Iwona Iskierka

Zapobieganie i zwalczanie zagrożeń za strony cyberprzestrzeni

Dydaktyka Informatyki 9, 82-90

2014

Iwona ISKIERKA

Politechnika Częstochowska

ZAPOBIEGANIE I ZWALCZANIE ZAGROŻEŃ ZE STRONY CYBERPRZESTRZENI

PREVENTION AND FIGHT AGAINST THREATS FROM CYBER SPACE

Słowa kluczowe: cyberzagrożenie, cyberatak
Keywords: cyber threats, cyber attack

Streszczenie

W pracy omówiono zagadnienia związane z ochroną przed cyberzagrożeniami. Zwrócono uwagę na wzrost cyberzagrożeń i konieczność skoordynowania działań w zakresie zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Ukazano działania zespołu CERT.GOV.PL, funkcjonującego w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW, które szczególnie uwzględniają ataki ukierunkowane na infrastrukturę obejmującą systemy i sieci teleinformatyczne. Wskazano na potrzebę cyberedukacji dla bezpieczeństwa.

Summary

The work discusses the issues related to the protection against cyber threats. Attention on the growth of cyber threats and the need to coordinate activities in the field of the prevention and control of risks on the part of cyberspace. Discusses the Team CERT.GOV.PL functioning within the framework of the Security Department of the ABW, which particularly include targeted attacks on infrastructure, including information and communication systems and networks. Indicated the need of education for cyber security.

Wstęp

Firma Kaspersky Lab opublikowała dokument zawierający przegląd zagrożeń internetowych, liczby incydentów naruszenia bezpieczeństwa dotyczących urządzeń mobilnych, ataków sieciowych oraz zagrożeń lokalnych w roku 2013[1]. Zwrócono uwagę, że w 2013 roku ogólny globalny poziom zagrożeń internetowych zwiększył się o 6,9 pkt proc. – w 2013 roku 41,6% komputerów zostało zaatakowanych co najmniej jeden raz. W celu przeprowadzenia wszystkich tych

[1] http://www.kaspersky.pl/about.html?s=news_reviews&cat=3&newsid=2166

ataków internetowych w 2013 r. cyberprzestępcy wykorzystali 10 604 273 unikatowe maszyny – o 60,5% więcej niż w 2012 roku. W 2013 roku miał miejsce dalszy wzrost liczby incydentów naruszenia bezpieczeństwa dotyczących urządzeń mobilnych, a wyrafinowanie i liczba tych zagrożeń osiągnęły nowy wysoki poziom. Głównym celem większości szkodliwych aplikacji mobilnych była kradzież pieniędzy, a następnie danych osobistych. Android nadal stanowi najpopularniejszy cel ataków, przyciągając aż 99,9% znanego szkodliwego oprogramowania. Kaspersky Lab jest jednym z najszybciej rozwijających się producentów rozwiązań bezpieczeństwa na świecie. Jest to międzynarodowa grupa działająca w prawie 200 krajach na świecie. Obecnie firma posiada ugruntowaną pozycję jednego z czterech wiodących na świecie producentów oprogramowania antywirusowego[2].

