Alcumena
Pismo Interdyscyplinarne
Interdisciplinary Journal

Nr 3(11)/2022

DOI: 10.34813/psc.3.2022.2
www.alcumena.fundacjapsc.pl

Charakterystyka wybranych ataków socjotechnicznych w ujęciu teoretyczno-psychologicznym

Characteristics of selected socio-technical attacks in theoretical and psychological terms

Daniel Szajstek
ORCID: 0000-0003-1849-104X
e-mail: daniel.szajstek@gmail.com
Akademia Marynarki Wojennej
Wydział Nauk Humanistycznych i Społecznych

Aleksander Farysej
ORCID: 0009-0001-2076-250X
e-mail: farysejaleksander@gmail.com

This article is an overview of some of the most common cyberattacks. During the ongoing technological development, more and more users of cyberspace are exposed to social engineering attacks. Their easy preparation and effectiveness of the attack can cause serious consequences for the victims. The psychological part of the article will focus on the mechanisms that social engineers use. The psychological basis behind phishing, vishing and smishing will be described. The article will explain how the weaknesses of the human mind are exploited.

Keywords:Social engineering, phishing, vishing, smishing, osint, malware, psychology, manipulation, persuasion, influence.

Wstęp

Od końcówki XX w. jesteśmy świadkami ciągłego postępu technologicznego. Powstanie ogromnych konglomeratów tworzących technologie, z których korzystają setki milionów ludzi w codziennych sytuacjach, jest zjawiskiem powszechnie występującym. Wprost proporcjonalnie do omawianego postępu rozwijają się nowe możliwości dla szeregowych użytkowników cyberprzestrzeni, nazywanej kolokwialnie siecią internet. Zakupy z drugiego końca świata, błyskawiczna wymiana wiadomości ze znajomymi znajdującymi się na drugim końcu globu, czy połączenia na żywo to tylko jedne z licznych udogodnień, które w znaczny sposób wpływają na dotychczasowe pojmowanie jakości i standardu życia. Nowoczesne technologie dodają nowych walorów życiowych i znacząco przyczyniają się do uproszczenia wielu sfer życia. Dobrym przykładem uzmysławiającym poruszane zagadnienie jest szeroko zaawansowana bankowość elektroniczna lub portale dla obywateli, w których znajdują się wszelakie dane zdrowotne, ubezpieczeniowe lub osobiste. Jednak omawiany postęp niesie ze sobą również szereg zagrożeń. Cyberprzestrzeń, która oferuje multum możliwości, została również wykorzystana jako narzędzie do przeprowadzania ukierunkowanych ataków (zwanych incydentami bezpieczeństwa) na jej użytkowników (Szajstek 2022, s.9). Faktem niepokojącym jest tendencja do rosnącej ilości opisywanych incydentów oraz ich rozmaitość, jednocześnie świadcząca o ich zaawansowanej formie. Zjawisko to można określić jako pewnego rodzaju aktualną zarazę, którą ogólnoświatowa sieć została zainfekowana. Jak już zostało wspomniane, ataki są różne i występują pod różnymi znamionami, jednak największą uwagę przykuwają ataki socjotechniczne, nazywane również inżynierią społeczną, cieszącą się złą sławą, ze względu na jej pewnego rodzaju unikatowość, polegającą na bardzo łatwym zaimplementowaniu w praktyce, a także bardzo wysoką skuteczność w oddziaływaniu na ofiary.

Celem artykułu jest popularyzacja wiedzy, na temat licznych zagrożeń w postaci ataków socjotechnicznych wobec znikomej wiedzy użytkowników cyberprzestrzeni na temat występujących niebezpieczeństw, na które są podatni. Autorzy uważają, że zapoznanie się z literaturą w znacznym stopniu zwiększa wiedzę i świadomość, która przyczyni się do zmniejszenia potencjalnego ryzyka. Niniejsza praca ma na celu przedstawić i scharakteryzować najczęstsze ataki socjotechniczne, a także wytłumaczyć zachodzące podczas ataków mechanizmy psychologiczne.

