

ROZDZIAŁ II

**BEZPIECZEŃSTWO INTELEKTUALNE
W DOBIE SPOŁECZEŃSTWA INFORMACYJNEGO**

Sławomir ISKIERKA
Janusz KRZEMIŃSKI
Zbigniew WEŹGOWIEC
Politechnika Częstochowska

MANIPULACJA INFORMACJĄ ZAGROŻENIEM DLA WOLNOŚCI JEDNOSTKI**Streszczenie**

W referacie przeanalizowano wpływ poziomu i jakości wykształcenia na percepcję informacji docierającej do odbiorcy poprzez środki masowego przekazu. Zwrócono uwagę na podejmowane działania związane z manipulacją informacją mające na celu wygenerowanie konkretnych zachowań tak wśród jednostek jak i określonych grup społecznych. W dobie społeczeństwa informacyjnego wszelkie tego typu działania mają natychmiast charakter globalny, co związane jest z niezwykle szybkim obiegiem informacji we współczesnym świecie. Podano przykłady działań socjotechnicznych funkcjonujących w Internecie, których celem jest pozyskanie informacji od użytkownika sieci i wykorzystania jej do wywołania u niego pożądanych, z punktu widzenia dokonujących tych socjotechnik, reakcji. Wskazano, że tego typu działania odbywające się bardzo często w sposób niezwykle dyskretny i zakamuflowany stanowią potencjalne zagrożenie dla wolności jednostki, która podświadomie zachowuje się według scenariusza przygotowanego wcześniej przez różnego typu organizacje, partie polityczne czy wręcz grupy przestępcze. Wydaje się, że jedną metod z walki z tego typu zagrożeniami jest konsekwentne i systematyczne podnoszenie poziomu nauczania na wszystkich stopniach kształcenia.

Wstęp

Na postawione pytanie, kto jest najłatwiej podatny na wszelkiego rodzaju manipulacje informacją, odpowiedź wydaje się być oczywista – człowiek niewykształcony. Ta prosta w swojej symbolice odpowiedź jest jednocześnie bardzo nieprecyzyjna. Trudność polega głównie na zdefiniowaniu cech, których posiadanie pozwala o danym człowieku mówić, że jest człowiekiem wykształconym. Dodatkowo problem ten jest zamazywany przez pojęcie inteligencji, które jako pojęcia psychologiczne definiowane jest w Nowej encyklopedii powszechnej PWN z 1997 roku w postaci „cecha umysłu odpowiadająca za sprawność w zakresie myślenia, rozwiązywania problemów i innych czynności poznawczych; od poziomu inteligencji zależy poprawność rozumienia złożonych problemów i skuteczność poszukiwania trafnych rozwiązań a także sprawność działania w sytuacjach nowych i trudnych”. Intuicyjnym wydaje się być pogląd, że inteligencja ułatwia zdobycie wykształcenia

a wykształcenie stanowi bazę intelektualną dla inteligencji. Zachodzi w tym przypadku zjawisko zwane w technice sprzężeniem zwrotnym dodatnim, które w procesie kształtowania osobowości odgrywa fundamentalną rolę.

