ARTYKUŁ PRZEGLĄDOWY

Rozprawy Społeczne 2016, Tom 10, Nr 3
ISSN 2081-6081

ZAGROŻENIA W CYBERPRZESTRZENI A BEZPIECZEŃSTWO JEDNOSTKI

THE CYBERSPACE HAZARD AND THE SAFETY UNIT

Jadwiga Żuk[1(A,B,C,D,E,F,G)], **Monika Żuk**[1(A,B,C,D,E,F,G)]

[1]Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach,
Wydział Humanistyczny, Instytut Nauk Społecznych i Bezpieczeństwa

Żuk J., Żuk M. (2016), *Zagrożenia w cyberprzestrzeni a bezpieczeństwo jednostki*. Rozprawy Społeczne, 3 (10), s. 71-77.

Wkład autorów:
A. Zaplanowanie badań
B. Zebranie danych
C. Dane – analiza i statystyki
D. Interpretacja danych
E. Przygotowanie artykułu
F. Wyszukiwanie i analiza literatury
G. Zebranie funduszy

Streszczenie
Dynamiczny rozwój technologii teleinformatycznych przyczynił się do powstania nowego pola aktywności, jakim jest cyberprzestrzeń. Jest to jedna z najważniejszych zmian w środowisku bezpieczeństwa, niosąca zupełnie nowe zagrożenia, a przez to wymagająca nowych uregulowań, zabezpieczeń i informacji celem zapewnienia bezpieczeństwa państwa, instytucji i osób korzystających z cyberprzestrzeni. W dobie globalizacji cyberprzestrzeń, która nie zna granic może być polem konfliktu wrogich państw, zorganizowanych grup przestępczych, ekstremistycznych, terrorystycznych, hakerów, oszustów, a nawet pedofilów. Jak widać stawka może być bardzo wysoka, od bezpieczeństwa infrastruktury krytycznej, poprzez wyniki finansowe przedsiębiorstw, szeroko rozumiane bezpieczeństwo obywateli, a nawet dzieci.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo jednostki

Summary
The dynamic development of Information and Communications Technology (ICT) contributed to the emergence of a new field of activity; that is cyberspace. It is one of the most important changes in the safety environment that carries a completely new security threat and, therefore, requires new regulations, protection and information to assure security of the institutions and people who use cyberspace. In the era of globalisation, cyberspace does not have any barriers, which can lead to many conflicts between hostile states, gangs, terrorists, extremist groups, hackers, the frauds or even paedophiles. Thus, as one can see, the stakes are high when it comes to securing critical infrastructure or financial companies' results as well as citizens' safety, including children.

Keywords: cyberspace, cyber security, a cyber crime, a safety unit

Tabele: 1
Ryciny: 1
Literatura: 23
Otrzymano: 11.04.2016
Zaakceptowano: 27.04.2016

Wraz z rozwojem technologii cyfrowej i związanego z nią społeczeństwa informacyjnego pojawił się nowy obszar bezpieczeństwa, który pozostaje nieograniczony terytorialnie, a dotyczy niemal wszystkich dziedzin życia przeniesionych do cyberprzestrzeni. Bezpieczeństwo zajmuje jedno z czołowych miejsc w sferze podstawowych potrzeb człowieka. Jest terminem interdyscyplinarnym i jest różnie definiowane. „Bezpieczeństwo – stan dający poczucie pewności i gwarancje jego zachowania oraz szansę na doskonalenie" (Słownik terminów… 2008, s. 14). Podejmując próbę zdefiniowania cyberprzestrzeni można przytoczyć kilka definicji: słownik języka polskiego: „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową" (http://sjp.pwn.pl). Tadeusz Jemioło twierdzi, że: „Cyberprzestrzeń to przede wszystkim ogromna ilość rozpowszechnianych informacji, przez co Internet stał się podatnym gruntem do szeroko zakrojonych działań wywiadowczych. Niektóre największe kraje na świecie (m. in. Rosja czy Chiny) prowadzą na dużą skalę szpiegostwo internetowe, głównie pod kątem zbierania niejawnych informacji gospodarczych dotyczących na przykład najnowszych technologii, systemów militarnych czy przemysłu farmaceutycznego danego państwa" (http://tadeuszjemiolo.natemat.pl/133631, cyberprzestrzen-nowa-sfera-walki-xxi-wieku). Pojęcie cyberprzestrzeni wraz z prawnymi podstawami nadzwyczajnego reagowania na występujące w niej zagrożenia do polskiego systemu prawnego zostało wprowadzone w 2011 roku m. in. w ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw i otrzymało brzmienie: „Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne(…)" (Ustawa