Ministerstwo Spraw Wewnętrznych udostępniło dokumentację związaną z „Rządowym Programem Ochrony Cyberprzestrzeni na lata 2011–2016". W załączniku czwartym umieszczono dokument: „Działanie Rządowego Zespołu Reagowania na Incydenty Komputerowe"[3]. Ze względu na potrzebę cyberedukacji dla bezpieczeństwa na uwagę zasługują: załącznik 10 „Prowadzenie społecznej kampanii edukacyjno-prewencyjnej w mediach publicznych" oraz załącznik 11 „Prowadzenie kampanii informacyjno-profilaktycznej na stronach internetowych". Bez edukacji nie będzie bezpieczeństwa w sieci, dlatego do szkół kierowanych jest większość projektów poświęconych tej tematyce. W partnerstwie z Fundacją Dzieci Niczyje oraz Fundacją „Kierowca Bezpieczny", Microsoft przygotował program bezpieczeństwa internetowego dzieci „3… 2… 1… Internet!". Kampania edukacyjna „3... 2... 1... Internet!" ma na celu nauczenie dzieci właściwych nawyków korzystania z technologii informacyjnych. Microsoft rozesłał do ponad 14 000 szkół podstawowych w Polsce oryginalne pakiety dydaktyczne z zakresu bezpieczeństwa internetowego dzieci. Jest to element zawartego we wrześniu 2009 roku porozumienia pomiędzy firmą Microsoft a Ministerstwem Edukacji Narodowej, w ramach programu „Partnerstwo dla Przyszłości". Materiały edukacyjne „3… 2… 1… Internet!", które nauczyciele mogą wykorzystywać podczas lekcji, zostały wspólnie opracowane przez Microsoft i Fundację Dzieci Niczyje, we współpracy z Fundacją „Kierowca Bezpieczny". Ambasadorem projektu jest Krzysztof Hołowczyc. W ramach projektu powstał serwis internetowy dla dzieci, www.321internet.pl, komiks oraz propozycja zajęć edukacyjnych przeznaczona do realizacji w szkołach podstawowych[4].

[2] http://www.kaspersky.pl/about.html
[3] http://bip.msw.gov.pl/portal/bip/6/19057
[4] www.321internet.pl

1. Najważniejsze incydenty dotyczące bezpieczeństwa w roku 2013 oraz prognozy bezpieczeństwa dotyczące roku 2014

Informacje dotyczące liczby cyberataków, zagrożeń mobilnych, aplikacji podatnych na ataki wykorzystywane przez cyberprzestępców, zagrożeń online obejmujących ataki poprzez strony WWW, zagrożeń lokalnych zostały zaprezentowane w raporcie Kaspersky Security Bulletin 2013. Podsumowanie 2013 r.[5] „Zgodnie z informacją" na powyższej stronie raport ten wchodzi w skład Kaspersky Security Bulletin 2013 i opiera się na danych uzyskanych i przetworzonych przy użyciu Kaspersky Security Network (KSN). KSN wprowadza technologie oparte na chmurze do produktów korporacyjnych oraz przeznaczonych dla użytkowników indywidualnych i stanowi jedną z najważniejszych innowacji firmy Kaspersky Lab. Statystyki prezentowane w raporcie oparte są na danych uzyskanych z produktów Kaspersky Lab zainstalowanych na komputerach użytkowników na całym świecie. Użytkownicy wyrazili zgodę na pozyskiwanie z ich komputerów informacji statystycznych na temat szkodliwej aktywności. W raporcie scharakteryzowano rok 2013 ze względu na liczbę cyberaktaków. W roku 2013 produkty Kaspersky Lab zneutralizowały 5 188 740 554 cyberataki na komputery użytkowników i urządzenia mobilne. W przypadku nowych modyfikacji szkodliwego oprogramowania na urządzenia mobilne wykryto ich 104 427, produkty Kaspersky Lab zneutralizowały 1 700 870 654 ataki zainicjowane z komputerów będących online na całym świecie, wykryto blisko 3 mld ataków wirusów na komputery użytkowników[6]. Z udaremnionych ataków łącznie 1,8 mln stanowiły szkodliwe i potencjalnie niechciane programy. W roku 2013 w dziedzinie mobilnego szkodliwego oprogramowania pojawił się szkodnik Obad, stanowiący prawdopodobnie najbardziej wszechstronne mobilne szkodliwe oprogramowanie spośród wykrytych do tej pory i obejmuje wiele rozmaitych metod i funkcji. Twórcy raportu zwracają uwagę na fakt, iż Obad jest dystrybuowany na wiele sposobów, w tym przez wstępnie ustawione botnety. Smartfony z systemem Android zainfekowane trojanem Opfake.a są używane do powielania i wysyłania wiadomości tekstowych zawierających złośliwe linki do każdego kontaktu na urządzeniu ofiary. Do ważnych wydarzeń dotyczących zagrożeń mobilnych w roku 2013 zalicza się: mobilny phishing, kradzież informacji dotyczących karty kredytowej przypisanej do mobilnego rachunku, mobilne trojany, które sprawdzają saldo na rachunku ofiary, co pomaga cyberprzestępcom w uzyskaniu jak największych zysków, wykorzystywanie mobilnych botnetów, używanie usługi Google Cloud Messaging (GCM) do kontroli urzą-

