ROZDZIAŁ 14

Badanie efektywności ataków socjotechnicznych w jednostkach samorządu terytorialnego

Mariusz NYCZ, Bartosz MICHNO, Rafał MLICKI
Politechnika Rzeszowska
MNycz@prz.edu.pl, BMichno91@gmail.com, RMlicki@stud.prz.edu.pl

Streszczenie

W rozdziale przedstawiono analizę podatności na ataki socjotechniczne w lokalnej siedzibie samorządu terytorialnego. Autorzy rozpoczynają rozdział od wprowadzenia w zagadnienia związane z socjotechniką i ich wpływ na bezpieczeństwo informacyjne. W kolejnych paragrafach zaprezentowano metodykę badań określenia podatności na ataki socjotechniczne. Badania bazują na testach penetracyjnych i ankiecie, w której poruszono problemy bezpieczeństwa informacji na poziomie zarówno podstawowym jak i bardziej rozbudowanym. Wyniki ankiety dały podstawy do zbudowania przybliżonych profili ankietowanych wraz z poziomem ich podatności na określone zagrożenia socjotechniczne. W celu porównania wyników, przeprowadzono również badania na innej grupie użytkowników. Ze względów bezpieczeństwa ankieta oraz jej bezpośrednie wyniki nie będą ujawniane.

1. Wprowadzenie

Socjotechnika może mieć wiele różnych definicji w zależności od książki, która ją opisuje lub osoby z którą prowadzi się rozmowę. Definicja, którą można znaleźć w słowniku Oxfordu brzmi:

Zastosowanie zasad socjologicznych do konkretnych problemów społecznych…

Pomimo, że porusza istotną część, definicja ta jest daleka od trafnego wytłumaczenia czym współcześnie jest socjotechnika. Inna definicja głosi:

Sztuka celowego manipulowania zachowaniem przy użyciu specjalnie stworzonych technik komunikacji.

Ta definicja ogranicza socjotechnikę do absolutnych podstaw wykorzystujących komunikację we wszystkich możliwych formach w celu wykorzystania czynnika ludzkiego. Gdziekolwiek zachodzi interakcja, tam występuje potencjał dla socjotechniki. Socjotechnika więc liczy sobie tyle samo lat co komunikacja.

Instytut SANS zaproponował bardziej poprawną definicję:

Socjotechnika to sztuka wykorzystania ludzkich zachowań do złamania zabezpieczeń bez spostrzeżenia przez uczestnika (lub ofiarę), że zostali oni zmanipulowani.

Ważną częścią tej definicji jest kontekst, w jakim pojęcie to jest stosowane. Socjotechnikę można zdefiniować jako techniki stosowane do uzyskania informacji lub manipulowania zachowaniem lecz nie ma to odniesienia w kontekście bezpieczeństwa informacji. Jeśli chodzi o zabezpieczenie ważnych firmowych danych socjotechnika staje się:

Sztuka pozyskiwania wrażliwych informacji i/lub manipulacji osób w określony sposób mający na celu złamanie zabezpieczeń.

Można się sprzeczać, że pozyskiwanie wrażliwych informacji samo w sobie jest złamaniem zabezpieczeń lecz w definicji chodzi np. o włamanie do sieci, złamanie fizycznych zabezpieczeń lub obie sytuacje naraz.

Zauważając, że w poprzedniej definicji użyto słowa „sztuka", można zadać pytanie: czy socjotechnika jest formą sztuki? Według autorów [1], odpowiedź brzmi tak. Socjotechnika nie jest do końca nauką i często występuje w niej kreatywne myślenie. Socjotechnika nie może być zredukowana jednak do prostego określenia: *„jeśli zestaw akcji A, to potem B"*.

Techniki socjotechniczne mają na celu wykorzystanie „luk" raczej w ludzkiej naturze, a nie w systemach komputerowych. W wielu artykułach o bezpieczeństwie lub nawet w powieściach używano określeń *„human hacking"* lub *„hacking wetware"*. Osoba używająca metod socjotechnicznych używa niezliczonych technik w celu manipulacji do swoich celów, od wywierania wpływu na ludzkie emocje aż po logicznie sformułowaną strukturę ataku i dostosowywanie się pod daną osobowość. Jednakże socjotechnika nie ogranicza się do tricków psychologicznych. Atakujący może stwarzać całe scenariusze, którymi będzie podpierał swoje akcje. Scenariusze te mogą być dzielone na wiele następujących po sobie etapów [1].