Adres korespondencyjny: Jadwiga Żuk, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Wydział Humanistyczny, Instytut Nauk Społecznych i Bezpieczeństwa, ul. Żytnia 39, 08-110 Siedlce, e-mail: j.zuk@interia.pl, tel.: 25 643 18 62

z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym…, art. 1 ust. 1). Zarówno Unia Europejska, jak i poszczególne państwa członkowskie podejmują działania na rzecz bezpiecznej cyberprzestrzeni, czyli bezpiecznego korzystania z technologii cyfrowej i informacyjnej i tak np. w 2004 r. powołana została ENISA, czyli Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, której celem jest zwiększenie możliwości Unii Europejskiej, państw członkowskich, a także sektora biznesu w zakresie ochrony i bezpieczeństwa w sieciach i systemach informatycznych. Mimo podejmowanych działań szybki rozwój technologii informatycznych uniemożliwia skuteczne zapewnienie bezpieczeństwa w sieci. Prawdopodobieństwo różnego rodzaju ataków stanowi zagrożenie dla bezpieczeństwa, obrony, stabilności i konkurencyjności państw oraz sektora prywatnego. Po serii fałszywych alarmów bombowych, ogłoszonych 25 czerwca 2014 r. szef BBN Stanisław Koziej powiedział: „Musimy pilnie zbudować fundamenty cyberbezpieczeństwa, by w sposób skoordynowany i bezpieczny reagować na ryzyko. Na szczęście ten alarm okazał się fałszywy, ale pokazał, co mogłoby się dziać, gdyby ktoś chciał nie tylko przesłać fałszywą wiadomość, ale np. spowodować jakąś awarię. To klarowny sygnał, że trzeba te zagrożenia traktować poważnie" (http: //www.bbn.gov.pl/pl/prace-biura/glowne-inicjatywy/doktryna-cyberbezpiecze/6058,Doktryna cyberbezpieczenstwa-RP.html). Fałszywe alarmy bombowe spowodowały, że sprawdzono 22 obiekty użyteczności publicznej – szpitale, sądy, budynki prokuratury i policji, a także centra handlowe. Ponad 2700 osób było zmuszonych do opuszczenia budynków. Ostrzeżenia te wysyłano z serwerów w kraju i za granicą. Bezpieczeństwo w cyberprzestrzeni ze względu na złożoność problemu jest rozpatrywane wielopłaszczyznowo i wymaga zintegrowanego i kompleksowego podejścia administracji, służb, sił zbrojnych, sektora prywatnego i obywateli. W Biurze Bezpieczeństwa Narodowego został opracowany i 12 stycznia 2015 roku zaakceptowany przez Radę Bezpieczeństwa Narodowego dokument - Doktryna cyberbezpieczeństwa RP, w którym określone są cele strategiczne takie jak, zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej w cyberprzestrzeni, a także wprowadzenie określonych rozwiązań formalno-prawnych. „Doktryna jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego RP. Określa cele w dziedzinie cyberbezpieczeństwa, opisuje środowisko, wskazując na zagrożenia, ryzyka i szanse, a także rekomenduje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa" (https://www.bbn.gov.pl/pl/wydarzenia/ 6336,Doktryna-cyberbezpieczenstwa-RP.html.). Jak słusznie zauważył Bronisław Komorowski: „Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi, czy zorganizowanymi grupami przestępczymi. Dlatego jednym z istotnych priorytetów polskiej strategii stało się bezpieczeństwo tego nowego środowiska" (B. Komorowski, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf). Jest to zupełnie nowy obszar działalności w zakresie bezpieczeństwa, a trudność w jej opanowaniu polega na dużej dynamice zmian. „Doktryna powinna stanowić punkt odniesienia i ukierunkowania dla dalszych prac, tworzących zaawansowane rozwiązania na rzecz bezpieczeństwa Polski i Polaków w cyberprzestrzeni" (http://www.bbn.gov.pl/pl/prace-biura/glowne-inicjatywy/doktryna-cyberbezpiecze/6058,Doktryna-cyberbezpieczenstwa-RP.html).