[5] http://securelist.pl/analysis/7256,kaspersky_security_bulletin_2013_podsumowanie_2013_r.html
[6] M. Zalewski, *Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW,* Gliwice 2012.

dzeń zombie podłączonych do botnetu, stosowanie plików z rozszerzeniem APK, dające możliwość szpiegowania danych osobowych na urządzeniach mobilnych ofiar i umożliwiając ich namierzenie.

Również firma Symantec opublikowała Raport Norton (dawniej Norton Cybercrime Report). Jest to jedno z największych badań dotyczących cyberprzestępczości dotykającej użytkowników indywidualnych na całym świecie. Raport Norton opiera się on na ankietach z udziałem ponad 13 000 dorosłych respondentów z 24 krajów[7]. Zawarto w nim informacje dotyczące polskich internautów. Według autorów raportu „w ciągu ostatnich 12 miesięcy 6 milionów Polaków padło ofiarą cyberprzestępców. tym czasie koszty związane z działalnością przestępców internetowych wyniosły w naszym kraju 6 miliardów złotych. Tylko 28% użytkowników używa podstawowych programów zabezpieczających na smartfonach, 50% użytkowników smartfonów nie kasuje maili od nieznanych nadawców, 21% polskich rodziców pozwala dzieciom korzystać ze swoich służbowych urządzeń, a w szczególności grać na nich, pobierać aplikacje oraz robić zakupy, a 31% Polaków dzieli się z innymi swoimi hasłami do mediów społecznościowych".

Raport zawierający prognozy dotyczące cyberbezpieczeństwa w 2014 roku „Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond" przedstawiła Trend Micro Incorporated (TYO: 4704, TSE: 4704), która jako światowy lider w dziedzinie oprogramowania i rozwiązań zabezpieczających dąży do zapewnienia bezpiecznego globalnego środowiska wymiany informacji cyfrowych[8]. Według Rika Fergusona, Global VP Security Research w Trend Micro: „Widzimy jak szybko wzrasta poziom zaawansowania cyberzagrożeń. Konsekwencje tego trendu odczują zarówno pojedynczy użytkownicy, jak i przedsiębiorstwa i instytucje rządowe. Zagrożenia czyhające na użytkowników mobilnej bankowości, ataki ukierunkowane, coraz większe zagrożenia wycelowane w prywatne dane oraz potencjalnie jedna poważna kradzież danych każdego miesiąca – wszystko to czeka nas w przyszłym roku. Będziemy też świadkami rozwoju trendu IoE, stanowiącego preludium do eksplozji przyszłych technologicznych przełomów, których możemy spodziewać się wraz z końcem tej dekady". W raporcie zawarto również prognozy na rok 2014 dotyczące działań cyberprzestępców. Dotyczą one wzrostu do 3 mln liczby złośliwych aplikacji oraz programów „wysokiego ryzyka" wymierzonych w system Android, bankowość online obsługiwana z poziomu urządzeń mobilnych będzie bardziej narażona na ataki typu „Man-in-the-Middle", co spowoduje, że dwustopniowy proces weryfikacji przestanie być wystarczającym zabezpieczeniem. Prognozy do-

[7] http://www.polskieradio.pl/111/1890/Artykul/951996,Raport-Norton-2013; http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[8] J. Petersen, *Cyberzagrożenia w 2014 wg Trend Micro*, http://www.polskieradio.pl/111/1890/ Artykul/1010793,Cyberzagrozenia-w-2014-wg-Trend-Micro