Ataki socjotechniczne – inżynieria społeczna – zarys teoretyczny

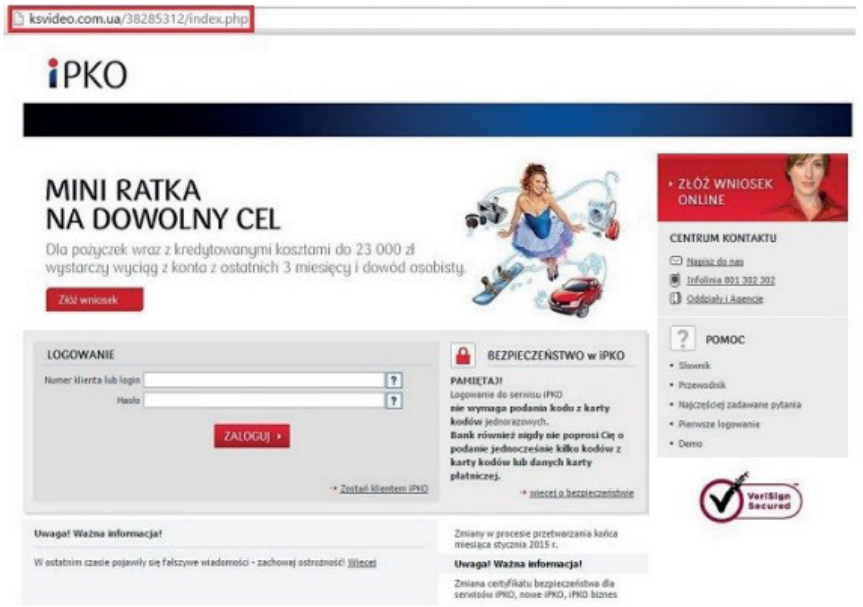
Pierwotna terminologia określa socjotechnikę jako zestaw starannie dobranych narzędzi, których praktyczne wykorzystanie daje efekt w postaci manipulacji stosowanej do osiągnięcia określonych celów. W literaturze przedmiotu można znaleźć badania wskazujące na wykorzystanie inżynierii społecznej między innymi przez stacje telewizyjne emitujące swoje programy do utwierdzenia swoich odbiorców w określonym nurcie, przemycając utwierdzony tok postrzegania występujących zjawisk w świecie rzeczywistym pod postacią najlepszych możliwych rozwiązań, gwarantujących największą skuteczność. Również często występującym przykładem są reżimy totalitarne. Ich działanie opiera się na przekształcaniu rzeczywistości, jednocześnie zyskując poparcie i nowy elektorat, który bez krzty krytycyzmu wiernie wyznaje przewijające się postulaty (Bogusz, Urbaniak, 2016, s.19). Bardzo podobny cel obiera socjotechnika wykorzystywana w atakach cybernetycznych. Prawidłowym terminem określającym omawiane zjawiska są ataki socjotechniczne (ang. social engineering). Cel przyświecający atakom socjotechnicznym nie różni się znacząco od macierzystych form inżynierii społecznej, jedynie forma przeprowadzanych manipulacji jest czynnikiem poróżniającym, ze względu na cyberprzestrzeń, w której się odbywają. Atakujący często, choć nie zawsze, bardzo starannie podchodzą do ataków. Określenie starannie obrazuje indywidualne podejście do każdej z wyznaczonych osób będących celem ataku, natomiast stwierdzenie, iż atakujący nie zawsze w sposób staranny podchodzą do wyznaczonych celów, przedstawia kolejne zjawisko, jakim są licznie występujące kampanie. Bowiem wspomniane kampanie są przeprowadzane na jak największej ilości osób. W tym przypadku słuszne będzie stwierdzenie, że dla atakującego liczy się ilość, a nie jakość. Jednak cały zamysł ataków socjotechnicznych skupia się, by podstępem zmanipulować osobę atakowaną w taki sposób, by utwierdzić ją w określonym toku prowadzanego działania, jednocześnie wykluczając wszelakie obawy i podejrzenia co do autentyczności prowadzonego działania.

Phishing

Ataki phishing'owe należą do grona najczęściej występujących i najbardziej rozpoznawalnych. Cały zamysł takiego ataku, nie licząc zastosowanej formy, opiera się na celu w postaci pozyskania poświadczeń bezpieczeństwa takich jak hasła i loginy atakowanego użytkownika, pobrania przez ofiarę złośliwego oprogramowania, czy

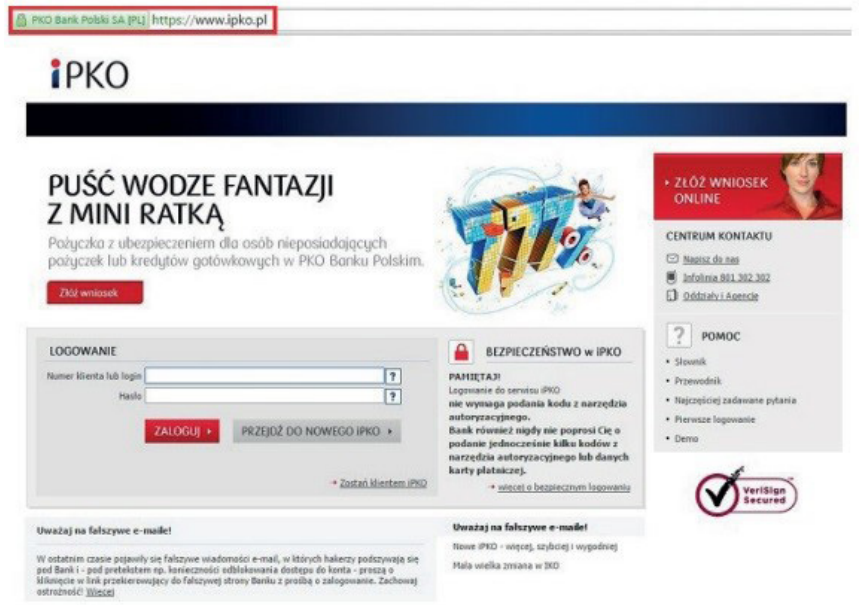
też szantażu. W wyniku jego działania, atakujący uzyskuje dostęp do kont bankowych, mediów społecznościowych lub innych istotnych z punktu widzenia atakującego danych, które mogą przynieść korzyści (Bieńkowska, Falkowski-Gilski, 2021, s.21). Użyta metoda w tego typu atakach może przybrać dowolną formę. Najczęściej adwersarze stwarzają pozory rzeczywistych instytucji lub osób, których ofiary są beneficjentami. Mogą to być na przykład specjalnie spreparowane wiadomości e-mail od banku z użytym pretekstem, że ktoś podejmuje próbę zalogowania na konto bankowe, które zostało zablokowane. Atakujący w taki sposób tworzą wiadomość, by ofiara bez chwili wątpliwości uwierzyła w jej autentyczność i podjęła się zalogowania na stronie, która została podstawiona w linku, w wiadomości email, celem odblokowania dostępu. W takim wypadku osoba, która postąpi w ten sposób, wysyła atakującemu swój login i hasło za pomocą podstawionej strony podanej w wiadomości. Istotnym faktem jest, że często atakujący bardzo dobrze modyfikują swoje wiadomości, do tego stopnia, że osoba o małej wiedzy technicznej lub dociekliwości może dać się oszukać. W celu dobrego zobrazowania poruszanego zagadnienia, poniżej zamieszczona grafika przedstawia drobne różnice pomiędzy oryginalną a spreparowaną stroną do logowania banku, zawartą w wiadomości e-mail.