Możliwe, że jednymi z osób najlepiej stosujących socjotechnikę są sprzedawcy handlowi. Przeciętny handlowiec ma jeden cel: sprzedać produkt lub usługę klientowi. W osiągnięciu celu sprzedawca nie zadaje klientowi prostych pytań, czy chciałby coś kupić, a raczej wykorzysta wszystkie możliwe opcje aby wpłynąć na jego decyzję. Dobrym przykładem może być użycie otwartych pytań zamiast zamkniętych, które kończąc się prostymi odpowiedziami „tak" lub „nie". Dla przykładu, sprzedawca może zapytać: *„Jaką ilość chciałby Pan zakupić?"* zamiast *„Czy chciałby coś Pan zakupić?"* lub *„Jak mogę panu pomóc?"* zamiast *„Czy mogę Panu pomóc?"*.

Istnieją nawet modele i metodologie skupione wyłącznie na obejściu zastrzeżeń klienta przy zakupie. Najlepsi sprzedawcy uważnie przestudiują wymagania klienta i jego samego, znajdując wspólne tematy do rozmowy. Powołując się na np. sukcesy w grze w tenisa, można zdobyć zaufanie klienta, który również obraca się wokół tego sportu. Taki wstępny rekonesans wygląda tak samo w przypadku ataku socjotechnicznego: profilowany jest np. zakres działalności firmy lub pro-

wadzone przez nią badania. Atakujący stara się zebrać jak najwięcej informacji. Każdy strzępek zwiększa szansę na powodzenie ataku.

Dodatkowo atakujący może przypisywać sobie fałszywą tożsamość – przez podszywanie się pod inną osobę może zdobywać pewne informacje do swoich celów. Handlowiec z poprzedniego przykładu, może wykonać bezpośredni telefon do odpowiedniego działu firmy i podać się za jednego z pracowników. Uzyskane stąd informacje pozwolą na stworzenie punktu zaczepienia w jego procesie sprzedaży. Osoba korzystająca z metod socjotechnicznych również skontaktuje się z firmą. Jedyną różnicą między handlowcem a nim jest cel zdobycia tych informacji – atakujący użyje ich do stworzenia metody socjotechnicznego ataku na daną firmę.

Stąd można powiedzieć, że to handlowiec stanowi najlepszego „inżyniera społecznego", ze swoją naturalną pewnością siebie, pozytywnym nastawieniem i doświadczeniem w wywieraniu wpływów. Ich celem jest sprzedanie produktu lub pomysłu. Jeśli jednak koncept zmienia się ze sprzedawania na podawanie swojego hasła, lepiej mieć się na baczności [1], [2], [3].

Obecnie ataki wykorzystujące socjotechnikę stają się coraz popularniejsze. Według firmy *Check Point Software Technologies*, 32% odpowiadających na sondaż stwierdziło, że byli świadkami około 25 ataków socjotechnicznych [4]. W *Verizon Data Breach Investigations Report* za 2013 rok, socjotechnika stanowiła aż 29% wszystkich włamań. Z tych ataków metody typu phishing stanowiły aż 71%. Jest to czterokrotny wzrost w porównaniu do roku 2012 [5].

2. Typy ataków socjotechnicznych

W socjotechnice występuje wiele różnych typów ataków. W zależności od potrzeby typy ataków mogą być kreowane na bieżąco, ulepszane bądź też łączone ze sobą. Jednak większość z nich bazuje na znanych popularnych typach. Oto niektóre z nich:

Kradzież urządzeń mobilnych. Najstarszy typ ataku. W czasach, gdy urządzenia przenośne nabierają coraz większego znaczenia i stają się coraz bardziej popularne, ten typ ataku okazuje się być jednym z najbardziej skutecznych. Prawdopodobieństwo sukcesu rośnie w firmach, gdzie wdrożona jest polityka BYOD.

Shoulder-surfing. Najprostszy typ ataku. Atakujący stara się monitorować fizyczną aktywność użytkownika i jego urządzenia. Atakujący może monitorować ekran, klawiaturę lub ruchy rąk w celu przechwycenia prywatnych informacji.