tyczą również metod wykorzystywanych przez cyberprzestępców. Cyberprzestępcy będą częściej korzystać z metod stosowanych podczas ataków ukierunkowanych, takich jak analizy oprogramowania open source oraz techniki spear phishing, doskonale dostosowane do danej sytuacji, urządzenia mobilne będą częstszym celem dla zaawansowanych zagrożeń, takich jak click jacking i ataki typu „watering hole". Według autorów raportu, w 2014 roku będziemy świadkami wzrostu tempa ataków ukierunkowanych. Autorzy podkreślają także wagę ataków na kluczowe elementy infrastruktury o znaczeniu strategicznym, nowe wyzwania związane ze sferą tzw. IoE (*Internet of Everything* – Internet wszystkiego) i Ukrytą Siecią – podziemiem Deep Web. Działania w zakresie poprawy bezpieczeństwa cyberprzestrzeni podejmuje Fundacja Bezpieczna Cyberprzestrzeń. Fundacja Bezpieczna Cyberprzestrzeń powstała w czerwcu 2010 roku, jej celem jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym działanie na rzecz poprawy bezpieczeństwa w sieci Internet. Fundacja ma swój udział w tworzeniu periodyka „CIIP focus" wydawanego przez Rządowe Centrum Bezpieczeństwa. W 2012 roku zainicjowała ona, współorganizowała i koordynowała pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE Polska 2012[9]. Fundacja opracowała własny raport dotyczący zagrożeń cyberprzestrzeni. Przygotowany raport na temat prognoz dotyczących zagrożeń teleinformatycznych w 2013 r. był najprawdopodobniej pierwszym tego typu raportem, na wyniki którego składały się głosy polskich specjalistów ds. bezpieczeństwa teleinformatycznego[10].

2. Rządowy Zespół Reagowania na Incydenty Komputerowe – działania w zakresie rozpoznawania, zapobiegania oraz zwalczania cyberzagrożeń

W dniu 1 lutego 2008 roku został powołany Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Zgodnie z dokumentem „Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku" wydanym przez Agencję Bezpieczeństwa Wewnętrznego, podstawowym zadaniem zespołu jest zapewnienie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty

[9] http://cybsecurity.org/pdfy/RaportCyber-EXE2012.pdf
[10] http://cybsecurity.org/pdfy/FBC_Predictions_RAPORT_2013.pdf

materialne, a także zakłócić funkcjonowanie państwa[11]. CERT.GOV.PL wykonuje testy bezpieczeństwa witryn dla administracji państwowej od 2008 roku[12]. Prowadzi program sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te mają na celu określenie poziomu bezpieczeństwa aplikacji WWW instytucji publicznych, a także usunięcie wykrytych nieprawidłowości. Instytucje, których witryny zostały przebadane, zostały poinformowane o wynikach audytu, wykrytych podatnościach istniejących w ich systemach i poinstruowane, jak podatności te usunąć. W 2012 roku przebadano 67 witryn należących do 33 instytucji państwowych. W 2012 roku w trakcie działania projektu skanowania witryn internetowych administracji publicznej wykryto ponad 1133 błędy. W 2012 roku, podobnie jak w latach poprzednich, odnotowana została znaczna liczba ataków typu website defacement. Ich wynikiem jest często podmiana zawartości strony głównej portalu, umieszczenie na serwerze strony phishingowej lub dodanie pliku do witryny. Pomimo prowadzonych przez zespół CERT.GOV.PL działań pro aktywnych takich jak testy bezpieczeństwa witryn oraz akcje uświadamiające, sektor polskiej administracji publicznej w dalszym ciągu jest podatny na tego typu ataki cybernetyczne. Użytkownik zainteresowany bezpieczeństwem teleinformatycznym może korzystać z informacji umieszczonych w witrynie[13]. Witryna jest źródłem specjalistycznych informacji związanych z bezpieczeństwem teleinformatycznym. Publikowane są tam m.in. aktualne informacje dotyczące istotnych zagrożeń, nowych podatności w popularnych systemach i aplikacjach, najczęstszych form ataków sieciowych oraz ochrony przed zagrożeniami. W zasobach witryny użytkownik znajdzie również biuletyny bezpieczeństwa udostępniane przez producentów sprzętu i oprogramowania.

