EDWARD ERAZMUS, ARTUR MICHAŁ BANASZAK

Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie

edart25@poczta.onet.pl

Edukacja dla bezpieczeństwa – jak być bezpiecznym w sieci?

Education for security – how to be safe in the net?

STRESZCZENIE

Sieć internetowa stwarza wiele możliwości dla wszystkich jej użytkowników. Wiele mówi się o korzyściach płynących z tego medium, a znacznie mniej o zasadach bezpieczeństwa w sieci. Internet umożliwia publikowanie własnych treści na różnego rodzaju serwisach, co może powodować pozytywne i negatywne skutki. Celem opracowania powyższego tematu jest edukacja i poszerzenie wiedzy na temat bezpieczeństwa w cyberprzestrzeni, a także uświadomienie społeczeństwa, że mimo wielu zalet i możliwości, jakie daje Internet, istnieją także poważne zagrożenia, które mogą mieć wpływ na funkcjonowanie człowieka.

ABSTRACT

The Internet network creates many possibilities for all its users. Much is said about the benefits of this medium, and much less about the security rules in the network. The Internet allows you to publish your own content on different types of websites, which can cause positive and negative effects. The aim of this article is to educate and broaden knowledge about security in cyberspace, and to make the public aware that despite many advantages and opportunities offered by the Internet, there are also serious threats that may affect the functioning of people.

Słowa kluczowe: Internet, cyberprzestrzeń, cyberprzestępczość, bezpieczeństwo.

Keywords: Internet, cyberspace, cybercrime, security.

Wprowadzenie

Pojawienie się Internetu przyniosło ludzkości wiele korzyści. Po raz pierwszy w historii ludzie są w stanie komunikować się i współpracować w niemal rze-

czywistym czasie, z łatwością, praktycznie niezależnie od granic państwowych i/lub stref czasowych. W ostatnich latach technologia informacyjna stała się tak nieodłączną częścią nowoczesnego biznesu, że niektórzy autorzy nie uznają już wykorzystania technologii informatycznych jako strategicznej korzyści. Zamiast tego można stwierdzić, że technologia informacyjna jest podstawowym dobrem, podobnym do elektryczności i że brak tego dobra uniemożliwia prowadzenie działalności gospodarczej (van Niekerk, Goss, 2013).

Każdy użytkownik zostawia ślady w sieci w sposób świadomy i nieświadomy. Świadomie w postaci umieszczania zdjęć, danych czy wpisów, natomiast nieświadomie – przez odwiedzanie stron internetowych. Takie informacje wykorzystują między innymi reklamodawcy lub cyberprzestępcy, którzy chcą pozyskać informacje na temat życia prywatnego internautów. Decyzja dotycząca udostępniania informacji powinna być świadoma oraz przemyślana[1].

Serwisy internetowe zaczęły zbierać cenne dane osobowe, takie jak: imię i nazwisko, datę urodzenia, miejsce zamieszkania, numer telefonu czy adres e-mail. Z tego powodu pojawił się problem przetwarzania i zabezpieczenia tych danych, ponieważ użytkownicy chcieli wiedzieć, co właściciele poszczególnych stron internetowych robią z takimi informacjami. Dzięki temu powstała polityka prywatności, która przedstawia zakres przetwarzanych informacji. Logując się do danego portalu, warto zapoznać się z tego typu dokumentem (Pieczyrak, 2013).

Świadome i bezpieczne korzystanie z Internetu z punktu widzenia użytkownika

Użytkownik komputera odgrywa istotną rolę w ochronie i zapewnieniu bezpieczeństwa w cyberprzestrzeni; jednak bezpieczeństwo komputerów pozostawia się inicjatywie użytkownika (Ng, Rahim, 2005). Dzieje się tak głównie dlatego, że ważkie decyzje dotyczące zachowania bezpieczeństwa podejmowane są podczas ich działań on-line: takie jak korzystanie z bankowości elektronicznej. Wszechobecność technologii informacyjnej zapewnia środki umożliwiające wiele różnych rodzajów działalności on-line: zakupy, bankowość i rekrutacja do pracy, rozrywka. Niestety, użytkownicy są nieświadomi, że korzystając z tych technologii, otwierają „tylne drzwi" dla hakerów. Są to główne możliwości włamania i innych naruszeń bezpieczeństwa. Dlatego warto przyjrzeć się ludzkiemu aspektowi bezpieczeństwa w ramach regularnego korzystania z komputera.