Jak można zaobserwować, jedyną różnicą pomiędzy dwiema stronami internetowym jest link do nich prowadzący, choć nawet jego można odpowiednio zmodyfikować, by wyglądał identycznie jak na autentycznej stronie. Bardzo często zdarzają się kampanie phishing'owe, polegające na masowym wysyłaniu wiadomości do określonej puli internautów. Dzieje się tak ze względu na wycieki danych dużych firm, gdzie użytkownicy są zarejestrowani. Atakujący w tym przypadku skupiają swoją uwagę na ilości, lecz nie skuteczności podjętej próby ataku. Jednak równie często zdarzają się ataki ukierunkowane na konkretne osoby. Technika ta nazywa się spear-phishing i polega na przeprowadzeniu bardzo dogłębnego rekonesansu za pomocą narzędzi służących do białego wywiadu. Kluczowe jest pozyskanie informacji na tyle użytecznych do przeprowadzenia ataku, by atakujący będzie miał bardzo dobrą możliwość podszycia się pod osobę, którą udaje. W dalszej kolejności adwersarz będzie chciał się podać za osobę, która w jakimś stopniu jest związana z ofiarą. W tym wypadku atakujący często podszywali się pod przełożonych swoich ofiar, stosując jako pretekst prośbę o przelanie pieniędzy metodą BLIK lub o dostęp do zasobów znajdujących się w infrastrukturze IT firmy. Ta metoda jest bardzo skuteczna w szczególności w korporacjach i dużych firmach, gdzie czynnikiem jest dobra relacja z przełożonym, na rzecz której obiektywne i konstruktywne podejście odstawiane jest na drugi plan.



Ilustracja 1. Fałszywa strona banku

Źródło: Protasowicki I. (2016). Phishing jako zagrożenie bezpieczeństwa osobistego w sieci. Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, t. 14, z. 4(37) 2016 , s. 39.



Ilustracja 2. Autentyczna strona banku

Źródło: Protasowicki I. (2016). Phishing jako zagrożenie bezpieczeństwa osobistego w sieci. Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, t. 14, z. 4(37) 2016 , s. 39.

Vishing

Wspomniany w niniejszej pracy rozwój technologii znacząco się przyczynił do ulepszenia standardów życiowych i wpłynął pozytywnie na wiele aspektów życia. Przykładem może być digitalizacja procesów bankowych pomiędzy pracownikami a klientami banków. Długie i mozolne czekanie w kolejkach jeszcze do niedawna było zmorą każdego petenta przekraczającego próg placówek bankowych. Omawiany postęp również stanowi alternatywę na problemy tej natury. Obecnie podejście banków do swoich klientów przeszło rewolucję. Niejednokrotnie można przekonać się, iż kwestie, które jeszcze nie tak dawno były uzależnione od fizycznej obecności w banku, można rozwiązać w prosty i szybki sposób za pomocą połączeń telefonicznych. Jednak i to rozwiązanie, zostało wykorzystane przez adwersarzy do prowadzenia manipulacji, wprowadzania ludzi w błąd i przeprowadzania rozmaitych oszustw (Bolibok, Bolibok-Mataras, 2014, s.7).

Vishing to jeden z rodzajów ataków socjotechnicznych, który określa działania adwersarzy stosujących narzędzie w postaci połączeń telefonicznych do przeprowadzania ataków. Atakujący podszywają się pod osobę, która pozornie daje rękojmie zaufania i autentyczności (najczęściej podając się za pracownika banku). Celem takich działań jest pozyskanie niezbędnych informacji, za pomocą których można w szybki i łatwy sposób się wzbogacić, np. poprzez uzyskanie danych do kont bankowych lub danych kart bankowych. Sposoby są różnorakie, jednak każdemu zachowaniu o znamionach działań vishing'owych przyświeca ten sam efekt w postaci zmanipulowania oraz oszustwa (Laszczak, 2019, s.138). Powodzenie tego rodzaju ataku jest podyktowane możliwością stosunkowo łatwego przełożenia teoretycznych założeń ataku do praktycznego działania. Współcześnie istniejące możliwości informatyczne, oferujące szereg rozwiązań, wykorzystywane w tego typu atakach, przyczyniły się do zautomatyzowania połączeń telefonicznych przez atakujących, poprzez wykorzystanie botnetów. Innym, równie dobrym przykładem jest wykorzystanie podstawionych i ogólnodostępnych głosów lektorów (takich jak Ivona) przy próbach połączeń. Takie działania mają na celu zwiększyć poziom anonimowości adwersarzy.

