-mail i ruch w witrynie; wszelkie zidentyfikowane złośliwe oprogramowanie powinno zostać zablokowane lub usunięte z wiadomości e-mail. Narzędzia do monitorowania poczty e-mail mogą być używane w trybie dwukierunkowym do sprawdzania zawartości w obu kierunkach. Ponadto do monitorowania słów kluczowych lub wyrażeń, które mogą wyzwalać sygnały wczesnego ostrzegania, można użyć mechanizmów monitorowania wiadomości e-mail i filtrów treści. Każdy podejrzany ruch, załącznik lub wiadomość e-mail należy poddać kwarantannie i sprawdzić przed dostarczeniem. Skanując i blokując zawartość, organizacje mogą zmniejszyć liczbę podejrzanych wiadomości e-mail wchodzących do ich sieci i zmniejszyć liczbę podejrzanych witryn internetowych, które odwiedzają pracownicy. Usługi poczty e-mail i produkty chroniące przed złośliwym oprogramowaniem udoskonalają swoje możliwości blokowania spamu, dzięki czemu nawet oszustwa phishingowe są skutecznie wychwytywane. Postępy w badaniach technologicznych zapewnią dodatkową ochronę przed inżynierią społeczną , w tym rozwój architektury obrony inżynierii społecznej (SEDA). Ta architektura próbuje wykrywać ataki socjotechniczne przez telefon, identyfikując legalnego pracownika w porównaniu z inżynierem społecznym. System ten nazywany jest niezależnym od tekstu systemem uwierzytelniania podpisów głosowych. System wykorzystuje technologię rozpoznawania głosu, która zmniejszyłaby ryzyko udanego ataku na helpdesk. Oprócz wykrycia nieautoryzowanego dzwoniącego, może wykryć poufne informacje udające pracownika o wyższej klasyfikacji bezpieczeństwa. Rejestrowanie zawarte w architekturze pomogłoby ekspertowi sądowemu podczas dochodzenia. Metody uwierzytelniania oparte na ryzyku mogą również pomóc ograniczyć potencjalne ataki socjotechniczne; na przykład jeśli klient lub użytkownik zawsze dzwoni z określonego numeru kierunkowego lub numeru telefonu, a potencjalny napastnik dzwoni z innego numeru kierunkowego, systemy mogą to zidentyfikować i poprosić o dodatkowe informacje przed uwierzytelnieniem danej osoby. Atakujący stają się coraz bardziej wyrafinowani. Ostatnie ataki phishingowe atakują specjalistów z zakresu systemów, sieci i bezpieczeństwa. W tego rodzaju atakach wiadomość e-mail wyłudzająca informacje jest wysyłana do organizacji od „klienta" informującego ją o stronie wyłudzającej informacje próbującej ukraść informacje o kliencie. Pracownicy ochrony odpowiadają na wiadomość e-mail i sprawdzają witrynę. Witryna instaluje złośliwe oprogramowanie, które umożliwia osobie atakującej zdalne sterowanie maszyną. Ta zmiana metodologii ataku wymaga od pracowników ochrony jeszcze bardziej podejrzliwości w stosunku do wszelkich pozornie nieszkodliwych wiadomości e-mail z informacją dla organizacji, że istnieją strony phishingowe atakujące tę firmę.

ODPOWIEDŹ.

Reagowanie na socjotechnikę i inne ataki z wykorzystaniem niskiej technologii powinno pasować do procesu zarządzania incydentami i reagowania w organizacji. Podobnie jak w przypadku wszystkich planów zarządzania incydentami, odpowiedzi powinny być dobrze określone, zakomunikowane i przetestowane. Organizacja powinna planować nieuniknione, zwłaszcza że ataki sieciowe i fizyczne coraz częściej wykorzystują wiele wektorów, aby odnieść sukces.

OBRONA I ŁAGODZENIE

Zapobieganie atakom inżynierii społecznej powinno być wieloaspektowe, powtarzalne i stanowić część szczegółowej strategii organizacji. Ponieważ samą naturą ataku jest ominięcie lub obejście obrony technicznej poprzez wykorzystanie dobrej natury ludzi i chęci zaufania innym ludziom, kroki w zapobieganiu takim atakom powinny koncentrować się na odrębnych obszarach, takich jak polityka, szkolenia i świadomość, technologia i obrona fizyczna. Koncentracja na wszystkich obszarach pomoże złagodzić zagrożenie udanym atakiem socjotechnicznym. Każdy obszar powinien mieć regularny proces

przeglądu i audytu. Dobrze napisane zasady zapewniają akceptowalny poziom zachowania i potencjalne konsekwencje, jeśli nie będą przestrzegane, ale muszą być dostępne dla pracowników. W przypadku szkolenia powinno ono zostać włączone do ogólnego programu uświadamiającego w zakresie bezpieczeństwa organizacji, uwzględnionego we wszystkich ocenach pracowników i powiązanego z premiami i wynagrodzeniami. Organizacje muszą szkolić swoich pracowników w zakresie akceptowalnego zachowania oraz zapewniać zasady i narzędzia do identyfikowania i zgłaszania potencjalnych ataków socjotechnicznych. Obrona fizyczna może potencjalnie blokować intruzowi wejście do zamkniętego budynku, ale poczucie koleżeństwa sprawia, że takie praktyki, jak na przykład piggybacking lub tailgating, są stosunkowo łatwe. Ostatnie badanie wykazało, że palacze powracający do budynku czasami wpuszczają osoby postronne w bezpieczne miejsce. Postęp technologiczny jest również ważny, ale nie można na nim polegać jako jedynej metody obrony.

