**Socjotechnika- Badania wpływu na poszczególne grupy wiekowe oraz sposób reagowania.**

Wasiak Damian, Tomasz Uryga, Patryk Wołożonek

Politechnika Opolska

**Słowa kluczowe:** Socjotechnika ,cyberataki, bezpieczeństwo, podatność grup wiekowych na atak , reagowanie na atak

ABSTRACT

Przeprowadzone badanie miało na celu sprawdzenie zachowań określonych grup ludzi w przypadku ataku cybernetycznego. Odpowiedzi na konkretne pytania były pozyskiwane w sposób anonimowy od grupy ankietowanych. Pod uwagę brano czynniki takie jak wiek badanych oraz czas spędzany dziennie w Internecie. Zauważono , że badani spędzający najwięcej czasu na co dzień w sieci , są bardziej zdecydowani i samodzielni w razie ataku oraz podejmują częściej właściwe kroki prewencyjne. Grupa spędzająca mniej czasu w większości przypadków przekierowuje konsekwencje ataku jednostkom zewnętrznym i częściej oświadcza , że nie wie jak postąpić w takim wypadku. Biorąc pod uwagę wiek , badani , uważani powszechnie za spędzających najwięcej czasu w Internecie (16-29lat), reagują najlepiej, w porównaniu do innych grup wiekowych.

SOCJOTECHNIKA W TEORII

Socjotechnika stosowana jest od bardzo dawana aż po dzień dzisiejszy, mówi się że sięga tysięcy lat wstecz - oszustwa i naciągacze to przecież nic nowego. Jest pewnego rodzaju atakiem psychologicznym

polegającym na tym że atakujący nakłania swoją ofiarę do wykonania jakieś czynności. Chociaż w codziennym życiu wiele osób błędnie uważa że crackerzy (internetowi przestępcy) używają zaawansowanych narzędzi i technologii, aby włamać się do komputerów, na konta internetowe czy też urządzenia mobilne a w większości przypadków jest to po prostu oszustwo wybranej osoby lub danej grupy osób lub nawet wielkiej korporacji jak robił to Kevin Mitnick. Techniki używane przez cyberprzestępców możemy podzielić na wirtualne, fizyczne i mieszane (hybrydowe).

Przykładem spear-phishingu, wzbogaconego dodatkowo o metodę fake news jest wykonanie przez hakera telefonu do osoby odpowiedzialnej za Public Relations z prośbą o wypowiedź odnośnie głośnej afery związanej z firmą. Niepodejrzewająca niczego ofiara dopytuje o jakiej aferze mowa, na co rzekomy dziennikarz przesyła na jej skrzynkę mailową link do spreparowanego artykułu o chwytliwym tytule np. „Firma X zamyka oddział w Poznaniu. Szykują się masowe zwolnienia”. Po chwili na stronie pojawia się popup, zawierający link do wirusa. Ofiara klika, żeby zamknąć go i wznowić lekturę artykułu, a wirus trafia prosto do jej komputera. Co więcej, jeśli prześle ona stronę kolejnym osobom w firmie — co prawdopodobnie nastąpi — w niedługim czasie wirus obejmie całe przedsiębiorstwo. Kiedy mowa o hakerach, wielu ludzi wyobraża sobie zakapturzonego mężczyznę, siedzącego w ciemnym pokoju, który rozświetlona tylko blask ekranu komputera. Ten znany z okładek gazet obraz, niekoniecznie dobrze odzwierciedla rzeczywistość. Hakerzy działają też w świecie rzeczywistym — i to z sukcesami.

Jedną z socjotechnik jest przebranie. Haker może pojawić się w firmie, na przykład udając serwisanta znanej firmy usługowej, któremu rzekomo zlecono zainstalowanie sterowników do drukarki. Wybierze przy tym idealny moment, kiedy w biurze nie ma akurat żadnej osoby, która mogłaby potwierdzić, czy faktycznie wzywano fachowca. W rezultacie, nie chcąc niepokoić szefa telefonami po godzinach, pracownik udostępni serwisantowi komputer celem zainstalowania sterowników i w pakiecie z nimi otrzyma złośliwe oprogramowanie. Wśród cyberprzestępców popularne jest też łączenie metod wirtualnych i fizycznych. Wszystko po to, aby przeprowadzać jeszcze skuteczniejsze ataki. Przekonali się o tym pracownicy warszawskiej korporacji, którzy kilka miesięcy temu otrzymali na służbowe maile informację o otwarciu nowej pizzerii i 30% zniżce dla pierwszych klientów. Podekscytowani szybko zorganizowali w firmie Pizza Day. Do biura trafiło 8 pudełek pizzy oraz gratis w postaci LED-owych lampek na USB — oczywiście zainfekowanych wirusem. Niepodejrzewający niczego pracownicy natychmiast podpięli prezent do swoich komputerów, dając do nich zdalny dostęp hakerom.