Teoria Motywacji do Ochrony (*Protection Motivation Theory*) zakłada, że motywacja do ochrony przed zagrożeniami jest związana z przekonaniami jednostki, iż osoba jest osobiście narażona na zagrożenie (Tu, Yuan, 2012). Jednak stosunkowo niewiele jest badań nad ludzkim aspektem bezpieczeństwa komputerowego i jego wpływem na praktykę bezpieczeństwa (Ng i inni, 2009, s. 815–825).

Dlaczego ludzki aspekt bezpieczeństwa jest tak ważny? Oczywiście trudno jest poznać i określić złożoność ludzkich zachowań i brak umiejętności obsługi komputera. Z tego względu naukowcy i osoby zajmujące się bezpieczeństwem wytyczają możliwe sposoby ochrony przed zagrożeniami IT. Komputery osobiste są popularnym celem hakerów (Doswell, 2008), ponieważ są oni zainteresowani tym, co użytkownicy przechowują na swoich komputerach. Na przykład poufne dane osobowe, takie jak nazwy użytkowników, hasła i dane konta bankowego. Z drugiej strony należy zauważyć, że poszczególnych użytkowników komputerów można łatwo oszukać ze względu na brak świadomości, jak zapewnić bezpieczeństwo w korzystaniu z komputera. Dlatego rozumienie bezpieczeństwa użytkownika w kontekście korzystania z komputera jest ważne dla ochrony przed złośliwymi atakami IT.

Niestety, większość użytkowników komputerów nie ma świadomości dotyczącej bezpieczeństwa w sieci z powodu luk edukacyjnych, braku profesjonalizmu i szkolenia (Hui, 2007). Świadomość bezpieczeństwa, stosunek do zaufania i ochrona prywatności zależą od kontekstu kulturowego i norm społecznych. Geert Hofstede opisuje szereg wskaźników wartości kulturowych mierzących różnice kulturowe między społeczeństwami (Hofstede, 1992). Definiuje on kolektywizm, jedną z cech określającą struktury w społeczeństwie, w której jednostki mogą oczekiwać, że ich krewni, rówieśnicy lub członkowie danej grupy będą dbać o nich w zamian za niekwestionowaną lojalność. Dlatego kultura może odgrywać znaczącą rolę w kształtowaniu stosunku ludzi do prywatności (Kumaraguru, Cranor, 2005). Na przykład kolektywizm w niektórych społeczeństwach tworzy lepsze wzajemne zaufanie i dlatego użytkownik może bez wahania dzielić się swoją tożsamością on-line, między innymi podając takie dane, jak nazwy użytkowników, hasła i dane kart kredytowych swoim rówieśnikom i rodzinie.

Bezpieczne witryny internetowe

Przeglądając strony internetowe, często nieświadomie udostępnia się dane osobowe, co jest spowodowane tym, że dana witryna jest niebezpieczna lub fałszywa (np. pishingowa strona logowania banku). Z tego powodu, przele-

wając pieniądze czy kupując w sieci, trzeba mieć pewność, że dana strona jest autentyczna oraz że nasze dane są chronione przed próbami wyłudzenia. Jest to trudne zadanie, ponieważ cyberprzestępcy potrafią wykorzystać elementy grafiki prawdziwych stron, zmieniając tylko szczegółowe elementy, np. jedna litera w adresie witryny i wielkość logo firmy (Sobianek, 2008).

Dlatego przed wykonaniem jakiejkolwiek czynności na danej stronie internetowej należy (Sobianek, 2008):

- zwracać uwagę na wygląd strony (kolorystyka, układ głównych elementów);
- dokładnie sprawdzić adres odwiedzanej strony (czy zgadza się cała nazwa adresu strony);
- zwracać uwagę, na proces autoryzacji na witrynie, prosta autoryzacja powinna wzbudzać podejrzenia (okna typu pop-up[2] nie wykorzystują banki i sklepy);
- przeczytać fragment strony (liczne błędy ortograficzne i literówki mogą świadczyć o fałszywej stronie);
- sprawdzić, czy komunikacja jest szyfrowana (opcja połączenia bezpiecznego powoduje, że pojawia się ikona kłódki – oznaczenie certyfikatu SSL oraz początek adresu strony zmienia się z „http://" na „https://", gdzie końcówka „s" oznacza „secure" – połączenie bezpieczne);
- pamiętać, żeby po zalogowaniu jeszcze raz sprawdzić adres i certyfikat strony oraz datę ostatniego logowania, ponadto za każdym razem przed wyłączeniem przeglądarki należy się wylogować.

Wymieniony wyżej certyfikat SSL to protokół, który zabezpiecza dane użytkownika podczas przesyłania ich z przeglądarki do serwera strony. Otrzymanie takiego certyfikatu wiąże się z przejściem przez daną witrynę procesu walidacji. Dlatego witryny bezpieczne to takie, które posiadają certyfikat[3].