W dobie globalizacji Internet dla współczesnego użytkownika stał się nieodzownym elementem egzystencji zarówno w życiu prywatnym, jak i zawodowym. Trudno sobie wyobrazić już nie tylko współczesnego nastolatka, który potrafi obejść się bez nowych technologii, ale również osoby dorosłe, a coraz częściej seniorów. Negatywnym skutkiem szybkiego rozwoju teleinformatycznego są nowe zagrożenia płynące z cyberprzestrzeni. Bezpieczeństwo w cyberprzestrzeni jest tym bardziej ważne, że korzystają z niej ludzie praktycznie w każdym wieku, z różnym poziomem wykształcenia i świadomości. Bezpieczeństwo to określa w następujący sposób Ministerstwo Administracji i Cyfryzacji: „bezpieczeństwo cyberprzestrzeni - zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni" (Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013, s. 5). Równocześnie z rozwojem i udoskonalaniem możliwości korzystania z nowych technologii rozwija się pomysłowość przestępców działających w sieci. Przestępstwa te określane są cyberprzestępstwami. Jak twierdzi Artur Kubiak z Wydziału do Walki z Cyberprzestępczością KWP w Katowicach „w polskim prawie nie ma legalnej, czyli jednolitej przyjętej przez prawo definicji cyberprzestępczości. Można więc posługiwać się tym pojęciem intuicyjnie (rozumując, iż są to przestępstwa popełniane za pomocą komputerów oraz Internetu), albo pomocniczo posłużyć się definicjami, które formułują inne podmioty np. ONZ, Rada Europy, Unia Europejska, czy też INTERPOL" (http://konferencje.alebank.pl/wp-content/uploads/2015/07/prezentacja.artur_.kubiak.pdf). W literaturze możemy spotkać wiele podziałów cyberprzestępstw. Jeden z nich prezentuje wspomniany już A. Kubiak: „Definicja sformułowana przez Interpol jest bardzo praktyczna i rozpatruje cyberprzestępczość w 2 ujęciach tzw. wertykalnym oraz horyzontalnym. Ujęcie wertykalne dotyczy przestępstw specyficznych dla cyberprzestrzeni, czyli takich które tylko tam mogą być dokonane np. hacking, sabotaż komputerowy. Z kolei ujęcie horyzontalne zakłada popełnianie przestępstw przy pomocy technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, carding, skimmingu, pranie brudnych pieniędzy, naruszanie praw autorskich, czy sprzedaż rzeczy zabronionych lub wymagają-

cych koncesji albo pedofilia, etc.)" (http://konferencje.alebank.pl/wp-content/uploads/2015/07/prezentacja.artur_.kubiak.pdf). Pojawienie się i szybki rozwój technologii informacyjnych w drugiej połowie XX w. wymusiło potrzebę opracowania instrumentów ochraniających użytkowników Internetu i ochrony danych osobowych osób fizycznych. Wynikiem tego było podpisanie 28 stycznia 1981 roku 108 Konwencji Rady Europy. „Konwencja nr 108 ma zastosowanie do wszelkich operacji przetwarzania danych prowadzonych zarówno przez sektor prywatny, jak i publiczny, np. do przetwarzania danych przez organy sądowe i organy ds. egzekwowania prawa. Zapewnia ona osobom fizycznym ochronę przed nadużyciami, które mogą towarzyszyć gromadzeniu i przetwarzaniu danych osobowych, a jej drugim celem jest uregulowanie transgranicznego przepływu danych osobowych" (Podręcznik europejskiego prawa o ochronie danych2014, s. 16). Internet przestał być tylko źródłem informacji czy rozrywki, a stał się niezbędny do pracy, edukacji, komunikacji, obsługi banku czy korzystania z usług urzędów, służby zdrowia i wielu innych. „Prawo do ochrony sfery prywatnej jednostki przed ingerencją ze strony innych, a zwłaszcza ze strony państwa, po raz pierwszy zapisano w międzynarodowym akcie prawnym w art. 12 Powszechnej Deklaracji Praw Człowieka Organizacji Narodów Zjednoczonych (ONZ) z 1948 r., który dotyczy poszanowania życia prywatnego i rodzinnego. PDPC wpłynęła na rozwój innych instrumentów ochrony praw człowieka w Europie" (Rada Europy (RE) i Europejski Trybunał Praw Człowieka (ETPC), Podręcznik europejskiego prawa o ochronie danych, Luksemburg 2014, s. 14).