W dniu 25 czerwca 2013 roku Komitet Stały Rady Ministrów przyjął dokument „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej”[14]. Zawarto w nim informacje dotyczące głównych przesłanek i założeń polityki ochrony cyberprzestrzeni RP, głównych działań związanych z bezpieczeństwem cyberprzestrzeni, procesem wdrożenia i mechanizmami realizacji zapisów dokumentu, finansowaniem oraz oceną skuteczności polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. W ramach realizacji Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej Rada Ministrów widzi potrzebę rozpoczęcia prac nad wdrożeniem działań edukacyjnych. Zakłada się, że działania z tego zakresu będą prowadzone wśród obecnych oraz przyszłych użytkowników Cyberprzestrzeni RP.

[11] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/605,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2012-roku.html

[12] E. Schetina, K. Green, J. Carlson, *Bezpieczeństwo w sieci*, Helion, Gliwice 2002.

[13] http://www.cert.gov.pl

[14] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej http://www.cert.gov.pl/cer/ publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html

3. Cyberedukacja dla bezpieczeństwa

W dokumencie „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" zostały przedstawione założenia dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa. Założenia te obejmują: szkolenia pełnomocników ds. bezpieczeństwa cyberprzestrzeni, wprowadzenie tematyki bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia na uczelniach wyższych, kształcenie kadry urzędniczej w administracji rządowej, prowadzenie kampanii społecznej o charakterze edukacyjno-prewencyjnym. Jednym z podstawowych aspektów zapewnienia bezpieczeństwa cyberprzestrzeni jest posiadanie wysoko wykwalifikowanych kadr w sektorze publicznym i prywatnym odpowiadających za utrzymanie systemów teleinformatycznych ze szczególnym uwzględnieniem zasobów kluczowych dla bezpieczeństwa państwa. W celu zapewnienia ciągłego dopływu odpowiednio wyszkolonych specjalistów z dziedziny bezpieczeństwa teleinformatycznego staje się konieczne zaangażowanie szkół wyższych w realizację tych założeń. Zakłada się, iż zagadnienia związane z bezpieczeństwem cyberprzestrzeni powinny stać się stałym elementem nauczania, a w szczególności powinno to dotyczyć uczelni technicznych kształcących informatyków. Zakłada się również uwzględnienie tematyki bezpieczeństwa teleinformatycznego wśród efektów kształcenia określonych w Krajowych Ramach Kwalifikacji dla Szkolnictwa Wyższego. Przedstawiono też założenia obejmujące przeprowadzenie kampanii społecznej o charakterze edukacyjno-prewencyjnym. Kampania społeczna adresowana do dzieci, młodzieży i ich rodziców w dużej mierze powinna być realizowana w placówkach oświatowych wszystkich szczebli. Przewiduje się również realizację kampanii za pośrednictwem środków masowego przekazu. Zwrócono uwagę na to, że powszechność korzystania przez obywateli z systemów dołączonych do sieci Internet oraz zwiększające się znaczenie dostępności usług oferowanych przez cyberprzestrzeń, wymuszają konieczność podnoszenia świadomości odnośnie do bezpiecznych metod korzystania z Internetu oraz uwrażliwienia obywateli na pojawiające się zagrożenia. Ważnymi elementami walki z cyberzagrożeniami są świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń. Podkreślono, że jedynie odpowiedzialne zachowanie wyedukowanego użytkownika może skutecznie minimalizować ryzyko wynikające z istniejących zagrożeń, we współczesnym świecie zapewnienie bezpieczeństwa teleinformatycznego w dużej mierze zależy od wiedzy i działań każdego użytkownika cyberprzestrzeni. Kampania społeczna o charakterze edukacyjno-prewencyjnym będzie miała charakter wielowymiarowy i w zależności od potrzeb jej adresatów nastąpi zróżnicowanie form i treści przekazu. Skierowana będzie do ogółu społeczeństwa, a w szczególności do: dzieci i młodzieży, rodziców oraz nauczycieli.