Monitorowanie sieci. Monitorowanie sieci może ukazać typy usług najczęściej używane przez użytkowników. Poprzez ich identyfikację atakujący może rozpocząć rekonesans zabezpieczeń danej usługi i przeprowadzić ewentualny atak.

Digital dumpster diving. Co raz krótszy czas życia urządzeń elektronicznych z racji postępującego rozwoju technologii sprawia, że przestarzałe urządzenia

w składowiskach np. elektrośmieci mogą mieć pozostawione w swojej pamięci prywatne i poufne dane.

Phishing. Przeważnie związany z fałszywymi stronami oraz wiadomościami e-mail. W przypadku fałszywych wiadomości e-mail, atakujący używa nieprawdziwej tożsamości internetowej w celu oszukania odbiorcy [1], [6].

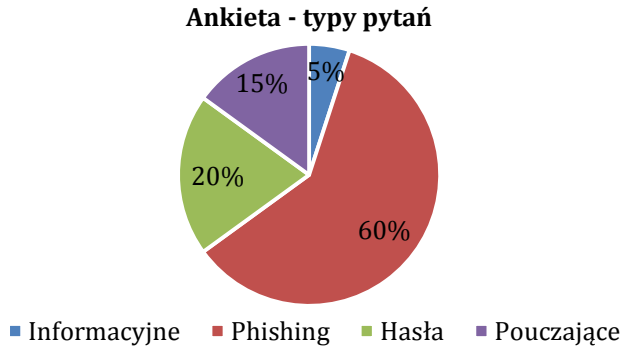
3. Metodyka badań

Badania zostały podzielone na dwie części. W pierwszej użytkownicy wypełnili ankietę, na podstawie której zostały wytypowane trzy kilkuosobowe grupy biorące udział w testach penetracyjnych z wykorzystaniem narzędzia Social Engineering Toolkit. Kryterium podziału na grup był stopień bezpieczeństwa określony dla badanych użytkowników. Powstała więc grupa o niskim, średnim i wysokim stopniu bezpieczeństwa. Pozwoliło to zbadać wpływ wiedzy teoretycznej na faktyczny stopień podatności na ataki socjotechniczne. Dla porównania wyników ankietę przeprowadzono również w sieci bezprzewodowej firmy PowerNet. Badanie było całkowicie anonimowe.

4. Ankieta

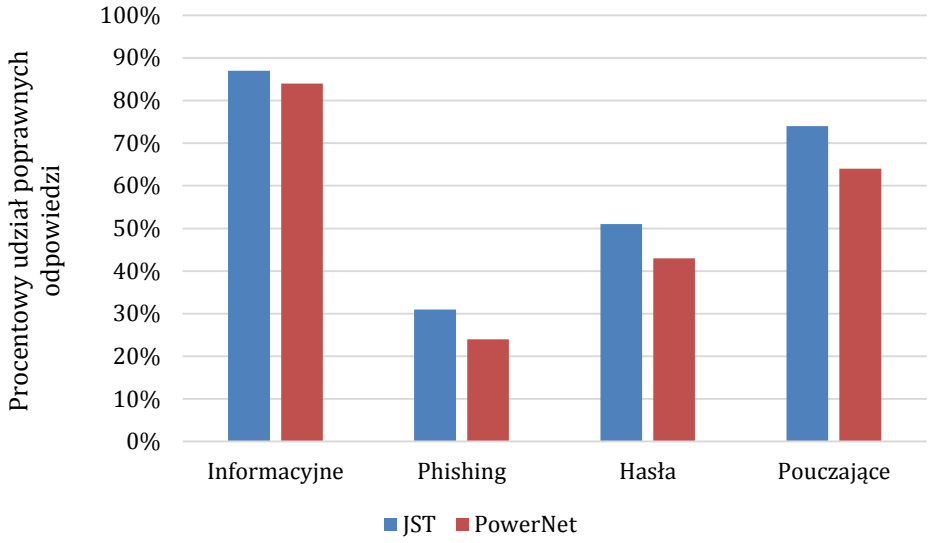
Ankieta została umieszczona na specjalnej witrynie przeznaczonej do ankietowania użytkowników. Znajdowała się ona pod prywatnym linkiem URL, niedostępnym z poziomu publicznego dla wyszukiwarek i użytkowników nieznających pełnego adresu.