Informacja we współczesnym społeczeństwie

Obecny etap rozwoju społecznego często nazywany jest erą społeczeństwa informacyjnego. Jedną z podstawowych jego cech jest dominująca rola, jaką informacja i jej obieg odgrywa w życiu gospodarczym, politycznym i społecznym. Zjawisko to zostało szczególnie wyeksponowane w momencie, gdy sieci komputerowe przestały być domeną świata nauki, a stały się narzędziem wykorzystywanym powszechnie przez obywateli. Fakt ten wygenerował określone problemy i zagrożenia związane z wytwarzaniem, przetwarzaniem, przekazywaniem i często manipulacją informacją. Dodatkowym zagadnieniem jest techniczna możliwość przesyłania dowolnej informacji tekstowej, czy też audiowizualnej w bardzo krótkim czasie, praktycznie bez ograniczeń i to dodatkowo w skali globalnej. Z tego też powodu pożądana reakcja na informację fałszywą, niepełną, czy też zmanipulowaną winna nastąpić w bardzo krótkim czasie, co praktycznie nie jest możliwe. Jedynym obiektem, który jest w stanie stosunkowo szybko zweryfikować uzyskaną informację jest jej odbiorca. Może tego dokonać jednak tylko wtedy, gdy posiada odpowiednią wiedzę, nawyki nie ulegania propagandzie i konstruktywne podejście do uzyskiwanych informacji, polegające przede wszystkim na umiejętności szybkiej jej weryfikacji w wielu dostępnych źródłach. Przykładem braku takiej cechy niechaj będzie reakcja większości akcjonariuszy, o czym doniosły media, jednej ze światowych firm komputerowych na wieść o chorobie jej szefa. W ciągu kilku godzin akcje firmy znacząco straciły na wartości a informacja o chorobie okazała się nieprawdziwa. Z doświadczeń autorów wynika, że umiejętnością tą w przeważającej większości nie wykazują się również studenci. Dowodem tego są bardzo wybiórczo prezentowane pozycje literaturowe w przedkładanych pracach seminaryjnych i dyplomowych, przy częstym powoływaniu się na jedyne źródło - encyklopedię Wikipedia.

Sposoby pozyskiwania informacji zagrożeniem dla wolności jednostki

Kluczowa rola, jaką odgrywa informacja we współczesnym świecie powoduje że staje się ona cennym towarem dla wielu ośrodków decyzyjnych między innymi: politycznych, wojskowych, gospodarczych, marketingowych. Chęć posiadania informacji o obywatelu a przede wszystkim o jego preferencjach, zachowaniach, czy nawet poglądach politycznych i religijnych, generuje określone działania techniczne zmierzające do ich pozyskania. We współczesnym świecie idealnym źródłem do uzyskania tego typu informacji jest Internet.

Korzystanie z sieci Internet staje się coraz bardziej powszechne a zakres jego wykorzystania znacząco się powiększył w ciągu kilkunastu ostatnich lat. Wykorzystanie sieci tylko do ściągania plików poprzez usługę FTP czy korzystania z poczty elektronicznej należy dawno do przeszłości. Popularyzacja usługi WWW stanowiła prawdziwy przełom w wykorzystywaniu sieci. Obecnie handel, usługi bankowe, zdalna nauka i praca, pozyskiwanie materiałów informacyjnych tekstowych i audiowizualnych, portale społecznościowe, blogi są codziennością sieci.

Rozwój elektronicznej wymiany informacji stwarza jednak, obok wygody i komfortu pracy konkretne zagrożenia wynikające z obecności użytkownika w glo-

balnej sieci. Z części tych zagrożeń użytkownicy, w większości zdają sobie sprawę. Kwestie bezpieczeństwa pracy w sieci, omawiane w licznych publikacjach prasowych, Internecie czy wreszcie w szkołach zaowocowały wzrostem świadomości wielu użytkowników. Praktycznie do normy, choć jeszcze niestety zdarzają się odstępstwa, należy już wykorzystywanie przez nich oprogramowania antywirusowego, antyspamowego, antyspyware i zapór firewall.

Udoskonalanie tego typu oprogramowania generuje jednak coraz to nowe formy pozyskiwania informacji wykorzystujące nieznanne dotychczas metody. Należą do nich między innymi: phishing – kradzież haseł za pomocą sfalszowanych stron internetowych, pharming, whaling – wyludzanie danych od kadry kierowniczej, minnowing – wyludzanie informacji od szeregowych pracowników firmy, którzy według badań wielu ośrodków zajmujących się bezpieczeństwem komputerowym są najsłabszym ogniwem w procesie bezpieczeństwa IT w firmie.

Obecnie w dobie kryzysu gospodarczego, w wyniku, którego następują zwolnienia pracowników w firmach, dodatkowym zagrożeniem jest problem związany z możliwością wyniesienia przez nich wrażliwych informacji dotyczących firmy takich jak: bazy danych klientów, plany badawczo rozwojowe czy listy haseł istotnych dla funkcjonowania przedsiębiorstwa. Zjawisko to jest tym bardziej niepokojące, że jak pokazują badania firmy analitycznych¹ może ono potencjalnie dotyczyć aż 88% administratorów systemów informatycznych.