Znajomości w świecie wirtualnym

Internet daje ludziom możliwość komunikowania się z innymi bez wychodzenia z domu. W dobie Internetu odległość między rozmówcami przestała mieć znaczenie, ponieważ sieć pozwala zbliżyć się do siebie ludziom z całego świata. Rozmowa w sieci nie ma także ograniczeń czasowych, może bowiem trwać od kilku minut do wielu miesięcy, a nawet lat. Użytkownik może odczytać wiadomość

w najdogodniejszej dla siebie chwili i nie ma obowiązku odpowiadać na nią od razu. Komunikacja między internautami zaczyna się najczęściej na forum dyskusyjnym, czacie lub na portalu społecznościowym – wystarczy kilka kliknięć, aby do drugiej osoby dotarła jakaś informacja (Kowalska, Bednarek, 2014, s. 138–140).

Wirtualną znajomością można określić utrzymywanie relacji z kimś poznanym w sieci. Rozmówcę internetowego można poznać na tyle, na ile on tego chce, tzn. w zależności od tego, jak dużo o sobie powie, oraz od tego, ile z tych informacji jest prawdą. Z jednej strony takie znajomości zwykle są krótkotrwałe, natomiast z drugiej bywa, że taka relacja pogłębia się, rozwija i umacnia. Najliczniejszą grupą ludzi zawierającą znajomości on-line są osoby młode i dzieci. Często przez małe zainteresowanie rodziców młodzież poszukuje zrozumienia wśród innych użytkowników sieci. Inną przyczyną szukania wirtualnych znajomych jest nieśmiałość w realnych kontaktach. Nawet jeżeli druga strona nie wykaże zrozumienia lub odrzuci nasze uczucia, znajomość w Internecie szybko i bez konsekwencji można zakończyć (Kozak, 2007, s. 167–168). Zdarza się, że relacje w cyberświecie są przedkładane nad kontakty w świecie realnym. Taka sytuacja może szczególnie negatywnie wpływać na młode osoby przebywające w sieci, tzn. może upośledzać ich zdolności komunikacyjne, które są bardzo potrzebne w relacjach „twarzą w twarz". Skutkiem tego w przyszłości może być nieumiejętność ludzi w radzeniu sobie w podstawowych życiowych sytuacjach (Kowalska, Bednarek, 2014, s. 141).

Nie każda relacja utrzymywana przez Internet musi zakończyć się źle – wiele znajomości może okazać się inspirującymi i ciekawymi. Sieć umożliwia poznanie ludzi o podobnych pasjach i zainteresowaniach. Niestety z Internetu korzystają także ludzie o złych zamiarach, tak więc trzeba pamiętać o podstawowych zasadach bezpieczeństwa – nie ufać bezgranicznie nowo poznanym osobom oraz nie podawać im swoich danych osobowych. Rozsądne korzystanie ze znajomości w sieci pozwoli uchronić siebie, a także dzieci przed przykrymi konsekwencjami w postaci oszustwa lub cyberprzemocy (Kozak, 2007, s. 169–170).

Regulaminy serwisów internetowych

Korzystanie z wszelkiego rodzaju serwisów internetowych wiąże się z akceptowaniem regulaminów tych stron przez zaznaczenie i kliknięcie w odpowiednie miejsce. W życiu realnym, gdy ktoś zostanie zapytany o dane osobowe do ankiety, zasłania się ochroną danych osobowych. Natomiast w Internecie bez-

myślnie zaakceptuje wszystkie regulaminy i politykę prywatności, nie czytając nawet jednego punktu z tych dokumentów.

Użytkownikom Internetu z pewnością trudno jest czytać regulaminy, które według badań Selectout mają przeciętnie 2460 słów. Przeczytanie tak dużego materiału może zająć nawet kilkanaście minut. Zdarza się również, że taki regulamin występuje w języku obcym, co może stanowić problem. Zazwyczaj zakładając, że wszystko jest w porządku, użytkownik akceptuje regulamin bez zapoznania się z nim. Firmy działające w Internecie zrobią wszystko, aby zniechęcić ludzi do czytania tego typu dokumentów. Jednak nie jest to powód, aby akceptować wszystko, co wyświetli się na monitorze, ponieważ w ten sposób można całkowicie pozbawić się prywatności. Z raportu Selectout jasno wynika, że większość serwisów internetowych udostępnia dane użytkownika dla innych firm na świecie, a część z nich nie posiada nawet polityki prywatności, bez której niebezpiecznie jest korzystać z portalu (Maikowski, 2014).

W związku z powyższym nie należy akceptować „w ciemno" takich regulaminów, ponieważ może to skutkować utratą panowania nad danymi osobowymi, którymi będą w dowolny sposób zarządzać inne podmioty.