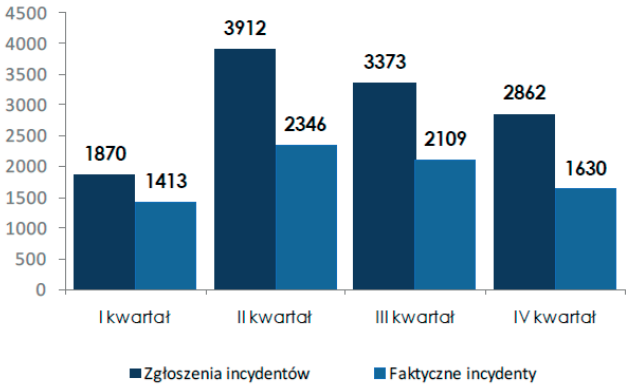
Na całym świecie podejmowane są różne inicjatywy na rzecz zwiększenia bezpieczeństwa w sieci. W 1999 roku został uruchomiony program Komisji Europejskiej „Safer Internet", ma on na celu promocję bezpiecznego korzystania z nowych technologii i Internetu wśród dzieci i młodzieży. W ramach tego programu prowadzone są również działania na rzecz zwalczania nielegalnych treści i spamu w Internecie. Również polski rząd podejmuje różne działania mające na celu zapewnienie bezpieczeństwa w cyberprzestrzeni. W dniu 01 lutego 2008 roku na mocy porozumienia Ministra Spraw Wewnętrznych i Administracji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego powołany został CERT.GOV.PL (ang. Computer Emergency Response Team) – Rządowy Zespół Reagowania na Incydenty Komputerowe. Mimo coraz większej ilości publikacji i akcji mających na celu świadome korzystanie z nowych technologii i jak najlepsze zabezpieczenie przed cyberprzestępstwami, liczba poszkodowanych z roku na rok jest większa. W strukturach policji od 1 października 2014 roku funkcjonuje wydział do walki z cyberprzestępczością powołany przy Biurze Służby Kryminalnej Komendy Głównej Policji.

Przestępstwa popełniane w cyberprzestrzeni A. Kubiak podzielił następująco:

„•Malware
•Spam
•Kradzież tożsamości
•Botnet
•Phishing
•DDos
•Darknet
•Płatności anonimowe i kryptowaluty
•Internet IPR
•Pornografia dziecięca
•Hazard internetowy
•Oszustwa na aukcjach internetowych
•Oszustwa telekomunikacyjne
•Pranie pieniędzy
•Carding" (http://konferencje.alebank.pl/wp-content/uploads/2015/07/prezentacja.artur_.kubiak.pdf).

Analizując dane CERT.COV.PL z raportu o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014 można dostrzec wyraźny wzrost dynamiki ataków. Również liczba internautów na świecie wzrasta praktycznie każdego dnia.

Poniższy wykres obrazuje ilość zarejestrowanych zgłoszeń oraz obsłużonych przez Zespół CERT.GOV.PL incydentów teleinformatycznych w poszczególnych kwartałach 2014 roku.



Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2014 roku
Źródło:http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html

Tabela 1. Katalog zagrożeń CERT.GOV.pl

ZAGROŻENIA		PODATNOŚCI				
1. DZIAŁANIA CELOWE	1.1 OPROGRAMOWANIE ZŁOŚLIWE	wirus	robak sieciowy	koń trojański	dialer	botnet
	1.2 PRZEŁAMANIE ZABEZPIECZEŃ	nieuprawnione logowanie	włamanie na konto/ataki sieciowe		włamanie do aplikacji	
	1.3 PUBLIKACJE W SIECI INTERNET	treści obraźliwe	pomawianie (zniesławienie)	naruszenie praw autorskich	dezinformacja	
	1.4 GROMADZENIE INFORMACJI	skanowanie	podsłuch	inżynieria społeczna	szpiegostwo	SPAM
	1.5 SABOTAŻ KOMPUTEROWY	nieuprawniona zmiana informacji	nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji			
		atak odmowy dostępu (np. DDoS, DOS)	skasowanie danych			
		wykorzystanie podatności w urządzeniach	wykorzystanie podatności aplikacji			
	1.6 CZYNNIK LUDZKI	naruszenie procedur bezpieczeństwa	naruszenie obowiązujących przepisów prawnych			
	1.7 CYBERTERRORYZM	przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni				
2. DZIAŁANIA NIECELOWE	2.1 WYPADKI I ZDARZENIA LOSOWE	awarie sprzętowe	awarie łącza	awarie (błędy oprogramowania)		
	2.2 CZYNNIK LUDZKI	naruszenie procedur	zaniedbanie	błędna konfiguracja urządzenia	brak wiedzy	naruszenia praw autorskich

Źródło: http://www.cert.gov.pl

Dostęp do usług elektronicznych stał się bardzo powszechny i jest możliwy przy użyciu różnych urządzeń, już nie tylko komputerów, ale również telefonów komórkowych, smartfonów czy tabletów. Cyberprzestępcy bardzo szybko wykorzystują nowe możliwości i coraz więcej ataków odnotowuje się na urządzenia mobilne, które obsługują coraz większą ilość aplikacji. „Zmiany zachodzące we współczesnym świecie, globalizacja procesów i zjawisk gospodarczych pociągają za sobą także globalizację bezpieczeństwa. Pojawienie się nowych, nieznanych dotąd zagrożeń, zatarcie granic między sferą militarną i pozamilitarną wymusza opracowanie nowego katalogu zagrożeń dla bezpieczeństwa powszechnego. Obecnie widać rosnącą współzależność poszczególnych sektorów gospodarki i całego życia społecznego, od zaawansowanych technologii, sprawnego funkcjonowania systemów energetycznych, transportowych i teleinformatycznych" (M. Tryboń, I. Grabowska - Lepczak, M. Kwiatkowski, Bezpieczeństwo człowieka w obliczu zagrożeń XXI).