Dodatkowo niepokojącym jest fakt, że pojawiają się coraz częściej luki w oprogramowaniu Open Source takim jak Joomla!, Drupal, WordPress i Linux, a strony WWW, blogi i sieci społecznościowe takie jak Facebook, MySpace, YouTube są coraz częściej źródłem złośliwych kodów.²

Bankowość elektroniczna czy też zakupy w sieci ze swej natury wymagają wprowadzenia przez operatorów tych usług mechanizmów kontroli i zabezpieczeń transakcji w sposób, który często jest formą inwigilacji (w tym przypadku w słusznej sprawie) tak użytkownika jak i jego stacji roboczej. Przykładem tego typu technologii są fraud dedection/prevention – środki wykrywania i zapobiegania nadużyciom. Umożliwiają one uzyskanie o użytkowniku między innymi następujących danych: adresu zamieszkania, numeru telefonu, domeny, w której się znajduje, rodzaju routingu, rodzaju i prędkości połączenia, obecności i rodzaju serwera proxy.³

Zgromadzone dane, jeżeli wymkną się z pod kontroli są potencjalnym zagrożeniem dla prywatności jednostki.

Interesujące informacje o zbieraniu danych o użytkownikach przeglądarek internetowych przedstawiono w dwutygodniku „Komputer Świat”.⁴ Z raportu, który przygotowali dziennikarze tego czasopisma wraz z dziennikarzami niemieckiego „Computer Bilda” wynika, że najpopularniejsze przeglądarki internetowe: Internet Explorer, Google Chrome, Firefox intensywnie zbierają szereg danych o ich użytkownikach i systemach komputerowych na których, pracują przekazując je do centralnych komputerów macierzystych firm. Danymi tymi są między innymi informacje o procesorze, pamięci operacyjnej, twardym dysku, zakodowane dane informacyjne o komputerze. Możliwe jest również na podstawie analizy odwiedzanych stron

¹ J. Muszyński: *Zwalniani – zagrożeniem dla firm*. „NetWorld” 2008, nr 10

² J. Muszyński: *Dziurawe strony WWW, aplikacje Open Source i sieci społeczne*. „NetWorld” 2008, nr 10

³ P. Królikowski: *Fraud dedection, czyli szelest elektronicznych pieniędzy*. „NetWorld” 2008, nr 10

⁴ Raport: *Prywatność w przeglądarkach*. „Komputer Świat” 2009, nr 4

i podjętych wyszukiwań w przeglądarkach, w razie potrzeby stworzyć profil psychologiczny użytkownika. Przedstawiciele firm zaznaczają, że pozyskiwane dane przeznaczone są tylko do celów statystycznych i rozwojowych konkretnych wersji programu i są one kasowane po z góry ustalonym czasie to jednak weryfikacja tych działań nie jest możliwa przez niezależnych ekspertów.

O roli przeglądarek internetowych niech świadczy fakt, że dane techniczne infrastruktury Google owiane są mgłą tajemnicy, niemniej znawcy rynku szacują, że Google zarządza około czterystu pięćdziesięcioma tysiącami serwerów o bliżej nie sprecyzowanej mocy obliczeniowej.⁵

Znanym i opisywanym w literaturze informatycznej zjawiskiem jest tak zwane pozycjonowanie stron w wyszukiwarkach internetowych. O ile rażące przykłady tego typu zachowań stosunkowo łatwo zdiagnozować to jednak bardziej subtelne generowanie określonych wyników wyszukiwania jest już problemem bardziej złożonym. Otrzymane w ten sposób informacje mogą mieć cechy świadomej manipulacji w celu uzyskania określonych zachowań u użytkownika.