Inżynieria społeczna, inżynieria socjalna, socjotechnika (ang. social engineering) – w politologii, socjologii i marketingu: zespół technik służących osiągnięciu określonych celów poprzez manipulację społeczeństwem. Innymi słowy jest to celowe, przemyślane przekształcanie społeczeństwa.

Stanowi jedną z najważniejszych form oddziaływania aparatu państwowego, partii politycznych i elity władzy na tych: -których się już kontroluje; -których się pragnie kontrolować; -którzy przeszkadzają w sprawowaniu pożądanej kontroli. Socjotechnika może być stosowana dla dobra społeczeństwa, zaś reżimy totalitarne wykorzystały socjotechnikę do utrzymania władzy. Manipulacja prowadziła często do rozniecania negatywnych uczuć jak strach, agresja i nienawiść.

Hakerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku. Wyszukują przy tym najsłabszy punkt systemu bezpieczeństwa, którym jest człowiek. Oszuści komputerowi często podają się za inne osoby, aby wyłudzić od swoich ofiar cenne dane. Cracker może dla przykładu podać się za administratora banku i przesłać ofiarom adres swojej strony, która łudząco przypomina stronę banku internetowego. Dzięki opanowaniu inżynierii socjalnej oszust wie, że przeciętny użytkownik nigdy nie sprawdza, czy strona jego banku jest oznaczona kłódką symbolizującą nawiązanie bezpiecznego połączenia. Nieostrożni klienci pozostawiają internetowemu złodziejowi swoje dane, które ten może wykorzystać do oczyszczenia ich kont z pieniędzy.

Działanie opisane w tym przykładzie określane jest mianem phishingu. Mimo wysokich kosztów ponoszonych przez większe przedsiębiorstwa na zapewnienie bezpieczeństwa, które obejmują zakup wyspecjalizowanej infrastruktury (np. zapora sieciowa) czy zatrudnianie najlepszych administratorów dbających o stałe aktualizowanie oprogramowania, wysiłki mogą okazać się bezowocne, jeżeli każdy pracownik nie zostanie poddany szkoleniu uczącemu go technik obrony przed inżynierią społeczną. Stosowanie technik inżynierii społecznej w celu uzyskania dostępu do danych w sposób nieuprawniony (bez zgody drugiej strony lub bez postanowienia wydanego przez prawomocny organ) jest przestępstwem ściganym przez prawo polskie. Podszywanie się pod inną osobę oraz przejmowanie informacji niejawnych jest zagrożone karą pozbawienia wolności. Instytucje publiczne oraz przedsiębiorstwa muszą wprowadzać systemy uwierzytelniania osób kontaktujących się z pracownikami przedsiębiorstwa elektronicznie.