Większość dziedzin aktywności człowieka została przeniesiona do sieci. W szybkim tempie wzrasta liczba przestępstw popełnianych w Internecie. Przestępcy wybierając na swoje pole działania sieć, liczą na pozostanie anonimowymi i łatwiejsze zacieranie śladów. Jak mówi rzecznik komendanta głównego policji: „Oszuści szukają swoich ofiar w „sieci", bo daje im ona anonimowość. - Z oszustem nie ma praktycznie żadnego kontaktu. Z kolei on sam, poprzez internet, może tworzyć dowolne scenariusze - sprzedawać „markowe rzeczy" w atrakcyjnych cenach, oferować fikcyjne apartamenty lub pokoje hotelowe, podawać się za krewnego z zagranicy, informującego o dużym spadku. Namierzenie go jest też trudne, bo często do oszustw wykorzystywane są zagraniczne serwery. Nawet, jeśli wiemy, że dana osoba odpowiada za zgłoszone nam przestępstwa, czasem

trudno jej to udowodnić" (M. Sokołowski,http://wiadomosci.onet.pl/kraj/w-2014-r-ponad-22-tys-internetowychoszustw/xgr95 stan na 23.03.2016r.). Przestępcy działający w Internecie szukają nowych metod, pomysłów i wykorzystują nowoczesne technologie i oprogramowanie dostosowując je do rodzaju przestępstwa. W XXI wieku nawet szukanie pracy najczęściej odbywa się przez Internet. Ta sama droga aplikacji jest wymagana niezależnie od stanowiska pracy. Niestety, przy tej okazji czyha wiele zagrożeń.

Przy zachowaniu największej ostrożności dotyczącej haseł, loginów itd. aplikując o pracę należy wysłać co najmniej CV i LM. Osoba aplikująca zdradza wówczas niemal wszystkie swoje dane, nie mając pewności, że ogłoszenie o pracę jest prawdziwe i uczciwe. Jest to bardzo prosty sposób na wyłudzenie danych. Zamieszczając w Internecie ogłoszenie o pracę z obietnicą dobrych warunków, przy tak dużym bezrobociu można mieć pewność, że odpowie wiele osób. Nie ma innej możliwości zgłoszenia swojej kandydatury niż przez Internet. Ogłoszenie o wolnych stanowiskach pracy może zamieścić każdy. Brak instrumentów weryfikacji wszystkich ogłoszeniodawców powoduje często bezkarne wyłudzanie danych osobowych, co w konsekwencji może być wykorzystywane przy różnego rodzaju przestępstwach. Najczęstszą praktyką przy użyciu takich dokumentów jest zaciąganie zobowiązań finansowych, wyłudzanie kredytów, podpisywanie umów na usługi mobilne, a nawet zakładanie fikcyjnych firm, które wystawiają fikcyjne zaświadczenia, co rozpoczyna falę zdarzeń czy przestępstw, które często niszczą życie właścicielowi dokumentów. Nawet bez dokumentów, mając tak wiele danych osobowych przestępca łatwo może podrobić dokumenty i dopisać całą historię człowieka. Coraz bardziej powszechne jest załatwianie spraw przez Internet bez konieczności wizyty w urzędzie, a parabanki prześcigają się w szybkości udzielania kredytów przez Internet.

Bywa, że przy ofertach pracy, szczególnie zagranicznych wymagany jest skan dokumentów. Osoby poszukujące pracy często są zdesperowane i nie podejrzewając niczego złego padają ofiarami przestępstw. Zakres danych zatrudnianych osób przetwarzanych przez pracodawcę jest tematem licznych wypowiedzi w polskiej literaturze. Jak twierdzi E. Kulesza: „pracodawca ma prawo żądać od pracownika podania imienia (imion) i nazwiska, imion rodziców, daty urodzenia, miejsca zamieszkania (adresu do korespondencji), informacji o wykształceniu oraz informacji o przebiegu dotychczasowego zatrudnienia. Ponadto także innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy oraz numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL)" (E. Kulesza, Kilka uwag o przetwarzaniu danych osobowych pracowników przez pracodawcę – regulacje obowiązujące i uwagi de lege ferenda, w Ochrona danych osobowych wczoraj, dziś, jutro, Warszawa 2006).