Wiadomości w sieci

Jednym z dóbr Internetu, który pozwala utrzymywać kontakt z ludźmi, jest poczta elektroniczna. Przesyłane za jej pośrednictwem wiadomości – listy docierają w bardzo szybkim czasie mimo dużych odległości. Jednak nieostrożne korzystanie z poczty e-mail może narazić posiadacza na niebezpieczeństwo.

Przed otwarciem każdej wiadomości należy sprawdzić, czy na urządzeniu jest zainstalowany aktualny program antywirusowy. Powinien on być ustawiony tak, aby działał w czasie rzeczywistym, tzn. żeby skanował wiadomości wtedy, gdy przychodzą, oraz sprawdzał typy załączników (Majewski, 2009). Niekontrolowane otwarcie podejrzanej wiadomości i/lub załącznika może skutkować zainfekowaniem urządzenia i kradzieżą danych.

Cyberprzestępcy, którzy wykorzystują pocztę elektroniczną jako obiekt ataków, zazwyczaj korzystają z poprzednio przygotowanych wzorów. W Polsce najpopularniejsze to[4]:

- faktura od kontrahenta,
- windykacja,
- paczka do odebrania,

- faktura od operatora telekomunikacyjnego,
- wiadomość od banku,
- wezwanie na rozprawę.

W związku z tym, że fałszywe wiadomości często się powtarzają, można je sprawdzić, korzystając z wyszukiwarki Google, wpisując, np. temat e-maila. Ponadto w razie wątpliwości zawsze można wykonać telefon do firmy bądź osoby, która podaje się za nadawcę e-maila, w celu potwierdzenia autentyczności danej wiadomości. Należy pamiętać, żeby nigdy nie odpowiadać i wysyłać podejrzanej wiadomości dalej. Stanowi to potwierdzenie dla sprawcy, że konto e-mail jest prawdziwe i wkrótce będzie można się spodziewać kolejnych wyłudzających dane wiadomości[5].

Przed podjęciem decyzji w sprawie otwarcia wiadomości e-mail warto dodatkowo zadać sobie kilka następujących pytań (Majewski, 2009):

1. Czy nadawca wiadomości jest znany?
2. Czy od tego nadawcy otrzymywano już wiadomości?
3. Czy spodziewana jest wiadomość od tego nadawcy?
4. Czy temat i nazwa załącznika są sensowne?

Pobieranie danych z sieci

W społeczeństwie informacyjnym najsłabszym ogniwem w kwestii bezpieczeństwa teleinformatycznego jest człowiek. Brak wiedzy, bezmyślność lub po prostu ludzki błąd mogą spowodować poważne zagrożenie funkcjonowania w sieci. Niestety wiele osób nie zdaje sobie sprawy z tego, jakie konsekwencje może wywołać ich błąd.

W Internecie istnieje niezliczona ilość szkodliwego oprogramowania, są to wirusy, trojany i zagrożenia typu spyware[6]. Najczęściej pojawiają się na podejrzanych stronach internetowych dla dorosłych, w pirackich materiałach oraz wiadomościach e-mail. Otwarcie zainfekowanej wiadomości lub instalacja pliku z Internetu, bez odpowiedniego zabezpieczenia urządzenia, może skutkować nie tylko kradzieżą danych, lecz także szpiegowaniem użytkownika przez długi czas. Ponadto już samo pobieranie różnego rodzaju danych z sieci (np. muzyka, filmy, programy, gry) może sprowadzić niechcianego szkodnika do systemu. Internauci najczęściej trafiają na szkodliwe oprogramowanie w programach i aplikacjach, które są reklamowane jako darmowe przez przyciski „free download"

lub „free software", w których ukryte są wirusy. Jeżeli dany program rzeczywiście jest darmowy, to z pewnością będzie on dostępny na stronie producenta[7].

Programy i aplikacje należy pobierać tylko ze stron producenta lub sprawdzonych serwisów godnych zaufania. Istnieje wiele podejrzanych stron, które wyglądem przypominają popularne witryny. Dlatego w razie wątpliwości informacje na temat danej strony internetowej można spróbować znaleźć w wyszukiwarce internetowej, a także przeskanować daną stronę za pomocą skanera on-line. Każdy pobrany plik z Internetu należy sprawdzić programem antywirusowym. W przypadku znalezienia zagrożenia antywirus spróbuje go wyleczyć lub usunąć. Bardzo ważnym aspektem jest aktualizacja oprogramowania systemu i bazy sygnatur wirusów, w przeciwnym razie nowe zagrożenia mogą być niewidoczne dla antywirusa[8].