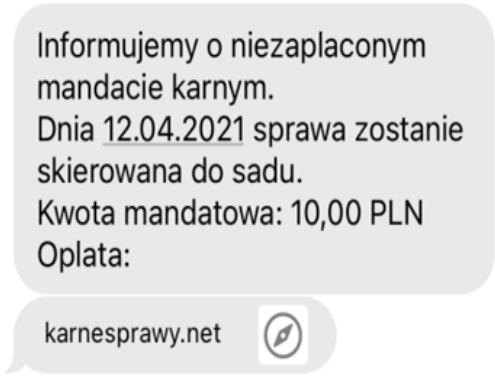
Swego czasu, wśród grup stosujących ataki vishing'owe, popularna stała się metoda „na wnuczka". Polegała ona na wyselekcjonowaniu ludzi starszych, by następnie podszyć się pod wnuka lub wnuczkę osoby atakowanej i wykorzystując jako pretekst krytyczną sytuację finansową, wymagającą szybkiego działania, wyłudzić pieniądze. Jako formę odbioru środków pieniężnych sugerowano przelew środków na wskazane konta

lub przekazanie ich za pośrednictwem rzekomych znajomych. Technika ta niestety wykazała się wysokim stopniem skuteczności, narażając na straty wielu nieświadomych seniorów.

Smishing

Smishing można określić jako pochodną od pierwotnej formy phishingu. Cel oraz sam sposób działania jest niezmienny, jedynie można dopatrzyć się różnicy w kwestii metodyki samego ataku (Laszczak, 2019, s.138). Ta metoda w swoim działaniu wykorzystuje wiadomości SMS. Grupa osób atakowanych pochodzi z wycieków danych, w których numery telefonu zostały zarejestrowane na poczet członkostwa, np. w programie lojalnościowym. Innym sposobem pozyskania danych jest wykorzystanie rachunku prawdopodobieństwa, w którym zbiór numerów jest wyliczany z potencjalnie dziewięciocyfrowych liczb. Wysyłane do atakowanych osób wiadomości charakteryzuje dobrze opracowany pretekst, którego zastosowanie będzie odnosiło się do większej ilości ofiar.

Oprócz samego działania i wyłudzeń można również dopatrzeć się bardziej zaawansowanej formy ataku. Niektóre z wiadomości SMS wręcz nakazują lub zachęcają do zainstalowania aplikacji na swój telefon, która ułatwi radzenie w stałych i cyklicznych czynnościach płatniczych. Jednak pobranie takiej aplikacji ma dość szerokie spektrum zastosowania na niekorzyść ofiary. Niektóre z omawianych aplikacji mogą kontrolować odbierane wiadomości z banku, przekierowywać na fałszywe witryny lub zawierać złośliwe oprogramowanie. Jednak najczęstszym pretekstem takich incydentów są sytuacje bazujące na zasadzie nagrody. Atakujący wymaga pewnej czynności ze strony użytkownika, którą może być np. rejestracja na portalu ukrytym w linku znajdującym się w podesłanej wiadomości. Natomiast ofertą może być nagroda w postaci dodatkowych punktów na koncie, w którym ofiara robi zakupy. Jednakże zdecydowana większość omawianych ataków bazuje na krótkiej i zwięzłej informacji, mówiącej o potrzebie przelania pieniędzy. Każdorazowo w takich wiadomościach jest przedstawiony rzekomy nadawca, którego ofiara jest beneficjentem (bank, operator komórkowy, kurier itp.). W drugiej kolejności wiadomość zawiera krótki pretekst, nakazujący wykonanie określonej czynności, w wyniku której poufność, integralność lub dostępność zostają naruszone. Poniższa grafika przedstawia autentyczną próbę takiego omawianego ataku.



Ilustracja 3. Atak vishing'owy

Źródło: https://niebezpiecznik.pl/post/uwaga-sms-mandat-karny/

Należy pamiętać, że rozwój zagrożeń w cyberprzestrzeni jest wprost proporcjonalny do rozwoju zasobów teleinformatycznych. Każdorazowo w sytuacjach o znamionach uwzględnionych w niniejszej pracy, powinna pojawić się dociekliwość, podejrzliwość, a także rozsądny i konstruktywny krytycyzm, bowiem takie podejście może uchronić przed poważnymi konsekwencjami. Adwersarze to osoby, które cechuje wysoki poziom inteligencji — potrafią, nie znając ofiary, zmanipulować ją w taki sposób, że spełni określone warunki, w wyniku których spełnią zamierzony przez atakującego cel. Hakerzy łamią ludzi nie hasła (Mitnick, Simon, 2003).

Metodologia psychologiczna

Postępy w technologii komunikacji cyfrowej sprawiły, że komunikacja między ludźmi stała się bardziej dostępna i natychmiastowa. Systemy pozwalające ludziom nawiązywać kontakt nie są jednakże pozbawione wad. Brakuje im odpowiedniej ilości zabezpieczeń, przez co dostęp do danych stał się ułatwiony. Jednym ze źródeł tego zjawiska jest sam człowiek. Przez to, że kontakt w sieci jest bezpośredni, ludzie są bardziej narażeni na wszelkiego rodzaju ataki socjotechniczne. Metody ich działania, które oparte są na psychologii, sprawiają, że tego rodzaju manipulacje są jednym z największych zagrożeń, przed którymi stoi Internet. Dzieje się tak, że wykorzystywana jest ludzka tendencja do ufności, brak dostatecznej wiedzy, strach czy presja. Tego typu mechanizmy są podstawą wszystkich ataków socjotechnicznych.