Inną sprawą jest wykorzystywanie danych osobowych niezgodnie z przeznaczeniem. Każde CV użyte w procesie rekrutacji musi być opatrzone klauzulą wynikającą z ustawy o ochronie danych osobowych o wyrażeniu zgody na przetwarzanie danych osobowych: „Wyrażam zgodę na przetwarzanie danych osobowych zawartych w aplikacji dla potrzeb procesu rekrutacji zgodnie z ustawą z dnia 29.08.1997 r. o Ochronie Danych Osobowych, tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926 z późniejszymi zmianami" (ustawa z dnia 29.08.1997 r. o ochronie danych osobowych, tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926 z późniejszymi zmianami). Czym jest owa zgoda na przetwarzanie danych osobowych i na co jest wyrażana? „Niektórzy uważają, że normy regulujące sferę ochrony prywatności nie powinny dotyczyć życia zawodowego. Jednak Europejski Trybunał Praw Człowieka przyjął w swoich orzeczeniach konsekwentne stanowisko, zgodnie z którym zasady ochrony prywatności powinny być stosowane również w przypadku pracowników, a nie odnosić się wyłącznie do ich życia prywatnego" (Biuro GIODO, Ochrona danych osobowych wczoraj, dziś, jutro, Warszawa 2006, s. 29). Osoba ubiegająca się o pracę zamieszczając powyższą klauzulę w dokumentach aplikacyjnych wyraża zgodę na to, aby pracownicy danej firmy zajmujący się rekrutacją przeglądali te dokumenty i upoważnia do wykorzystania tych dokumentów w konkretnym procesie rekrutacyjnym danej firmy. Wysłanie dokumentów nieopatrzonych wymaganą klauzulą powinno skutkować odrzuceniem kandydatury bez rozpatrzenia. Nie jest to jednak wyrażenie zgody na obrót danymi osobowymi w innym celu, np. marketingowym, co nie jest niestety rzadkością. Takie działanie jest niezgodne z prawem. Jeśli firma rekrutująca chce zarekomendować kandydata innemu pracodawcy, musi mieć jego pisemną zgodę na przekazanie dokumentów aplikacyjnych. Idealnym stanem byłoby utworzenie portalu z ogłoszeniami o pracę, gdzie oferty byłyby weryfikowane, co dawałoby aplikującym poczucie bezpieczeństwa. Niezaspokojenie tej potrzeby, czyli brak poczucia bezpieczeństwa równa się z poczuciem zagrożenia. Zarówno w ujęciu globalnym, jak i jednostkowym wpływa destrukcyjnie na jednostkę, a często dotyczy to osób znajdujących się w trudnej sytuacji życiowej.

W przeciwieństwie do konieczności ujawniania danych osobowych przy aplikowaniu do pracy, portale społecznościowe stały się „kopalnią" takich informacji. Dzielenie się swoim życiem prywatnym w sieci stało się powszechne, a zamieszczanie aktualnych informacji jest niemal równoległe do życia w realu, dzięki zaawansowanym technologiom i coraz powszechniej dostępnemu Internetowi. Zachowując wypracowane zasady bezpieczeństwa przy korzystaniu z Internetu zmniejsza się ryzyko kradzieży tożsamości. Nie ma stuprocentowego zabez-

pieczenia przed kradzieżą czy wyłudzeniem danych, ale poza stosowaniem programów antywirusowych należy zachować szczególną ostrożność stosując wypracowane zasady przez odpowiednie służby i instytucje. Oszustwa na aukcjach internetowych stają się codziennością. Mimo ostrzeżeń, aby z rezerwą podchodzić do „super okazji", ciągle znajdują się nowe osoby dające się na to nabierać.

Trudniejsze wydaje się zabezpieczenie przed hakerami, którzy przesyłają na komputer ofiary samo instalujące się programy szpiegowskie wyłudzające loginy i hasła dostępu do kont. W ostatnim czasie jest również wiele prób przekierowania na strony łudząco przypominające stronę banku.