Pobierając treści komercyjne (muzyka, filmy, gry), trzeba również pamiętać, że można się narazić na złamanie postanowień licencyjnych, co idąc dalej – powoduje konsekwencje prawne. Witryny oferujące darmowe filmy i muzykę bardzo często zawierają wirusy, a poza tym pobranie takich plików często powoduje łamanie prawa.

Odpowiednie zabezpieczenie komputera i innych urządzeń mobilnych oraz kierowanie się zdrowym rozsądkiem i rozwagą zapewni wysoki poziom bezpieczeństwa.

Ochrona danych osobowych

Na podstawie ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku za dane osobowe uznaje się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W związku z powyższym dane osobowe to informacje, które określają konkretną osobę fizyczną oraz pozwalają na jej zidentyfikowanie, np. PESEL, NIP, imię i nazwisko, adres zamieszkania. W określonych przypadkach za takie dane mogą być uznane również: adres e-mail czy numer IP. Z kolei w myśl powyższej ustawy przetwarzanie danych to wszystkie jakiekolwiek operacje wykonywane na tych danych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a szczególnie te, które wykonuje się w systemach teleinformatycznych[9].

Bezpieczeństwo danych osobowych w Internecie w głównej mierze zależy od użytkowników. Nieprzemyślane działania w sieci mogą być przyczyną utraty kontroli nad danymi. Trzeba czytać regulaminy serwisów internetowych i zwra-

cać uwagę, na co wyraża się zgodę. Warto korzystać również z ustawień prywatności, które ograniczą widoczność danych osobowych dla osób postronnych (Szafrańska, Szafrański, 2014, s. 211–233).

Korzystając z portalu społecznościowego, należy udostępniać tylko te dane, które są niezbędne do korzystania z tego portalu. Udostępnianie zdjęć, które zdradzają wiele szczegółów (to, kto i co się na nim znajduje oraz metadane zdjęcia), powoduje obniżenie poziomu bezpieczeństwa danych. W sytuacji gdy ktoś ze znajomych udostępnił zdjęcie osoby trzeciej, które narusza dobro osobiste, może spodziewać się przykrych konsekwencji. Osoba, której zdjęcie dotyczy, może dochodzić swoich praw na podstawie art. 23 Kodeksu cywilnego. Ponadto w rozumieniu prawa autorskiego rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej[10].

Po zakończeniu pracy na stronie danego portalu, poczty czy banku, należy pamiętać, aby zawsze wylogować się z konta. Pozostawienie zalogowanego konta, „otwartych drzwi" znacznie ułatwia działanie hakerom. Podobnie wygląda możliwość zapamiętywania haseł przez przeglądarkę, gdy podczas logowania dane w odpowiednich polach uzupełniają się automatycznie. Dzięki temu cyberprzestępcy w prosty sposób mogą wejść w posiadanie loginu i hasła. W miejscach publicznych nie warto zostawiać komputera bez opieki, a także wypożyczać do użytkowania osobom niezaufanym, ponieważ grozi to utratą danych, podszywaniem się pod właściciela oraz kradzieżą danych, a nawet szantażem (Turek, 2015).

Stale włączona geolokalizacja oraz funkcja Wi-Fi na urządzeniu mobilnym powodują, że znany jest każdy ruch użytkownika tego urządzenia. Geolokalizacja za pomocą systemu GPS dokładnie namierza osobę. Następnie odpowiednie aplikacje i serwisy, które zbierają dane, wskazują lokalizację miejsca pracy, zamieszkania i przebywania, a także czas dojazdu do pracy czy wyjazdy wakacyjne. Funkcja bezprzewodowego Internetu (Wi-Fi) również pozwala na śledzenie każdego ruchu użytkownika[11].

Automatyczne łączenie się z darmowymi „otwartymi" sieciami stwarza bardzo duże niebezpieczeństwo, ponieważ niektóre sieci tego typu są tworzone przez hakerów specjalnie do kradzieży danych. Zazwyczaj nie posiadają żadnych zabezpieczeń szyfrujących. Takie „hotspoty" nie wzbudzają żadnych podejrzeń, ponieważ ich nazwy nawiązują do pobliskich sklepów czy restauracji. Po połączeniu haker przejmie każdą informację, która będzie przesyłana z i do

urządzenia, np. po zalogowaniu na pocztę uzyska login i hasło. Poza tym cyberprzestępca za pomocą takiej sieci może również nagrywać obraz i dźwięk oraz rejestrować każdy naciśnięty klawisz przez wgranie wirusa do urządzenia. Właściciel urządzania mobilnego (np. smartfonu) nie ma pojęcia o przeprowadzonym ataku i kradzieży danych. Zazwyczaj nie posiada on nawet aktualnego oprogramowania antywirusowego. Wirus zainstalowany na urządzeniu z pewnością może zostać wykorzystany wielokrotnie przez hakera, podczas połączenia z Internetem. Dlatego zdecydowanie bezpieczniej jest wyłączać funkcje GPS oraz Wi-Fi, gdy nie są używane, a także korzystać tylko z szyfrowanych, pewnych i bezpiecznych połączeń internetowych. Dodatkowo warto zabezpieczyć się przynajmniej w program antywirusowy i zwrócić szczególną uwagę, jakie materiały posiadamy na swoich urządzeniach. O bezpieczeństwo w sieci każdy musi zadbać indywidualnie[12].