Konieczne jest ciągłe podnoszenie kwalifikacji wszystkich pracowników posiadających dostęp do informacji niejawnych w zakresie zasad bezpieczeństwa teleinformatycznego. Podstawowe metody socjotechniki to np. perswazja, manipulacja, intensyfikacja lęku. Mimo, że wymienione różnią się od siebie w sposobie i skutku działania, łącza się w nacisku wywieranym na drugiego człowieka. Przykładowe techniki: zdanie większości – nic innego jak twierdzenie, że wszyscy tak mówią i podzielą tą opinie, to społeczny dowód słuszności; bo jak większość coś uważa, to pewnie jest to dobre i potwierdzone pozorny wybór – masz przedstawione kilka punktów widzenia, ale ten, który jest wyborem mówiącego jest przedstawiony w pozytywnym świetle i w superlatywach autorytet – odwołanie się do znanego i powszechnie cenionego autorytetu zawsze pozytywnie wpływa na nasze zdanie (zasada autorytetu) niezależne zdanie – mówiący tak formułuje zdanie, że masz wrażenie, że nie zależy mu na przekonaniu Cię do niego; a jeżeli nie nalega i nie jest natarczywy, to szybciej wzbudzi zainteresowanie ośmieszenie – mówiący stara się ośmieszyć nieodpowiadające mu założenia selekcja faktów – manipulujący wybiera do przekazu tylko te fakty, które są dla niego wygodne i pozwalają przeforsować swoje zdanie wskazanie wroga (negatywnych grup odniesienia) – mówiący sprytnie wskazuje wspólnego wroga, który chce zakłócić wspólne dobro, tym bardziej powoduje koncentracje grupy wokół swoich przekonań zamiana nazw (nowomowa) – czyli tworzenie nowych pojęć, którym nadaje się silne tło emocjonalne, po to by wykorzystywać je w przekazie do znającej temat grupy kłamstwo – najprostsze i najbardziej nieetyczne zachowanie; mówiący celowo zataja pewne fakty i ogranicza dostęp do źródeł informacji stereotypy – manipulator wykorzystuje utarte stereotypy i sam tworzy nowe, aby później wykorzystywać je w swoim przekazie, wzmocnić jego siłę tło emocjonalne – wzbudzenie przez manipulującego pozytywnego odbioru pozwala mu na szybsze i szersze docieranie ze swoim przekazem, przecież jak ktoś ma sympatyczny wizerunek to pewnie mówi prawdę (3 zasady lubienia) slogany – tworząc własny slogan, można go rozpowszechnić i zakorzenić w umyśle odbiorców; rozpoczyna się identyfikacja osoby, marki

NARZĘDZIA POMIAROWE

Narzędzia pomiarowe , które wykorzystaliśmy do naszego badania to formularze Google forms , z wykorzystaniem dodatku Advanced Summary by Awesome Table, który umożliwia filtrowanie odpowiedzi respondentów, według podanych przez nich parametrów, tj. wiek , ilość spędzanego czasu oraz przeszłe doświadczenie z internetowym oszustwem.

METODOLOGIA BADAŃ

Technika zastosowana w naszym badaniu to anonimowe ankiety internetowe zawierające pytania zamknięte. Dotyczyła ona ogólnego pojęcia i postepowania w przypadku ataków w sieci . Mierzyliśmy ilość poprawnych odpowiedzi do zadanych pytań z ankiety. Parametry, które były zmienne dotyczyły wcześniej wspominanego „obycia” w Internecie. To oznacza, że odpowiedzi pochodzą od osób , które mają odmienne doświadczenia oraz spędzają różną ilość czasu dziennie w sieci. Jest też brany pod uwagę ich wiek, co może dać dodatkowy obraz na dane zagadnienie. Wnioski zostają wyciągnięte na podstawie ilości poprawnych odpowiedzi, dotyczących zadanych pytań. Weryfikacja wyników została zapewniona poprzez pytania zamknięte, ponieważ nie dało się w tym przypadku popełnić błędu technicznego, udzielając odpowiedzi. Sama rzetelność uzyskanych odpowiedzi została zapewniona poprzez anonimowość ankiety ,gdyż sprawia , że respondenci chętniej odpowiadają zgodnie z prawdą.

WNIOSKI I DYSKUSJA

Wyniki dzielimy głównie na 3 kategorie. Jest to związane z tym , że respondenci posiadają w różnym stopniu dane czynniki: - ilość spędzanego czasu - wiek - doświadczenie z oszustwem w Internecie

Z racji krótkiego czasu użytkowania Internetu , grupa mniej niż 1h dziennie jest prawdopodobnie najmniej świadoma konsekwencji ataku ,więc podejmuje radykalne i tradycyjne metody radzenia sobie w sytuacji utraty kontroli nad urządzeniem.

Użytkownicy z grupy 2-4h dziennie są nieco bardziej samodzielni, gdyż wykorzystują głównie metody zmuszające do ich samodzielnego przeprowadzenia, natomiast nie są to najlepsze decyzje.