Ankietowani odpowiadali na ponad 20 pytań. Niektóre z nich miały charakter pouczający, sugerujący prawidłową odpowiedź. Pytania te były nieliczne i znajdowały się na końcu ankiety. Pytania wstępne zawierały podstawowy zestaw typowej ankiety dotyczącej tematów informatycznych. Pytano w niej o system operacyjny oraz rodzaj używanej przeglądarki internetowej. Poniżej znajdują się cechy ankiety przedstawione na wykresach.



Rys. 1. Procentowy udział pytań w ankiecie

Wyniki ankiet przedstawione na rys. 2, jednoznacznie informują, że poziom wiedzy w przypadku pracowników samorządów jest nieznacznie większy w porównaniu z użytkownikami domowymi.



Rys. 2. Prezentacja wyników ankiety dla Jednostek Samorządu Terytorialnego (JST) i użytkowników bezprzewodowej sieci PowerNet

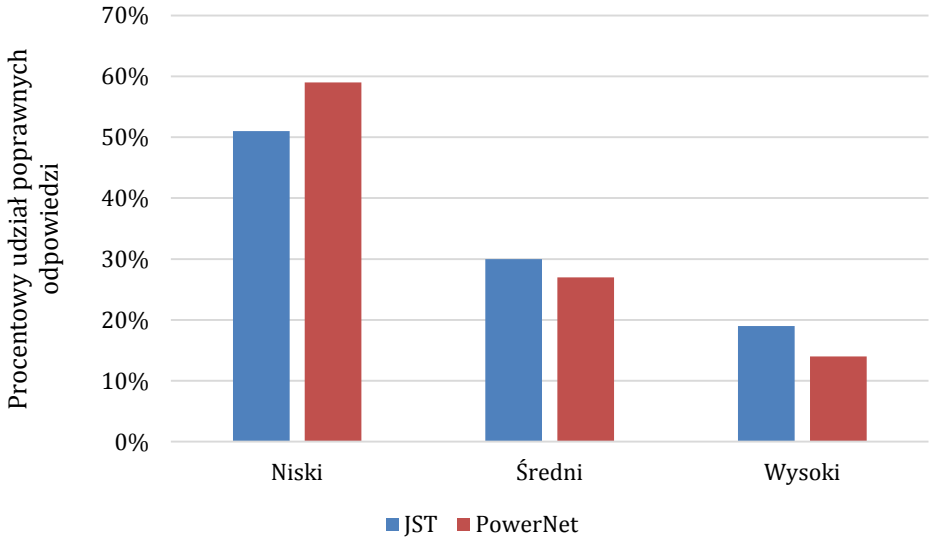
5. Testy penetracyjne

Testy penetracyjne są obecnie jedną z najskuteczniejszych metod weryfikowania zabezpieczeń, w którym testujący przeprowadzają symulowane ataki realizowane w czasie rzeczywistym. Uzyskane informacje pozwalają określić, które elementy systemu są podatne na ataki stosowane powszechnie przez napastników.

Testowanie zostało przeprowadzone na wyselekcjonowanej grupie respondentów. Selekcja została przeprowadzona na podstawie wyników ankiety, z której wyłoniono 15 osób i przydzielono je do trzech grup z wynikami odpowiednio:

- poniżej 40% poprawnych odpowiedzi (niski poziom odporności),
- od 41% do 70% (średni poziom odporności),
- powyżej 70% (wysoki poziom odporności).

Przynależność do poszczególnych grup w jednostce samorządu terytorialnego oraz lokalnego operatora internetowego, ilustruje poniższy wykres:



Rys. 3. Klasyfikacja poziomów dla JST i użytkowników sieci PowerNet

Testy zostały przeprowadzone przez administratorów w badanych jednostkach zgodnie z uprzednio przygotowaną instrukcją oraz oprogramowaniem. Poszczególne składniki testów to:

1. Exploit związany z przestarzałą i nieaktualną wersją środowiska Java, zainstalowanego na komputerze z systemem Windows;
2. Wiadomości e-mail korzystające z fałszywej tożsamości bądź wykorzystujące załącznik ze złośliwą zawartością;
3. Strona internetowa podszywająca się pod znany portal internetowy, przesyłająca wpisane poświadczenia użytkowników;
4. Wykorzystanie luki w starej wersji przeglądarki Internet Explorer,
5. Opis rozmowy telefonicznej wyłudzającej informacje;
6. Wykorzystanie luki w nieaktualnym systemie operacyjnym Windows.