Ochrona danych osobowych w ostatnim czasie jest bardzo ważnym elementem zachowania bezpieczeństwa, a w szczególności bezpieczeństwa w sieci. Jedną z podstawowych instytucji zajmujących się tą tematyką jest GIODO (Generalny Inspektor Ochrony Danych Osobowych), działający na podstawie Ustawy z dnia 29 sierpnia 1997r. GIODO wychodząc naprzeciw użytkownikom Internetu opracował wskazówki jak bezpiecznie korzystać z Internetu. Oto kilka z nich:

- „Internet jest pamiętliwy! Zachowaj ostrożność w dzieleniu się informacjami o sobie – cokolwiek napiszesz na swój temat lub na temat innych osób, usunięcie takiej informacji i wszystkich powielonych jej kopii z sieci Internet jest bardzo trudne lub wręcz niemożliwe.
- Bądź ostrożny w nawiązywaniu znajomości w sieci – tak jak w życiu - osoby, które poznajesz w sieci, mogą nie być tymi, za które się podają i wcale nie muszą chcieć być Twoimi przyjaciółmi.
- Zastanów się jakie informacje o sobie umieszczasz w sieci. Czy chciałbyś, aby te informacje były znane Twoim pracodawcom, nauczycielom, kontrahentom…?
- Podczas rejestracji w portalu i w czasie późniejszego korzystania z niego, nie wpisuj swoich pełnych danych osobowych – wystarczy, że wpiszesz tylko te, które pomogą Twoim faktycznym znajomym w łatwym odnalezieniu Ciebie.
- Celem podniesienia Twojego bezpieczeństwa w portalu staraj się używać bezpiecznych haseł i okresowo je zmieniaj.
- Brak szyfrowania sesji nawiązywanej pomiędzy Tobą a portalem społecznościowym może skutkować w najlepszym wypadku przejęciem lub zmanipulowaniem informacji, które w danym momencie wysyłasz, a w najgorszym kradzieżą Twojej tożsamości – podszyciem się pod Twoje dane w celu osiągnięcia korzyści.
- Publikując zdjęcia z własnym wizerunkiem lub z wizerunkami innych osób musisz mieć świadomość, że znacznie ułatwiasz identyfikację siebie i innych oraz możesz przekazać w ten sposób znacznie więcej informacji niż zdajesz sobie sprawę.
- Podając w portalu społecznościowym informacje o innej osobie oraz publikując jej zdjęcia, upewnij się, że ta osoba nie ma nic przeciwko takiej publikacji.
- Pamiętaj, że pomimo zachowania prywatności w portalu, Twoja anonimowość jest ograniczona i nie istnieje dla osób utrzymujących portal oraz dla organów wymiaru sprawiedliwości w sytuacji naruszenia prawa" (http://nk.pl/bezpieczenstwo/rodzice/giodo/wskazowki).

W czasach, gdy rozwój nowych technologii stwarza wiele możliwości i ułatwia życie, staje się równocześnie pułapką. Cyberbezpieczeństwo jest stosunkowo nowym polem działania państwa i instytucji specjalizujących się w zapewnianiu bezpieczeństwa. Jeśli użytkownicy nie dołożą wszelkich starań do zachowania bezpieczeństwa w sieci, żadna instytucja nie jest w stanie obronić przed skutkami lekkomyślności.

„Dzisiejsze zagrożenia dla bezpieczeństwa to ataki cybernetyczne i terrorystyczne. Hakerzy są w stanie sparaliżować ważne systemy państwa, w tym systemy wojskowe" (T. Siemoniak, http://wiadomosci.wp.pl/kat,1020223,title,Cyberterroryzm-co-robi-Polska-by-uchronic-sie-przed-atakami-hakerow,wid,16257187,wiadomosc.html?ticaid=116bb6, stan na dzień 26.03.2016 r.) – stwierdza na łamach portalu WP.PL, w grudniu 2013 r., minister obrony narodowej, Tomasz Siemoniak. W czasach globalnej wioski, kiedy wszyscy niemal każdego dnia korzystają z dostępu do usług elektronicznych i teleinformatycznych, bezpieczeństwo w cyberprzestrzeni nabrało szczególnego i ważnego znaczenia, chociaż wydaje się trudniejsze do opanowania niż bezpieczeństwo militarne, chociażby ze względu na dynamikę rozwoju, brak granic w świecie wirtualnym, a także niejednolite przepisy w różnych państwach. Istnienie cyberprzestrzeni to niezaprzeczalny fakt tego, iż mamy do czynienia z globalną rewolucją informatyczną. Ogólnoświatowy zasięg w połączeniu z możliwością natychmiastowego dostępu z niemal każdego miejsca na Ziemi i niewielki koszt użytkowania sprawia, że Internet stał się nie tylko formą szybkiej wymiany informacji, czy też głównym motorem napędzającym gospodarkę XXI wieku, ale także przekształcił się w skuteczny instrument działalności przestępczej i terrorystycznej w cyberprzestrzeni, stając się przez to wirtualnym odzwierciedleniem rzeczywistości. Wydaje się, że tylko wspólne działania jak największej ilości państw i organizacji, oraz jednolite w tym zakresie przepisy prawne, będą w stanie ograniczyć cyberprzestępczość i skuteczną z nią walkę. Głównym jednak elementem bezpieczeństwa osobistego każdego internauty jest zachowanie szczególnej ostrożności w sieci, zdrowego rozsądki i zasada ograniczonego zaufania.