Zdobywanie informacji

Pierwszą rzeczą przy przygotowaniu ataku socjotechnicznego jest zebranie danych. W poprzedniej części artykułu były wspomniane metody podszywania się poprzez bezpośrednią komunikację np. telefoniczną (vishing), mailową (phishingu) czy SMS-ową (smishing). Wiedza o tym jak wyglądają ataki jest równie istotna jak stojąca za nimi metodyka. Jednym z głównych źródeł informacji jest człowiek. Atakujący poprzez sprawną komunikację potrafią wyciągnąć od nic nieświadomych ofiar bardzo dużo danych. W literaturze do zobrazowania tych działań korzysta się z porównania osób korzystających z socjotechniki do sprzedawców (Hadnagy, 2011, s.49). W obu przypadkach odpowiednie formułowanie pytań jest w stanie wydobyć od ofiary wiele informacji. Sprzedawca zbiera informacje od swojego obecnego klienta, a następnie bazuje na nich w sposób, który sprawi, że „cel" będzie bardziej podatny na kontynuowanie rozmowy i wykaże rosnące zainteresowanie. Ponadto, używając słów takich jak „premium" i „z góry", sprzedawca wstępnie obciąża nowy cel słowami kluczowymi, których za chwile przeciwko niemu użyje.

Ten sam schemat działania występuje w socjotechnice. Wykorzystywane są identyczne mechanizmy, lecz zmienia się wykorzystane słownictwo. Atakujący mogą podszyć się przykładowo pod konsultanta banku, technika sieciowego, funkcjonariusza czy pod osobę sprzedającą coś w sieci. Techniki te są skuteczne dzięki temu, że budują zaufanie. Socjotechnicy używają podobieństw (z reguły sfabrykowanych) między sobą a celem, przez co rozmówca zaczyna czuć się bardziej komfortowo, jednocześnie niwelując dystans, który ich dzieli. Socjotechnik nigdy nie będzie pytał o newralgiczne informacje na samym początku. Spowoduje to tylko strach i podejrzliwość. Częstym zjawiskiem jest, że braki informacyjne atakującego są nadrabiane podczas rozmowy. Na im więcej pozornie nieistotnych pytań ofiara odpowie, tym większą pewność i wiedzę będzie zyskiwał manipulator. Przykładowo, zamiast dopytać bezpośrednio o korzystanie z sieci VPN może paść pytanie typu: „Nasz system zarejestrował próbę logowania z państwa poza Unią Europejską. W ramach bezpieczeństwa chciałbym zapytać, czy mógłby Pan/Pani potwierdzić te informacje". Ofiara nie jest świadoma, że tak skonstruowane pytanie nie dość, że dostarczy informacji na temat czy dana osoba używa VPN, ale także może zdradzić, czy znajduje się obecnie w tym samym kraju co pytający. Ludzie w pewnym sensie spodziewają się tego typu pytań (przykładowo, gdy ktoś podaje się za pracownika banku) i podchodzą do nich z brakiem sceptycyzmu. Problemem jest to, że szanse powodzenia rosną wprost proporcjonalnie do wiedzy o ofierze.

Osoby, których informacje są łatwo dostępne publicznie (np. prowadzą własny biznes w Internecie) na stronach internetowych, portalach biznesowych czy mediach społecznościowych powinny być wysoce świadome, jakiego rodzaju są to dane. Często zamieszczane są informacje dotyczące dzieci, biznesu, domu czy innych części życia. Socjotechnik, mając do dyspozycji tego typu informacje, nie będzie miał problemu w zbudowaniu zaufania z drugą osobą, wykorzystując te dane. Zbieranie informacji w taki sposób nazywa się białym wywiadem (Hrabiec-Hojda, Trzeciakowska, 2019, s.176). Sposobem na ograniczenie skuteczności takich działań jest świadomość, jakie informacje dotyczące nas samych są w sieci oraz możliwe jak największe ograniczenie ich ilości.

Perswazja

Podstawą w atakach socjotechnicznych jest psychologia perswazji (Uebelacker, Quiel, 2014, s.24). Większość ocen i decyzji w życiu człowiek podejmuje, opierając się na heurystyce. Pozwala to w naturalny sposób zmniejszyć obciążenie poznawcze mózgu poprzez ograniczenie się tylko do wybiórczej analizy każdej pojawiającej się sytuacji. Jednakże takie podejście nie jest odpowiednio dostosowane do wszystkich sytuacji, co może rodzić możliwości na wykorzystanie tej chwili braku czujności. Takie momenty są pożądane przez osoby chcące użyć socjotechniki. Pozwala to im na zmanipulowanie ofiar do wykonania działań lub ujawnienia informacji. Działania te mogą zostać wzmocnione (będąc ułatwieniem) poprzez silne afekty, brak motywacji, brak wiedzy na poruszany temat, niewystarczający poziom zdolności poznawczych do prawidłowego przetworzenia wiadomości, brak asertywności czy łatwowierność (Kusev i in., 2017, s.102). Każda z tych rzeczy składa się na wpływ, jaki atakujący ma na ofiarę. Podstawą tego jest perswazja. Dobrze znana metoda, która jest również wykorzystywana w kilku innych dziedzinach nauki takich jak sprzedaż, marketing czy ubezpieczenia. R. Cialdini w swoich pracach dotyczących marketingu wskazał na 6 głównych zasad wpływu na drugą osobę, które są podstawą w socjotechnicznych atakach opierających się na perswazji (Cialdini, Goldstein, 2004, ss.591-621).