Do wykonania testów użyto m. in. narzędzia SET [6].

Po przeprowadzonych badaniach wyniki zebrano i uporządkowano przypisując im mniejsze lub większe znaczenie pod względem skuteczności w badanej grupie. Tabela poniżej przedstawiaja wagi wyrażone w punktach dla każdego typu testu penetracyjnego. Wartość maksymalna - 5, oznacza, że grupa jest najbardziej podatna na określony atak.

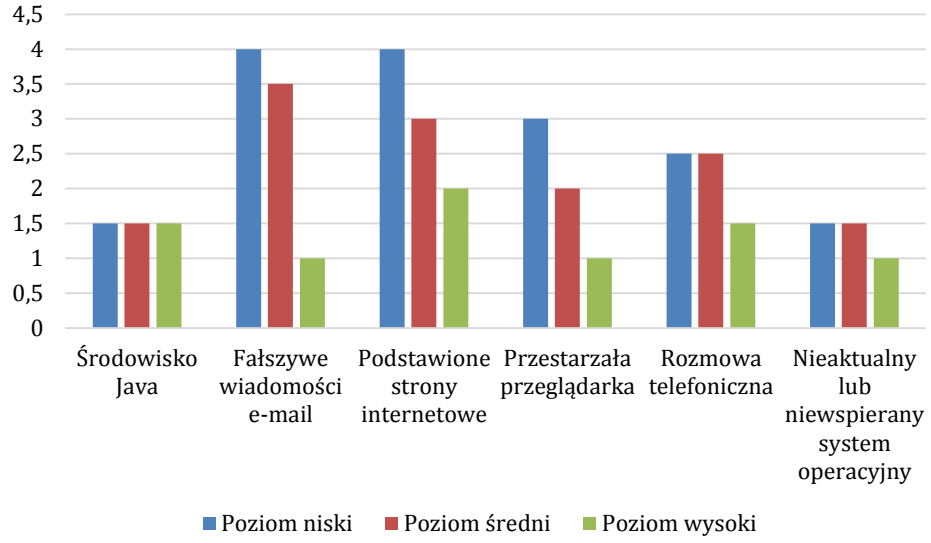
Na uwagę zasługują punkty przydzielone środowisku Java. We wszystkich grupach stopień podatności jest taki sam. Jest tak dlatego, ponieważ atak na Javę nie miał szerokiego wyboru narzędzi i obejmował tylko jedną metodę. Obierała sobie ona na cel jedną lukę w tym środowisku, stąd w każdej grupie wyniki są podobne.

Tabela 1. Klasyfikacja podatności z uwzględnieniem zdefiniowanych wag

Typ zagrożenia	Podatność w pkt (maks. 5)		
	Grupa najsłabsza	Grupa średnia	Grupa najodporniejsza
Środowisko Java	1,5	1,5	1,5
Fałszywe wiadomości e-mail	4	3,5	3,5
Podstawione strony internetowe	4	3	3
Przestarzała przeglądarka	3	2	2
Rozmowa telefoniczna	2,5	2,5	2,5
Nieaktualny lub niewspierany system operacyjny	1,5	1,5	1,5

Z kolei znacznie bardziej zróżnicowane są podatności na np. ataki związane z phishingiem. Ataki te można wykonywać na setki różnych sposobów, stąd podatność w każdej grupie jest słabsza lub większa.

Ostateczne wyniki w jednostce samorządu prezentują się na wykresie poniżej.

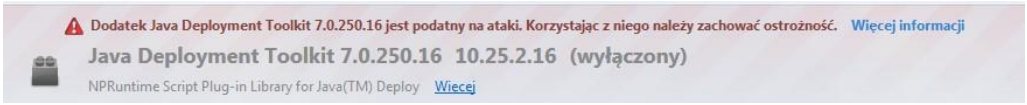


Rys. 4. Wyniki testu.