SZKOLENIE I ŚWIIADOMOŚĆ

Organizacje muszą zapewnić pracownikom narzędzia i wiedzę, które pomogą zidentyfikować potencjalne ataki i zareagować na podejrzane ataki. Zapewnianie świadomości jest ciągłym procesem i nie powinno dotyczyć wyłącznie nowych pracowników. Szkolenie i świadomość, tam gdzie to możliwe, powinny zawierać przykłady z życia, aby pracownicy mogli odnosić się do problemu i rozumieć poziom zaufania wynikający z ich dostępu do obiektu i danych wykorzystywanych na ich stanowiskach. Pracownicy powinni zrozumieć obowiązki powierzone im przez firmę. Zasadniczo pracownicy muszą zostać ponownie przeszkoleni, aby można było zapytać, dlaczego żąda się pewnych informacji lub zobaczyć odznakę osoby za nimi. Podstawowy program uświadamiający może obejmować plakaty, korespondencję e-mailową i laminowane karty instrukcji (twarde karty) zawierające numery alarmowe lub inne informacje. Bardziej dojrzałe programy uświadamiające mogą obejmować filmy wideo lub lunche informacyjne w brązowej torbie. Gdy tylko jest to możliwe, uczenie pracowników obrony przed atakami inżynierii społecznej powinno być prezentacją na żywo z przykładami z prawdziwego świata. Idealnie, prezentacja powinna być dostosowana specjalnie dla każdej publiczności. Na przykład, jeśli publicznością jest personel działu pomocy technicznej, przykłady potencjalnych ataków socjotechnicznych powinny zostać opisane lub przedstawione i omówione. Szkolenie pracowników może również obejmować instrukcje dotyczące zamykania szafek z plikami, gdy nie są używane, blokowania stacji roboczych i korzystania z blokad kablowych oraz zawierają instrukcje dotyczące tworzenia i zapamiętywania dobrych haseł. Podstawą szkolenia uświadamiającego jest dobrze zdefiniowany i realizowany program polityki bezpieczeństwa informacji.

TECHNOLOGIA ZAPOBIEGANIA

Technologia pojawia się jako obrona przed niektórymi rodzajami ataków socjotechnicznych. Technologia umożliwia organizacjom wykrycie niektórych ataków socjotechnicznych bez polegania na pracownikach. Ta proaktywna identyfikacja umożliwia organizacji ograniczenie ryzyka. Technologia powinna obejmować tylko jedną warstwę obrony i nie można na niej polegać jako jedynej obronie. Technologie, takie jak systemy monitorowania treści zarówno dla wiadomości e-mail, jak i treści internetowych, mogą pomóc w identyfikacji ataków phishingowych. Ponadto organizacje mogą instalować poprawki bezpieczeństwa w odpowiednim czasie oraz korzystać z aktualnego oprogramowania antywirusowego i antyspyware, aby zmniejszyć ryzyko wystąpienia wirusów, trojanów i robaków. Większość wersji przeglądarek i wtyczek do przeglądarek umożliwia użytkownikom ocenę wiarygodności stron internetowych. Idealnie byłoby, gdyby pracownicy nie mieli możliwości pobierania i instalowania niezatwierdzonego oprogramowania. Organizacje mogą jednak stosować systemy magazynowe lub inne metodologie do wykrywania nielegalnych programów w sieci. Niektóre typy systemów mogą uniemożliwić zainfekowanym komputerom dostanie się do sieci. Można zmienić konfigurację komputera stacjonarnego i laptopa, aby zmniejszyć ryzyko udanego ataku; zmiany obejmują wyłączenie wyskakujących okienek w przeglądarkach, niedopuszczenie do automatycznej instalacji formantów Active-X, wielu wersji Java, ograniczenie rodzajów plików cookie, które strony

internetowe mogą umieszczać na komputerach lokalnych, przy użyciu automatycznych wygaszaczy ekranu chronionych hasłem, a na koniec używania certyfikatów e-mail dla poświadczenie. Z tego samego względu organizacje powinny dokonać przeglądu procesów technologicznych i zweryfikować, czy nie dostarczają nieumyślnie informacji potencjalnym inżynierom społecznym. Na przykład metadane w dokumentach powinny zostać usunięte, zanim będą dostępne dla osób postronnych, i należy regularnie wyszukiwać w Internecie, aby upewnić się, że byli lub obecni pracownicy nie publikują informacji w Internecie.