Jako grupę najbardziej podatną na wpływy i narażoną na zagrożenia z cyberprzestrzeni wskazano dzieci i młodzież. Celem wytworzenia nawyków, które uchronią młodych ludzi przed zagrożeniami czyhającymi na nich w sieci (np. przed zjawiskiem zwanym *cyberbullying* – przemocy w sieci, zawieraniem niebezpiecznych znajomości, niecenzuralnymi treściami, piractwem, uzależnieniem od Internetu) edukacja powinna rozpocząć się już od najmłodszych lat[15]. Wiedzę na temat zagrożeń z cyberprzestrzeni dziecko powinno uzyskiwać przede wszystkim w szkole na wszystkich poziomach edukacji (szkoła podstawowa, gimnazjum, szkoła ponadgimnazjalna). Kolejną grupą, do której adresowana będzie kampania, są rodzice. To rodzice są odpowiedzialni za przygotowanie dzieci do funkcjonowania w społeczeństwie w tym w społeczeństwie informacyjnym. Celem skutecznego nadzoru nad działalnością dziecka w Internecie rodzice powinni zdobyć odpowiednią wiedzę na temat zagrożeń z cyberprzestrzeni oraz metod ich eliminowania. Kampania społeczna adresowana jest również do nauczycieli. Podkreślono, że od roku 2004 kształcenie nauczycieli w ramach specjalizacji odbywa się zgodnie z Rozporządzeniem Ministra Edukacji Narodowej i Sportu, określającym standardy kształcenia nauczycieli [16]. W ramach zajęć obowiązkowych na studiach wyższych nauczyciele uzyskują podstawową wiedzę z zakresu technologii informacyjnych, w tym również bezpiecznego i świadomego korzystania z systemów teleinformatycznych. Założeniem jest, że w ramach kampanii społecznej informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach Polityki będą prezentowane na stronach internetowych Ministerstwa Administracji i Cyfryzacji oraz na stronie Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL. Należy także zwrócić szczególną uwagę na jedną z największych inicjatyw poświęconych bezpieczeństwu w sieci, jaką jest projekt „3… 2… 1 Internet!". Program „3... 2... 1... Internet!" jest jednym z działań w ramach inicjatywy Microsoft „Partnerstwo dla Przyszłości", który dedykowany jest polskiej edukacji i wspiera wszelkie innowacyjne inicjatywy przeciwdziałające zjawisku „wykluczenia cyfrowego" młodego pokolenia.

Zakończenie

Analizując przedstawione powyżej dokumenty należy pamiętać o skoordynowaniu działań z zakresu zapobiegania i zwalczania zagrożeń ze strony

[15] J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzież,* Kraków 2012.

[16] Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 7 września 2004 r. w sprawie standardów kształcenia nauczycieli (Dz.U. nr 207, poz. 2110).

cyberprzestrzeni. W dokumencie „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" zaprezentowano przewidywalne efekty polityki ochrony cyberprzestrzeni. Obejmują one spójną dla wszystkich zaangażowanych podmiotów politykę dotyczącą bezpieczeństwa cyberprzestrzeni, skuteczny system koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni oraz tymi, które dysponują zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa. Działania te zwiększą również świadomość obywateli, co do metod bezpiecznego użytkowania systemów dostępnych elektronicznie i sieci teleinformatycznych.

Bibliografia

Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzież,* Kraków 2012.

Schetina E., Green K., Carlson J., *Bezpieczeństwo w sieci,* Gliwice 2002.

Zalewski M., *Przewodnik po bezpieczeństwie nowoczesnych aplikacji WWW,* Gliwice 2012.

Netografia

http://www.kaspersky.pl/about.html?s=news_reviews&cat=3&newsid=2166

http://www.kaspersky.pl/about.html

http://bip.msw.gov.pl/portal/bip/6/19057

www.321internet.pl

http://securelist.pl/analysis/7256,kaspersky_security_bulletin_2013_podsumowanie_2013_r.html

http://www.polskieradio.pl/111/1890/Artykul/951996,Raport-Norton-2013; http://www.symantec.com/ about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

http://cybsecurity.org/pdfy/RaportCyber-EXE2012.pdf

http://cybsecurity.org/pdfy/FBC_Predictions_RAPORT_2013.pdf

http://www.cert.gov.pl