Pierwszą z nich jest autorytet. Sprawia on, że ludzie, którzy są pod jego wpływem, dają się przekonać do zachowań, które stoją w kontrze do ich przekonań czy zasad moralnych. Dobrym tego przykładem był eksperyment Stanleya Milgrama (Milgram, 1965, ss.57-76), który udowodnił, jak autorytet nawet sztucznie nadany silnie oddziałuje na zachowanie ludzi. Jest to dodatkowo ułatwione w konwersacjach telefonicznych,

a więc w oszustwach opisanych w tym artykule, czyli: phishingu i smishingu. Bardzo popularnym sposobem jest podszywanie się pod konsultanta banku, z którego korzysta ofiara. Szybko i z dużą pewnością siebie podane sfałszowane dane osobowe oraz numer pracownika buduje w ofiarach poczucie, że rozmówca jest rzeczywiście konsultantem.

Drugą zasadą stosowaną przez atakujących jest zaangażowanie w połączeniu z konsekwencją. Polega to na utwierdzaniu osoby manipulowanej w sytuacji, w której się znajduje i tego czego jest ona pewna. Oznacza to, że ofierze (przywołując vishing konsultanta banku) jest stale przypominane, że ma do czynienia z osobą pracującą w banku, że sytuacja jest pod kontrolą, wszystko to jest rutynowym działaniem, które ma na celu bezpieczeństwo konta etc. Z biegiem czasu, gdy ofiara czuje się coraz bezpieczniej, manipulujący nakierowuje ją na osiągnięcie swojego celu.

Trzecią zasadą jest zasada wzajemności. Ma ona swoje podstawy w normie społecznej, która obliguje osoby, które coś otrzymały do zwrócenia przysługi. Zasada ta jest szczególnie skuteczna, gdy poziom zaufania między atakującym a ofiarą jest już wysoki. W niektórych przypadkach poprawne wykorzystanie zasady wzajemności może skutkować tym, że osoba, na której tę technikę manipulacji się stosuje, zwróci dającemu więcej, niż sama otrzymała.

Kolejną z zasad jest sympatia. Jest ona w teorii najprostsza, lecz nie zawsze ma to odwzorowanie w praktyce. Osobę, którą lubimy łatwiej obdarzyć zaufaniem czy zrobić to, o co nas prosi. Wstępną sympatię można budować na przykład na prostych rzeczach takich jak wspólna data urodzin czy takie samo imię. Użycie tego typu informacji podczas ataku socjotechnicznego może znacząco podnieść szansę jego powodzenia poprzez utrzymanie osoby manipulowanej z dala od podejrzliwych myśli, czy niepewności.

Piątą zasadą jest tak zwany dowód społeczny. Jest on podobny do budowania zaufania poprzez sympatię, lecz w tym przypadku podstawą nie jest rzecz względnie trywialna jak podobieństwo imion czy fakt posiadania psa. Dowód społeczny opiera się na adaptacji zachowań oraz przekonań osób, z którymi ma się kontakt w celu osiągnięcia akceptacji społecznej. Posiadanie tych samych opinii, szczególnie na tematy niejednoznaczne lub wywołujące społeczny dyskurs, wzmacnia poczucie zaufania między osobami. Tak samo w tym jak i w poprzednim przypadku, tego typu metody są szczególnie niebezpieczne, gdyż wszystkie fakty, które w teorii mają łączyć ofiarę i atakującego mogą w pełni mijać się z prawdą.

Ostatnią z metod, która jest również nagminnie używana w marketingu, jest zasada niedoboru. W uproszczeniu polega na zwiększaniu wartości rzeczy poprzez zmniejszenie jej dostępności. Dowodzi ona temu, że człowiek na niedobór reaguje zwiększoną

chęcią posiadania. Ma to swoje zastosowanie nie tylko do rzeczy materialnych, lecz także informacji, które także stają się bardziej wartościowe, im ciężej je się zdobywa.