Badania CBOS z 2015 r. pokazały, że świadomość zagrożeń jest na niskim poziomie, a dane osobowe nie są dostatecznie chronione. Społeczeństwo w sieci chętnie dzieli się danymi o sobie, w szczególności użytkownicy serwisów społecznościowych, którzy nie zwracają uwagi na możliwe konsekwencje.

Stosowanie silnych haseł

Głównym kluczem dostępu do informacji o użytkownikach Internetu jest hasło. Wiele osób dla własnej wygody korzysta z bankowości internetowej, a także posiada inne konta w różnych serwisach. W związku z tym dane osobowe tych użytkowników są dostępne w sieci. Logowanie do poczty elektronicznej, konta w serwisie społecznościowym czy banku następuje przez wpisanie nazwy – loginu lub adresu poczty e-mail oraz hasła. Odpowiednie zabezpieczenie dostępu przed osobami niepowołanymi to podstawowy element ochrony swoich danych w Internecie, na komputerze i urządzeniach mobilnych.

Włamanie do konta może spowodować, że dane użytkownika zostaną skradzione i wykorzystane przez cyberprzestępców do zawierania transakcji internetowych, utworzenia nowego konta lub podpisania umowy kredytowej. Dlatego tak ważne jest tworzenie silnych i skutecznych haseł trudnych do złamania. Niestety większość osób nie zna zasad tworzenia bezpiecznych haseł, korzystając z ciągu kolejnych liter i cyfr. Jest to błędem, ponieważ takie hasło można łatwo złamać. Kolejnym poważnym problemem jest stosowanie jednego hasła do wszystkich posiadanych kont. W takiej sytuacji, gdy przestępca

złamie jedno hasło, będzie miał dostęp do wszystkich witryn. Silne hasło ma utrudnić życie przestępcom i ochronić przed utratą danych[13].

Społeczeństwo internetowe nadal nie zdaje sobie sprawy z tego, na jakie niebezpieczeństwo jest narażone, korzystając z sieci. Badania Europ Assistance pokazują, że wiele osób korzysta z różnych stron i aplikacji, które wymagają logowania przez hasło. Okazuje się, że 37% osób ma kilka haseł do wszystkich stron. Poza tym 33% użytkowników tego typu serwisów nigdy nie zmienia hasła, a 43% zmienia je czasami, co jest powodem do zaniepokojenia.

Tworząc hasła, warto kierować się poniższymi zasadami[14]:

1. Hasło powinno zawierać przynajmniej 8 znaków. Wzorowe będzie takie, które posiada 14 znaków. Jeśli jest to możliwe, stosowanie spacji spowoduje, że hasło będzie złożone z kilku słów, co utrudni jego złamanie i ułatwi zapamiętanie.
2. Do tworzenia hasła należy wykorzystywać całą klawiaturę, różnorodne znaki: litery, cyfry i symbole, a nie tylko podstawowe. Im bardziej są różnorodne, tym trudniej odgadnąć hasło. Im mniej takich znaków, tym hasło powinno być dłuższe.
3. Budując hasło, należy używać łatwych do zapamiętania słów i zwrotów, które jednocześnie będą trudne do odgadnięcia przez osoby trzecie. Hasło można zapisać na papierze, ale trzeba je odpowiednio zaszyfrować i przechowywać w bezpiecznym miejscu.

Tworząc hasło, warto zacząć od ułożenia zdania, które będzie łatwo zapamiętać. Następnie dodajemy wielkie lub małe litery, cyfry i symbole. Siłę hasła można sprawdzić przez narzędzie do sprawdzania siły haseł. Należy pamiętać, aby unikać[15]:

- powtórzeń znaków lub sekwencji,
- korzystania z własnej nazwy użytkownika,
- korzystania z jednego hasła,
- przechowywania haseł w sieci (np. poczta e-mail) i na komputerze,
- używania wyrazów ze słownika dowolnego języka,
- zamiany liter na znaki wyglądające podobnie.