6. Opis metodyki realizacji testu

Informacje przedstawione w tej sekcji opisują kolejno metody oszustw socjotechnicznych stosowanych w ankiecie i w testach penetracyjnych. Nie wszystkie z nich są czysto socjotechniczne, ale przenoszone są z wykorzystaniem ataków socjotechnicznych. W takich przypadkach socjotechnika jest dopiero pierwszym etapem przeprowadzania ataku, a właściwe wykorzystywanie luk bezpieczeństwa występuje jako faza druga.

Ataki z spreparowanym apletem Java. Z przeprowadzonej analizy wynika, że najwięcej użytkowników może być narażonych na ataki związane ze środowiskiem programistycznym Java. Java jest bardzo popularnym oprogramowaniem wśród internautów – często wymagana jest do poprawnego wyświetlania stron internetowych. W przeglądarkach internetowych Java występuje pod postacią wtyczek włączanych na żądanie. W nowszych wersjach przeglądarek wtyczki te wyłączane są automatycznie. Jedna z nich, Mozilla Firefox, informuje użytkownika o niebezpieczeństwie związanym z użytkowaniem Javy.



Rys. 5. Wbudowane zabezpieczenia w przeglądarce Firefox dot. Javy

Niektóre aplikacje, ze względu na konieczność obsługi wielu platform systemowych są napisane w Javie. Jest ona wobec tego środowiskiem bardzo podatnym na ataki, ponieważ większa uniwersalność ułatwia wyszukiwanie luk. Java jest również oprogramowaniem bardzo skomplikowanym. Wbrew pozorom również umożliwia to nadużywanie Javy w celu łamania jej systemów bezpieczeństwa (im bardziej *rozległe* oprogramowanie, tym większa szansa natrafienia na ewentualną lukę). Atak na Javę może zostać przeniesiony np. w załącznikach wiadomości e-mail.

Fałszywe wiadomości e-mail. Kolejną metodą ataku, na którą podatni byliby użytkownicy rozwiązujący ankietę to wiadomości e-mail, gdzie nadawca używa fałszywej tożsamości. Wiadomości te wyglądają bardzo autentycznie. Istnieje wiele metod uwiarygodniania takich e-maili. Jedną z nich jest adres nadawcy – wykorzystuje się łatwe do przeoczenia literówki. Drugim sposobem jest wysyłanie wiadomości ze specjalnych generatorów wiadomości (najczęściej strony www). Cechą takich generatorów jest to, że oprócz podania adresata wiadomości podaje się również adres nadawcy. Generator oszukuje serwery pocztowe i przesyła taką wiadomość dalej. Niektóre serwisy pocztowe, np. Gmail są w stanie wykryć większość takich oszustw i wyświetlają stosowne ostrzeżenie dla użytkownika [7].

Rys. 6. Ostrzeżenie w usłudze Gmail

To ostrzeżenie jest wyświetlane, gdy nadawca twierdzi, że wysyła wiadomość z Gmaila, ale nie może to być potwierdzone. Można na przykład otrzymać e-maila pochodzącego rzekomo z adresu support@gmail.com, który w rzeczywistości nie został wysłany z Gmaila. Wszystkie wiadomości wysyłane z tej usługi powinny

zawierać dane uwierzytelniania, które pozwalają na weryfikację tego, czy wiadomość została wysłana z Gmaila. Jeśli jest wyświetlany komunikat ostrzegawczy, który informuje, że wiadomość mogła nie zostać wysłana przez użytkownika Gmaila, oznacza to, że brakuje w niej danych uwierzytelniania [8].

Podstawione strony internetowe. Sfabrykowane strony internetowe wykorzystują identyczny lub do złudzenia podobny wygląd oryginalnej witryny. Z autentycznej strony zachowany został tylko układ elementów, a faktyczna funkcjonalność strony to przesyłanie wpisanych poświadczeń użytkownika (login, hasło, inne) do atakującego.

Oszustwa telefoniczne. Podobnie jak w przypadku wiadomości e-mail, kluczem jest tutaj podstawiona tożsamość. Oszustwo może ułatwić fakt samej rozmowy telefonicznej, która odbywa się „w locie". W przeciwieństwie do e-maili, gdzie treść wiadomości można analizować wiele razy po odebraniu, w rozmowie telefonicznej czas na namysł jest ograniczony. Sprzyja to skuteczności ataku w przypadku rozmowy kreowanej na nagły i niespodziewany przypadek, wymagający szybkiej interwencji użytkownika.