BEZPIECZEŃSTWO FIZYCZNE

Mechanizmy bezpieczeństwa fizycznego mogą zmniejszyć ryzyko udanego ataku socjotechnicznego. Wszyscy pracownicy powinni mieć przy sobie karty identyfikacyjne, które muszą być zawsze widoczne. Zabezpieczone obszary w organizacji powinny być zamknięte, mieć ograniczony dostęp i być monitorowane pod kątem niezgodności. W obszarach można zainstalować alarmy drzwiowe, które mogą wykryć „tailgating" lub „piggybacking". Kamery lub inna technologia monitorowania obwodu zamkniętego może udaremnić potencjalnych intruzów. Bezpieczny personel powinien obserwować wszystkie punkty dostępu do obiektu. Wszystkie drzwi, biurka, szafki na dokumenty i inne urządzenia do przechowywania powinny mieć klucze i pozostać zamknięte, gdy nie są dostępne. Pojemniki na śmieci lub pojemniki do recyklingu powinny również posiadać zamki, które zapobiegałyby usuwaniu dokumentów przeznaczonych do niszczenia lub spalania.

* Komputery stacjonarne, laptopy i inny sprzęt komputerowy powinny być fizycznie zablokowane. Od użytkowników należy wymagać posiadania silnych haseł, a w przypadku laptopów lub komputerów stacjonarnych automatycznych wygaszaczy ekranu, które wymagają hasła do odblokowania. Wszystkie nośniki magnetyczne muszą mieć bezpieczne przechowywanie.

* Większość organizacji ma pewien procent pracowników mobilnych. Należy zapewnić im specjalne szkolenie, aby zapobiec utracie sprzętu lub informacji. Szkolenie powinno obejmować takie informacje, jak:

- Laptopy powinny pozostać przy podróżnym i nie powinny być odprawiane w bagażu.
- Laptopy powinny być przez cały czas zamknięte w bezpiecznej lub zabezpieczonej powierzchni.
- Urządzenia peryferyjne, takie jak dyski USB i urządzenia przenośne, powinny mieć silne hasła.
- Rozmowy dotyczące poufnych informacji powinny być zabronione publicznie.
- Podróżni powinni być świadomi swojego otoczenia i należy wziąć pod uwagę szczególne względy dotyczące komunikacji elektronicznej i użytkowania sprzętu, gdy nie przebywają w Stanach Zjednoczonych i Europie

UWAGI KOŃCOWE

Ataki socjotechniczne różnią się od ataków komputerowych na technologie. Wektor ataku jest ludzki, charakter ataku polega na obejściu kontroli, a powodzenie ataku zależy od gotowości ludzi do zaufania innym. Po prostu uprzejmość i otwieranie drzwi nieznajomemu może być szkodliwe dla organizacji, jeśli nieznajomy jest inżynierem społecznym. Ataki socjotechniczne nie są niczym nowym w społeczeństwie; były używane od tysiącleci. Inżynierowie społeczni wykorzystują wiele różnych metod do przeprowadzania ataków socjotechnicznych i low-tech. Metody te mogą obejmować kontakt z człowiekiem, brak kontaktu z człowiekiem lub połączenie technologii i taktyk socjotechniki. Psychologowie i psychologowie społeczni przedstawili wiele powodów sukcesu inżynierii społecznej. Teoretyzują, że ludzka natura pozwala napastnikom oszukać lub oszukać rozsądnych ludzi w celu ujawnienia informacji. Profil socjotechnika nie pasuje do jednego modelu, a ich ataki są trudne do wykrycia. Ataki socjotechniczne stały się bardziej płodne, skuteczne i niebezpieczne zarówno dla organizacji, jak i osób. Mimo, że ataki socjotechniczne są trudne do obrony, istnieją zabezpieczenia techniczne, procesowe i osobiste, które organizacja może zastosować, aby im zapobiec i zminimalizować ich skutki. Podobnie jak w przypadku wszystkich kwestii związanych z bezpieczeństwem informacji, strategia obrony niezależnej może pomóc w zmniejszeniu ryzyka

związanego z inżynierią społeczną. W okresie od lipca do sierpnia 2011 r. Firma Dimensional Research przeprowadziła ankietę wśród 835 specjalistów IT w zachodnich gospodarkach. Niektóre z ich odkryć wzmacniają potwierdzają nasze przypuszczenia:

* Zagrożenie inżynierią społeczną jest realne.
* Zyski finansowe są główną motywacją inżynierii społecznej.
* Ataki socjotechniczne są kosztowne, szczególnie w dużych organizacjach.
* [Brakuje] proaktywnego szkolenia w celu zapobiegania atakom socjotechnicznym.

Chociaż wydaje się, że praktyka zapewniania informacji koncentruje się na atakach technicznych, ataki socjotechniczne i ataki technologiczne nadal będą istotne i niebezpieczne zagrożenia, godne uwagi i łagodzenia