Po utworzeniu hasła trzeba kierować się zasadami bezpieczeństwa, między innymi:

- należy chronić zapisane hasła,
- nie wolno udostępniać hasła osobom trzecim,

- nie należy podawać hasła w wiadomościach e-mail,
- należy regularnie zmieniać hasło,
- nie wolno wpisywać haseł podczas korzystania z komputerów, nad którymi nie posiada się kontroli.

Istotnym faktem jest to, że nie można zapewnić 100% ochrony w systemach teleinformatycznych. Podobnie jest w przypadku powszechnego użytkownika serwisów internetowych (Banaszak, 2013, s. 139–158). Można jedynie ograniczyć niebezpieczeństwo płynące z sieci, ponieważ nawet najsilniejsze hasło może zostać złamane. Dlatego należy często zmieniać hasło, a każde podejrzenie uzyskania dostępu do konta przez osoby trzecie, warto zgłosić odpowiednim instytucjom (Pieczyrak, 2013).

Zapewnienie bezpieczeństwa w cyberprzestrzeni jest dużym wyzwaniem dla służb państwowych i instytucji. Dynamiczny rozwój Internetu i nowych technologii oraz masowa komputeryzacja prawie każdej dziedziny życia, są skutkiem powstania świata wirtualnego, w którym istnieje i funkcjonuje społeczeństwo. Internet stał się potężnym medium komunikacji międzyludzkiej i wymiany informacji.

Bibliografia

13 zasad bezpiecznego Internetu, http://www.bezpiecznypc.pl/zapobieganie.php (dostęp: 12.09.2017).

Banaszak A. (2013). *Oświata i edukacja a bezpieczeństwo społeczne*, [w:] M. Such-Pyrgiel, *Bezpieczeństwo społeczne w XXI wieku w ujęciu socjologicznym, pedagogicznym, prawnym i nauk o zarządzaniu*. Józefów: Wydawnictwo WSGE.

Bezpieczeństwo w cyberprzestrzeni zarys problemu, wyzwania i zagrożenia, https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 12.09.2017).

Bezpieczeństwo w internecie. Ogólne zasady, http://www.nina.gov.pl/baza-wiedzy/bezpieczeC5%84stwo-w-internecie-og%C3%B3lne-zasady/ (dostęp: 12.09.2017).

Doswell F. (2008). *A case study on computer security for non-expert computer user*, USA, 361-365, doi.acm.org/10.1145/1593105.1593201 (dostęp: 12.09.2017).

Hofstede G. (1992). *Cultural and Organizations – Software of the Mind Intercultural Cooperation and its importance for survival*, New York: McGraw-Hill.

Jak rozpoznać niebezpieczne wiadomości e-mail?, https://kapitalni.org/pl/artykuly/jak-rozpoznac-niebezpieczne-wiadomosci-e-mail,73,21 (dostęp: 12.09.2017).

Jak sprawdzić, czy strona internetowa jest bezpieczna, http://pl.ccm.net/faq/9732-jak-sprawdzic-czy-strona-internetowa-jest-bezpieczna (dostęp: 12.09.2017).

Jak uchronić się przed niebezpiecznymi wiadomościami e-mail?, https://artykuly.softonic.pl/jak-uchronic-sie-przed-niebezpiecznymi-wiadomosciami-e-mail (dostęp: 12.09.2017).

Kowalska W., Bednarek W. (red.). (2014). *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*. Warszawa: Difin.

Kozak S. (2007). *Patologie wśród dzieci i młodzieży. Leczenie i profilaktyka*. Warszawa: Wydawnictwo Difin.

Które pliki z internetu są bezpieczne, a które niebezpieczne?, https://www.akademiakomputronik.pl/ artykul/ ktore-pliki-z-internetu-sa-bezpieczne-a-ktore-niebezpieczne (dostęp: 12.09.2017).

Maikowski D., *Pomyśl zanim klikniesz: dlaczego warto czytać regulaminy serwisów internetowych*, http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/800428,pomysl-zanim-klikniesz-dlaczego-warto-czytac-regulaminy-serwisow-internetowych.html. dn. 31.05.2014 (dostęp: 12.09.2017).

Majewski A., *Jak sprawdzić, czy można ufać wiadomości e-mail?*, http://www.ekademia.pl/blog/ bezpieczenstwoinformacji/4395. dn. 19.02.2009 (dostęp: 12.09.2017).

Ng B.Y., Rahim M.A. (2005). *A Socio-Behavioral Study of Home Computer Users Intention to Practice Security, Proceedings of the Ninth Pacific Asia Conference on Information Systems*, Bangkok, 7–10 July, Thailand.