Zakończenie

Postęp technologiczny przyczynił się do niespotykanego wcześniej rozwoju cywilizacyjnego, ale również do powstania nowych zagrożeń. Jest to jedna z najtrudniejszych przestrzeni wymagająca zapewnienia bezpieczeństwa. Działania mające na celu zapewnienie bezpieczeństwa w sieci muszą być prowadzone z jednoczesnym uwzględnieniem

ochrony praw człowieka, oraz poszanowaniem wolności słowa i prywatności. Intensywność działania cyberprzestępców wymusza działania zapewniające bezpieczeństwo społeczeństwu informacyjnemu, jak również poszukiwanie rozwiązań prawnych, a stały postęp techniczny skłania do ciągłych weryfikacji ustalonych przepisów i szukania nowych rozwiązań bezpieczeństwa pozamilitarnego.

Literatura:

1. Bednarczyk D., *Przeciwdziałanie cyfrowemu wykluczeniu (e-integracja) w Polsce*, http://open.ebib.pl/ojs/index.php/ebib/article/viewFile/297/469, na dzień 23.03.2016r.
2. Bógdał-Brzezińska A., Gawrycki M. (2003), *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. wydawnictwo, Warszawa.
3. Dijk Van J. (2010), *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci.* Wydawnictwo, Warszawa.
4. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej,* (2015), Warszawa, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, (data dostępu:……).
5. Jemioło T., *Cyberprzestrzeń nową sferą walki XXI wieku*, http://*tadeuszjemiolo.natemat.pl/133631,cyberprzestrzen-nowa-sfera-walki-xxi-wieku*, (data dostępu: 25.03.2016).
6. GIODO, *Ochrona danych osobowych wczoraj, dziś, jutro*, Warszawa 2006.
7. Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, www.bbn.gov.pl/* (data dostępu: 28.05.2015).
8. Kożusznik B. (2004), *Zarządzanie i technologie informacyjne. T. 1, Komunikacja w dobie Internetu*. Wydawnictwo, Katowice.
9. Kubiak A., *Cyberprzestępczość*, *http://konferencje.alebank.pl/wp-content/uploads/ 2015/07/ prezentacja. artur_.kubiak.pdf*, (data dostępu: 20.03.2016).
10. Kulesza E. (2006), *Kilka uwag o przetwarzaniu danych osobowych pracowników przez pracodawcę – regulacje obowiązujące i uwagi de lege ferenda*, W: *Ochrona danych osobowych wczoraj, dziś, jutro*, Red. Biuro GIODO- materiały zebrane, Warszawa 2006 r.
11. Ministerstwo Administracji i Cyfryzacji, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej*, Warszawa 2013r.
12. Rada Europy (RE) i Europejski Trybunał Praw Człowieka (ETPC), *Podręcznik europejskiego prawa o ochronie danych*, Luksemburg 2014.
13. Sokołowski M., *W 2014 r. ponad 22 tys. internetowych oszustw*, http://wiadomosci.onet.pl/kraj/w-2014-r-ponad-22-tys-internetowych-oszustw/xgr95na (data dostępu: 02.02.2016).
14. Tadeusiewicz R. (2002), *Społeczność Internetu. AOW EXIT,* Warszawa.
15. Tryboń M., Grabowska-Lepczak I., Kwiatkowski M. (2011), *Bezpieczeństwo człowieka w obliczu zagrożeń XXI wieku,* Zeszyty Naukowe SGSP, Nr 41, strony od-do.
16. *Polska Cyfrowa - Raport Polska 2030;* http://zds.kprm.gov.pl/ sites/default/ files/03_polska_cyfrowa_at.pdf; (data dostępu: 14.06.2015).
17. *rozporzadzenia/strategia_rozw_spol_inf_2007_2013.pdf*, (data dostępu: 15.02.2011).
18. *Słownik języka polskiego*, http://sjp.pwn.pl., (data dostępu: 01.03.2016).
19. *Słownik terminów z zakresu bezpieczeństwa narodowego*, (2008), AON, Warszawa.
20. Stańczyk J. (1996), *Współczesne pojmowanie bezpieczeństwa.* Instytut Studiów Politycznych PAN, Warszawa.
21. *Strategia rozwoju społeczeństwa informacyjnego w Polsce na lata 2007–2013*, Warszawa, 27 czerwca 2007,
http://www.unizeto.pl/upload_module/downloads/unizeto/ (data dostępu: 01.06.2015).
22. *Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*.
23. *Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych*, tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926 z późniejszymi zmianami.