Wpływ społeczny

Wpływ społeczny jest kolejnym istotnym narzędziem w socjotechnice. Polega on na celowej lub nie, zmianie zachowania drugiej osoby poprzez przetwarzanie peryferyjne. Podstawą tego działania jest pozostawienie ofiary w stanie nieświadomości wywieranego na niej wpływu. Zależnie od typu ataku wyróżnia się różnego rodzaju wpływy społeczne (Siddiqi, Pak, Siddiqi, 2022, s.7). Pierwszym jest konformizm występujący w grupach. Polega on na wpływie grupy na poszczególną jednostkę. Atakujący może stworzyć grupę zapełnioną sztucznymi kontami czy botami i poprzez zainfekowany link udostępniony na forum zdobyć informacje od ofiary. Kolejnym przykładem jest wpływ normatywny, który działa w sposób wykorzystywania informacji do stworzenia sytuacji, gdzie osoba manipulowana jest przekonywana do zainstalowania darmowego oprogramowania, podpierając się łatwością użycia lub ograniczonym czasem dostępności. Teoria wymiany społecznej, która jest istotnym czynnikiem odwróconych ataków technicznych, o których będzie mowa w dalszej części artykułu, działa wykorzystując świadome lub nieświadome wartościowanie informacji u ludzi. Najlepszym tego przykładem jest wymiana przysług. Możliwe są też przypadki, gdzie niekoniecznie musi wystąpić wymiana. Wystarczy sytuacja, gdzie to ofiara zrobić coś dla osoby atakującej co podświadomie stawia ją w bezpiecznej pozycji. Kolejną metodą jest wpływ moralny nazywany także odpowiedzialnością społeczną. Może być ona wykorzystana na dwa sposoby. Pierwszą jest wykorzystanie dobrodusznej natury człowieka, aby wydobyć od niego informacje (brak asertywności) lub zyskać przychylność co ułatwi kolejne kroki ataku. Drugą jest wywarcie presji poprzez odwołanie się do moralnego obowiązku. Gdy ofiara nie jest chętna, by sama z siebie zaangażować się w proces ataku, to może zostać do tego niejako zobligowana przykładowo poprzez sfabrykowanie historii, która miałaby wywołać współczucie. Ostatnią z metod jest budowanie relacji poprzez podobieństwa. Polega na wspomnianym wcześniej budowaniu zaufania i pozytywnych odczuć poprzez prostą, często sfabrykowaną zgodność między rozmawiającymi. Tego typu wpływy bardzo często działają podświadomie i niezwykle ciężko je wychwycić komuś, kto nie jest świadomy przekroju ich działania.

Programowanie językowe

Posiadanie informacji dotyczących metod socjotechnicznych nie zda się na wiele, jeżeli nie będą one wykorzystane w przekonujący sposób. Podstawą dobrej komunikacji oraz manipulacji jest odpowiednie wykorzystanie języka. Tak jak w języku programowania, człowiek słyszy słowa jako wejście, przetwarza informacje, a następnie generuje odpowiedź jako wyjście. Istotnym jest dobranie odpowiedniego słownictwa, które w wyczerpujący sposób wyjaśni kontekst tematu oraz odpowiednio wyrazi uczucia. Oznacza to, że tworzenie i opracowywanie metod ataków socjotechnicznych w dużym stopniu opiera się na języku, który jest używany do interakcji z ofiarą (Handoko, Putri, 2019, s.2-3). W podrozdziale dotyczącym zbierania informacji było wspomniane, że istotą socjotechniki jest sposób komunikacji. Poznawcze uprzedzenie, które opiera się na ramach językowych, może prowadzić do bardzo prostych błędów poznawczych. Produkt, który zawiera 80% składników pochodzenia naturalnego, będzie brzmiał bardziej atrakcyjnie niż ten, który zawiera 20% sztucznych składników. Ofiary są bardzo podatne na tego typu sposób myślowy. Podobnie działa dezorientacja myślowa (Yasin i in., 2021, s.2). Doprowadza się do niej poprzez wywołanie zmieszania i niepewności wykorzystując do tego wypowiedź, która jest oparta w dużej mierze na domniemaniach i niejasnym znaczeniu. Przykładowo stwierdzenie „coś nas przerywa" może zachęcić ofiarę do upewnienia się, czy aby na pewno jej sieć działa w poprawny sposób lub czy sprzęt wymaga regulacji. Daje to duże pole do manipulacji i potrafi dać informację manipulatorowi, w jakim kierunku idzie tok myślenia ofiary. Język jest podstawą w atakach socjotechnicznych, gdyż to on sprawia czy dana metoda jest odpowiednio przekonująca i ma szanse powodzenia. Używanie także sfałszowanych stopek w mailach czy odpowiednie słownictwo może znacząco przyczynić się do skutecznego ataku poprzez zbudowanie poczucia przekonania w ofierze, iż w istocie jest w kontakcie z konsultantem banku lub funkcjonariuszem.

Odwrócone ataki socjotechniczne

Metody manipulacji są na tyle różnorodne, iż nie opierają się one tylko na atakującym jako punkcie wyjścia. Tak zwane odwrócone ataki socjotechniczne (Reverse Social Engineering Attacks) polegają na tym, że osobą inicjującą kontakt jest ofiara (Krombholz i in., 2015, ss.113-122). Atakujący wmanipulowuje swój cel poprzez perswazję i inne techniki opisane wcześniej. Tego typu atak ma miejsce w kontekście opisanych wcześniej phishin-

gu, vishingu oraz smishingu. Reverse Social Engineering przebiega w trzech podstawowych krokach (Salahdine, Kaabouch, 2019, s.89).

Pierwszym jest stworzenie problemu jak na przykład niesprawnie działająca sieć, zagrożenie na koncie bankowym lub innego rodzaju problem wymagający wiedzy technicznej lub pomocy osób trzecich. Gdy ofiara jest już w pozycji, w której nie jest w stanie samodzielnie poradzić sobie z zaistniałą sytuacją, wtedy wkracza atakujący, który ukazuje się jako jedyna osoba będąca w stanie pomóc ofierze. W ten sposób kontakt nie jest inicjowany ze strony agresora, co dodatkowo buduje większą pewność poprzez zbudowanie fałszywego poczucia panowania nad sytuacją. Ofiara jest pozbawiona podejrzeń, gdyż to ona inicjuje kontakt. Trzecim krokiem jest pomoc atakującego w rozwiązaniu problemu, z jednoczesnym zdobyciem pożądanych informacji, nie będąc zdemaskowanym na żadnym etapie działania. Ofiara może dowiedzieć się o tym, że została oszukana po czasie, co daje dodatkowy czas manipulatorowi na zatuszowanie śladów.