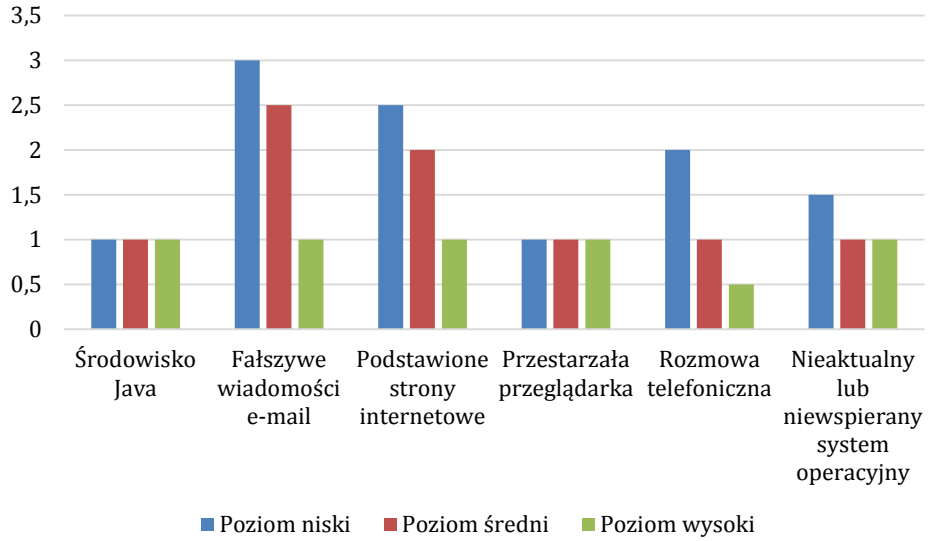
Stare wersje przeglądarki Internet Explorer. Pewna część użytkowników ciągle używa wersji Internet Explorer, która jest przestarzała. Wersja wspomnianej przeglądarki o numerze 7 została wydana siedem lat temu. Z kolei wersja 8 swoją premierę miała pięć lat temu. Przeglądarka Microsoftu jest bardzo chętnie atakowanym oprogramowaniem – wśród internautów znana jest z ilości luk w bezpieczeństwie. Korporacja często wydaje aktualizacje typu security do IE i stara się niwelować braki.

Według raportu firmy *Bromium Endpoint Exploitation Trends H1 2014* [9] za pierwszą połowę 2014r., liczba luk i zagrożeń w Internet Explorerze (w porównaniu do 2013r.) jako jedyna wzrosła. Inne programy wymieniane tutaj zanotowały poprawę bezpieczeństwa i liczba zagrożeń ich dotyczących drastycznie spadła.

System operacyjny. Ten problem dotyczy użytkowników korzystających z systemu Microsoft Windows XP. System przestał być wspierany w kwietniu 2014 r. Microsoft przestał wydawać aktualizacje bezpieczeństwa dla tego systemu. Czyni to go podatnym na ataki typu „zero day" – poważne luki bezpieczeństwa, nieznane do czasu pierwszego ataku z nią w roli głównej. Jeśli taka luka zostanie odkryta, deweloperzy Microsoftu nie zapewnią już łatki bezpieczeństwa.

7. Szkolenie

W ciągu trzech miesięcy od przeprowadzenia ankiety i testów penetracyjnych, w badanych obiektach przeprowadzono szkolenie, obejmujące zagadnienia wykorzystywane w ankiecie i testach penetracyjnych. Zauważono wzrost świadomości użytkowników oraz przeprowadzono kolejne testy penetracyjne (tylko w jednostce samorządowej). Po analizie wyników okazało się, że testy wykonane po szkoleniu dały lepsze wyniki, zilustrowane na wykresie poniżej.