Użytkownicy grupy ponad 5 h dziennie są również samodzielni i podejmują radykalne i prawidłowe decyzje, które niejako „odcinają” urządzenie od źródła ataku. W przypadku poważniejszych konsekwencji, które są w stanie przewidzieć, zgłaszają sprawę na policję .

Użytkownicy grupy 10-15 lat zlecają ochronę przed atakiem zewnętrznym organizacjom, gdyż prawdopodobnie nie mają odpowiedniej wiedzy na temat technicznej strony dotyczącej problemu.

Użytkownicy grupy 16-29 lat podejmują samodzielne akcje, są one zróżnicowane , natomiast w większości skuteczne. Użytkownicy grupy 30 i więcej podejmują nieco bardziej radykalne działania i akcje , które wymagają większego zaangażowania i poświęcenia. Grupa osób , która kiedyś została oszukana , podejmuje radykalne działania, ponieważ z racji doświadczenia , zaatakowani ponownie, są zaskoczeni , że ktoś zdołał przejąć kontrole nad ich urządzeniami , więc podejmują dosyć radykalne kroki aby temu zapobiec. W grupie osób, która nigdy nie została oszukana, sytuacja wygląda podobnie jak w grupie , która doświadczyła kiedyś oszustwa. Oprócz podejmowania samodzielnych radykalnych kroków, decydują się oni na oddanie telefonu do serwisu.

Może to wynikać z tego , że nie są w stanie oszacować stopnia zagrożenia przez co zwykła usługa serwisowa wydaje się wygodniejsza i mniej problematyczna.

WNIOSKI I PODSUMOWANIE

Zrealizowane badanie miało na celu pokazać z różnych perspektyw, biorąc pod uwagę różne czynniki , jak ludzie reagują na cyberatak. Okazuje się , że badani którzy spędzają więcej czasu w Internecie (grupa 2-4h oraz grupa ponad 5h), są bardziej samodzielni w kwestii reakcji na dane zagrożenia, tzn. częściej formatują swoje urządzenia co wymaga pewnego własnego wkładu. Natomiast grupa spędzająca najmniej czasu przeważnie wybiera formy zlecenia danego problemu jednostkom zewnętrznym tj. policja lub serwis komputerowy. Biorąc pod uwagę czynnik wieku badanych, można zauważyć , że grupa najmłodszych oraz najstarszych użytkowników (gr 10-15 lat oraz gr 30 i więcej lat) czuje się niepewnie w razie ewentualnego ataku i zleca w większości przypadków rozwiązanie problemu w ręce policji lub serwisu . Grupa zawierająca ludzi 16-29 letnich, wykazuje się większą pewnością w swojej reakcji i nie zlecają działań prewencyjnych jednostkom zewnętrznym. Podejmują akcje, które są w stanie ich uchronić w przypadku standardowych , niezbyt zaawansowanych ataków. W przypadku ludzi , którzy mieli styczność bądź nie mieli styczności z atakiem w przeszłości, deklarują w większości , że robią radzą sobie samodzielnie, bądź zlecają naprawę zewnętrznym jednostkom. W przypadku oszukanych wcześniej badanych , zlecają oni to na policję , natomiast nieoszukani oddają telefon do serwisu. Biorąc pod uwagę powyższe rezultaty można stwierdzić , że żaden z badanych czynników nie odnosi się do zdolności reakcji na zagrożenia. Badani rzadko stosują się do zaleceń dotyczących korzystania z antywirusowego oprogramowania, co w naszej opinii jest najbardziej odpowiednim i niezbędnym krokiem do zapewnienia sobie znacznego bezpieczeństwa w sieci. Ludzie mający pewne doświadczenie z atakami, spędzający więcej niż 1 h dziennie oraz będący w przedziale 16-29 lat wydają się najbardziej rozsądną grupą, podczas takiego ataku, natomiast ich działania nie są wystarczające, gdyby doszło do poważniejszego ataku lub też przejęcia konta bankowego. Rezultaty naszych badań jasno wskazują , że należy wdrażać wszelkiego rodzaju powiadomienia oraz szkolenia dotyczące bezpieczeństwa w sieci. Kluczowym elementem jest nakłanianie w nich do stosowania antywirusów oraz innych środków prewencyjnych dotyczących codziennego poruszania się w Internecie.

BIBLIOGRAFIA