W tego typu działaniach wykorzystywana jest niedostateczna wiedza techniczna osób atakowanych oraz obniżona czujność związana z tym, że uwaga nie jest skupiona na osobie, do której zwraca się o pomoc a na samym problemie. Potrafi to przysłonić niektóre proste fakty, które mogłyby zapobiec byciu oszukanym jak na przykład podejrzliwość co do danych atakującego, jego umiejętności (czemu tylko on może pomóc?) czy samodzielnego znalezienia kontaktu do osób, które będą w stanie pomóc (np. kontakt zamieszczony na stronie banku). Faktowi, iż specjalistyczna wiedza techniczna nie jest powszechna nie pomaga to, że osoby korzystające z sieci nie przywiązują wagi do bezpieczeństwa swoich danych w Internecie (Farysej, 2021, s.65). Doprowadza to do zwiększenia się podatności ludzi na ataki socjotechniczne. Im więcej informacji o użytkowniku w sieci, tym większa wiedza atakującego. Przekłada się ona również na siłę perswazji, a co za tym idzie szansę powodzenia samej manipulacji.

Podsumowanie

Socjotechnika jest dziedziną, która – jak udowodnił to powyższy artykuł – tworzy wiele niebezpieczeństw przed każdym użytkownikiem internetu. Jej specyfika, która charakteryzuje się stawianiem za cel człowieka, a nie komputer sprawia, iż ochrona przed nią staje się ciężkim zadaniem. Coraz większa digitalizacja życia sprawia, że dużą część codziennych czynności załatwia się poprzez komputer lub telefon. Sprawia to, że spada czujność wobec potencjalnych zagrożeń. Umiejętność rozpoznania i zapobiegnięcia ich negatywnym skutkom jest celem, który przyświecał autorom tego

artykułu. Najlepszą obroną przeciwko atakom typu phishing, vishing czy smishing jest zdroworozsądkowe podejście, świadomość ich istnienia oraz sposobu działania. Przedstawione powyżej ataki, ich przekrój oraz kolejne etapy pozwolą użytkownikom Internetu na zachowanie bezpieczeństwa i podniesienia poziomu cyber-higieny.

Bibliografia

Bieńkowska D., Falkowski-Gilski P. (2021). Nauka w świecie cyfrowym okiem młodego inżyniera - phishing w mediach elektronicznych. *Pismo PG, Nr 5(256) Rok XXVIII*, ss. 21-26.

Bogusz M., Urbaniak M. (2016). *Socjotechnika – Inżynieria społeczna w życiu codziennym*.

Bolibok P., Bolibok-Mataras A. (2014). Bankowość mobilna jako innowacyjny kanał dostępu do usług bankowych. *Rocznik Ekonomii i Zarządzania t.6(42) nr.2*, ss.7-22.

Cialdini, R. B., Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology, 55(1)*, ss.591-621.

Farysej, A. (2021). *Badanie świadomości użytkowników Internetu dotyczącej bezpieczeństwa danych i prywatności w sieci*. Uniwersytet Gdański.

Gass, R.H. (2015). *International Encyclopedia of the Social & Behavioral Sciences, 2nd ed.*; Elsevier: Houston, TX, USA, s.348–354.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Handoko, H., Putri, D. (2019). *Threat language: Cognitive exploitation in social engineering*. [W:] Proceedings of the first International Conference on Social Sciences, Humanities, Economics and Law, September 5-6 2018, Padang, Indonesia, s.2-3.

Hrabiec-Hojda, P., Trzeciakowska, J. (2019). Techniki wyszukiwania informacji w mediach społecznościowych dla celów białego wywiadu. *Studia Politologiczne, 54*, ss.175-190.

Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, ss.113-122.

Kusev, P., Purser, H., Heilman, R., Cooke, A. J., Van Schaik, P., Baranova, V., ... Ayton, P. (2017). Understanding risky behavior: The influence of cognitive, emotional and hormonal factors on decision-making under risk. *Frontiers in psychology, 8, Article 102.*

Laszczak M. (2019). Zarządzanie bezpieczeństwem w erze cyfrowej. *Bezpieczeństwo. Teoria i Praktyka, (4)*, ss.135-150.

Milgram, S. (1965). Some Conditions of Obedience and Disobedience to Authority, *Human Relations, vol. 18, no. 1.* ss.57–76.

Mitnick, K., Simon, W. (2003). *Sztuka podstępu. Łamałem ludzi, nie hasła*. Gliwice: Wydawnictwo Helion.

Protasowicki I. (2016). Phishing jako zagrożenie bezpieczeństwa osobistego w sieci. *Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, t. 14, z. 4(37) 2016*, ss. 35-46.

Salahdine, F., Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11(4)*, Article 89.

Siddiqi, M. A., Pak, W., Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences 12(12): 6042*.

Szajstek D. (2022). *Cyberbezpieczeństwo jako wyzwanie XXI wieku*. Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni.

Uebelacker, S., Quiel, S. (2014). *The social engineering personality framework*.

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., Wei, Z. (2021). Understanding and deciphering of social engineering attack scenarios. *Security and Privacy, 4(4)*.