Zakładanie kont pocztowych też jest najczęściej połączone z prośbą o zadeklarowanie swoich preferencji, co do zainteresowań. Dane te są formalnie wykorzystywane przez operatorów serwerów (bezpłatnych) do przygotowania oferty, na przykład reklamowej, dla użytkownika konta. Niemniej mogą posłużyć do głębszej analizy jego zachowań w sieci.

Klasycznym przykładem możliwości pozyskania dużej ilości informacji o użytkownikach jest portal Nasza-klasa. Zamieszczane tam materiały są wręcz wymarzone kompendium wiedzy o użytkownikach tego portalu, dla osób, które chcą i potrafią je wykorzystać w sposób nieetyczny. Przykłady hakerskich ataków na ten portal są znane z doniesień prasowych.

Przytoczone przykłady, obrazujące stosunkowo proste sposoby pozyskiwania informacji o użytkownikach sieci pokazują skalę zagrożenia, jakie może stanowić ich wykorzystanie niezgodnie z obowiązującym prawem.

Podsumowanie

Skuteczną obroną przed uleganiem zmanipulowanej informacji wydaje się być jedynie rzetelna wiedza uzyskana przez obywateli na wszystkich etapach edukacji. Wiedza zarówno charakterze humanistycznym jak i technicznym.

Wnioski płynące z toczącej się dyskusja na temat stanu wiedzy młodego pokolenia nie są budujące. Wynika z nich, że obecny system szkolnictwa w Polsce, pomimo deklaracji płynących z kręgów oświatowych nie kształci obywatela na świadomego uczestnika społeczeństwa informacyjnego.

Interesującą kontestacją tego stanu rzeczy jest opinia prof. Jana Hartmana zamieszczona w „Gazecie Wyborczej” „Uczniowie wychodzą ze szkoły z właściwym wszystkim ignorantom przekonaniem, że bardzo wiele umieją. Jednocześnie przez wiedzę rozumieją przypadkowe wiadomości, które nic ich nie obchodzą, z niczym im się nie kojarzą i do niczego nie wydają im się przydatne. Tak to widzą. W istocie nie mają żadnych wiadomości ani nawet mglistej intuicji, czym mogłaby być wiedza i wykształcenie. Owo bez ustanku powtarzane przez uczniów: „po co ma się tego uczyć?” (dziś dodają, poniekąd słusznie: przecież wszystko mogę zawsze sprawdzić w sieci) doskonale oddaje kompletną porażkę systemu edukacji

⁵ R. Janusz: *Maszynaria Google'a*. „PC Word Komputer” 2008, nr 7

nie tylko w samym nauczaniu, ale we wzbudzaniu w umysłach młodzieży jakiejś ogólnej idei wykształcenia i ambicji, aby być mądrzejszym niż się jest”⁶.

Sposobem, natomiast, postrzegania technicznej mentalności Polaków niechaj będzie komentarz, jaki przedstawiła pani Anna Strężyńska, prezes Urzędu Komunikacji Elektronicznej, dotyczący wprowadzania w Polsce telewizji cyfrowej DVB-T „*W Polsce jest cała masa osób technicznie bezradnych, w tym i ja, i tu będzie trzeba ludziom pomagać dom po domu, chałupa po chałupie, aby przełączyć się z telewizji analogowej na cyfrową*”⁷.

Przedstawione powyżej opinie mogą mieć charakter zbyt emocjonalny. Nie zmienia to jednak obserwowanego od kilku lat faktu, drastycznego obniżania się poziomu wiedzy młodzieży. Może to skutkować stosunkowo łatwą możliwością ulegania wszelkiego typu manipulacji, głównie poprzez odpowiednio spreparowaną informację umieszczoną w sieci. Stan ten może być szczególnie groźny w dobie ewentualnych napięć społecznych związanych z kryzysami politycznymi i gospodarczymi. W takich sytuacjach prawidłowo odczytana informacja i jej weryfikacja może okazać się równie skuteczną bronią jak działania o charakterze siłowym.

⁶ J. Hartman: *Szkoła buja w obłokach*. „Gazeta Wyborcza” 9 kwietnia 2009

⁷ *Wiadomości i informacje*. „PCFormat” 2008, nr 11