Ng B.Y., Kankanhalli A., Xu Y.C. (2009). *Studying users' computer security behavior: A health belief perspective*, "Decision Support System", 46 (4), 815–825.

Otwarte sieci wi-fi – czy mogą być niebezpieczne?, http://www.systel.pl/otwarte-sieci-wi-fi/ (dostęp: 12.09.2017).

Pieczyrak P., *Poradnik – Jak być bezpiecznym w Internecie*, https://www.purepc.pl/oprogramowanie/ poradnik_jak_byc_bezpiecznym_w_internecie. dn. 18.09.2013 (dostęp: 12.09.2017).

Sobianek M., *Bezpieczna strona internetowa – jak ją rozpoznać?*, http://biznes.gazetaprawna.pl/ artykuly/28904,bezpieczna-strona-internetowa-jak-ja-rozpoznac.html. dn. 31.07.2008 (dostęp: 12.09.2017).

Strzałkowski M., *3 kroki do ochrony danych w sieci*, http://nf.pl/manager/3-kroki-do-ochrony-danych-osobowych-w-sieci,,45324,276 (dostęp: 12.09.2017).

Szafrańska E., Szafrański J. (2014). *Edukacja na rzecz bezpieczeństwa*, „Journal of Modern Science", 21(2).

Tu Z., Yuan Y. (2012). *Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft, 2012 45th Hawaii International Conference on System Science (HICSS)*, 4–7 January 2012, 1393-1402, doi:10.1109/HICSS.2012.620.

Turek A., *5 sposobów na ochronę danych osobowych w sieci*, http://innpoland.pl/115009,5-sposobow-na-ochrone-danych-osobowych-w-sieci. dn. 29.01.2015 (dostęp: 12.09.2017).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2016 r. poz. 922).

Van Niekerk J., Goss R. (2013). *Towards information security education 3.0: A call for information security educational ontologies*, January 2013 IFIP Advances in Information and Communication Technology 406, 180–187, doi: 10.1007/978-3-642-39377-8_20.

Wiśniewska A., *Ochrona danych osobowych w serwisach społecznościowych*, http://www.infor.pl/ prawo/ prawo-karne/ ciekawostki/298879,Ochrona-danych-osobowych-w-serwisach-spolecznosciowych.html (dostęp: 12.09.2017).

Zasady tworzenia silnych i skutecznych haseł, http://www.bezpiecznypc.pl/zasady-tworzenia-hasel.php (dostęp: 12.09.2017).

Endnotes

[1] *Bezpieczeństwo w internecie. Ogólne zasady*, http://www.nina.gov.pl/baza-wiedzy/bezpieczne%C5%84stwo-w-internecie-og%C3%B3lne-zasady/.

[2] Okna pop-up – okna internetowe, które pokazują się na wierzchu, zasłaniając stronę główną.

[3] *Jak sprawdzić, czy strona internetowa jest bezpieczna*, http://pl.ccm.net/faq/9732-jak-sprawdzic-czy-strona-internetowa-jest-bezpieczna.

[4] *Jak rozpoznać niebezpieczne wiadomości e-mail?*, https://kapitalni.org/pl/artykuly/jak-rozpoznac-niebezpieczne-wiadomosci-e-mail,73,21.

[5] *Jak uchronić się przed niebezpiecznymi wiadomościami e-mail?*, https://artykuly.softonic.pl/jak-uchronic-sie-przed-niebezpiecznymi-wiadomosciami-e-mail.

[6] Spyware – szkodliwe oprogramowanie szpiegujące, którego celem jest gromadzenie informacji o użytkowniku, a także ich przesyłanie bez jego wiedzy innym osobom.

[7] *Które pliki z internetu są bezpieczne, a które niebezpieczne?*, https://www.akademiakomputronik.pl/ artykul/ ktore-pliki-z-internetu-sa-bezpieczne-a-ktore-niebezpieczne.

[8] Tamże.

[9] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., nr 133 poz. 883).

[10] A. Wiśniewska, *Ochrona danych osobowych w serwisach społecznościowych*, http://www.infor.pl/ prawo/ prawo-karne/ ciekawostki/298879,Ochrona-danych-osobowych-w-serwisach-spolecznosciowych.html.

[11] M. Strzałkowski, *3 kroki do ochrony danych w sieci*, http://nf.pl/manager/3-kroki-do-ochrony-danych-osobowych-w-sieci,,45324,276

[12] *Otwarte sieci wi-fi – czy mogą być niebezpieczne?*, http://www.systel.pl/otwarte-sieci-wi-fi/

[13] *Zasady tworzenia silnych i skutecznych haseł*, http://www.bezpiecznypc.pl/zasady-tworzenia-hasel.php.

[14] Tamże.

[15] Tamże.