Rys. 7. Wyniki testu po przeprowadzonym szkoleniu

Podatność na określone grupy ataków istotnie się polepszyła. Należy zauważyć m. in.:

1. Podział na grupy nie został zmieniony – obowiązywał taki jaki wyłoniony był po pierwszych testach;
2. W przypadku środowiska Java, przeglądarek internetowych i systemów operacyjnych poziom podatności polepszył się i mniej więcej wyrównał; dzieje się tak, ponieważ dbanie o aktualizacje programów i systemów operacyjnych przeważnie nie leży w gestii użytkowników, a administratorów; administratorzy jednostki samorządowej również brali udział w szkoleniach, a po wyeliminowaniu przestarzałego software'u i aktualizacjach, na wszystkich stacjach roboczych występował podobny zbiór programów (i ich wersji), przez co liczba zagrożeń, na które są one podatne stoi na mniej więcej tym samym poziomie [10], [11].

8. Wnioski

Najczęstszymi obiektami ataków socjotechnicznych są pracownicy firm, instytucji. To pracownicy często nieświadomi, niedoszkoleni lub posiadający specjalne przywileje, „atrakcyjne" z punktu widzenia dla atakującego. Ofiarą ataków mogą paść też pracownicy kluczowych działów instytucji.

Co sprzyja atakom socjotechnicznym? Niska świadomość użytkowników to najpoważniejszy powód. Dlatego tak ważne jest wykonywanie okresowych szkoleń pracowników (zalecane jest przeprowadzanie ich 1–2 razy w roku) [12].

Jednoznacznie można stwierdzić, że socjotechnika to najniebezpieczniejsza forma ataków na bezpieczeństwo z racji swojej natury. Ponieważ socjotechnika nadużywa cech ludzkich. np. zaufania, nie ma możliwości obrony przed nią tylko i wyłącznie za pomocą hardware'u i software'u.

Obecnie nie są dostępne rozwiązania, które mogłyby zapobiec atakowi socjotechnicznemu. Można jedynie zmniejszyć prawdopodobieństwo wystąpienia udanego ataku poprzez:

1. Wdrożenie polityki haseł dla instytucji;
2. Politykę klasyfikacji danych: z danych przepływających przez instytucję wybiera się te najbardziej istotne i stosuje się środki mające na celu chronienie ich;
3. Prowadzenie audytu wewnętrznego bezpieczeństwa informacji przetwarzanych w systemie teleinformatycznym;
4. Ograniczenie dostępu do sieci społecznościowych dla pracowników;
5. Administracyjne zarządzanie aktualizacjami oprogramowania i systemu operacyjnego;
6. Kształtowanie świadomości użytkowników poprzez nieustanne doszkalanie [1], [12].

Bibliografia

[1] G. Watson, A. Mason i R. Ackroyd, Social Engineering Penetration Testing, USA: Elsevier, 2014.

[2] E. Nyamsuren i H. Choi, Preventing Social Engineering in Ubiquitous Environment, IEEE Xplore Digital Library.

[3] I. Kotenko, M. Stepashkin i E. Doynikova, Security Analysis of Infor-mation Systems taking into account Social Engineering Attacks, IEEE Xplore Digital Library.

[4] „http://www.cleveland.com/business/index.ssf/2012/10/social_engineering_is_a_growin.html", 20 10 2012. [Online].

[5] „http://www.phishingbox.com/verizon-data-breach-investigations-report-summary/", 08 10 2013. [Online].

[6] N. Pavkovic i L. Perkov, Social Engineering Toolkit - A Systematic Approach To Social Engineering, IEEE Xplore Digital Library.

[7] E. Rabinovitch, Staying protected from social engineering, IEEE Communications Magazine, September 2007.

[8] „https://support.google.com/mail/troubleshooter/2411000?p=sent_warning&rd=1", 17 06 2014. [Online].

[9] „http://www.bromium.com/sites/default/files/bromium-h1-2014-

threat_report.pdf", 23 07 2014. [Online].

[10] B. Michno, M. Nycz i P. Hajder, „Social engineering-penetration testing", in *Computer Science for the Information Society*, tom Vol. 5, Lugansk, 2014, pp. Vol. 5, pp. 93-97.

[11] R. Mlicki, M. Nycz i R. Korostenskyi, „Social engineering-analysis of vulnerability", w *Computer Science for the Information Society*, Lugansk, 2014, pp. Vol. 5, pp. 97-100.

[12] L. Laribee, S. B. David, C. R. Neil i H. M. Craig, Analysis and De-fensive Tools for Social-Engineering Attacks on Computer Systems, IEEE Xplore Digital Library.