Ochrona danych,
Naruszenie bezpieczeństwa,
Zagrożenia w Internecie

Eugenia BUSŁOWSKA[1]
Agnieszka TRĘBICKA [2]
Romuald KOTOWSKI [3]

ZAGROŻENIA POCHODZĄCE Z INTERNETU I METODY OCHRONY PRZED NIMI

Wraz z upowszechnianiem się Internetu oraz przenoszeniem coraz większej liczby obszarów życia do sieci, rośnie znaczenie bezpieczeństwa. Bezpieczeństwo wszystkich działań w sieci zależy w bardzo dużym stopniu od świadomości występowania zagrożeń i dbałości o zabezpieczenie własnego komputera. W artykule przedstawione są aspekty bezpieczeństwa, typy zagrożeń w Internecie oraz metody ochrony.

THREATS FROM THE INTERNET AND METHODS OF PROTECTION

Along with the popularization of the internet and connecting more and more aspects of life with the network, importance of safety is increasing. The protection of all activities in the network depends very largely on the prevalence of risk and attention to secure personal computer. The article provides aspects of security, types of threats on the internet and methods of protection.

1. WSTĘP

Społeczeństwo XXI wieku oczekuje na możliwość łatwego dostępu do najnowszych osiągnięć z dziedziny informatyki i telekomunikacji. Żyjąc w społeczeństwie informacyjnym dążymy do uzyskania jak największej ilości informacji w jak najkrótszym czasie. Staje się oczywistym, że dostęp do informacji jest bezwzględnie konieczny do realizacji bardzo wielu zadań życia codziennego. Kto ma informacje ten ma władzę. Im bardziej wiarygodna informacja i im więcej jej jest - tym bardziej wzrastają szanse na podjęcie optymalnej decyzji. Mając informacje, a przynajmniej łatwy dostęp do niej, człowiek może podejmować racjonalne decyzje. Ma materiał do przeanalizowania. W dodatku może odpowiednio wcze-

[1] Politechnika Białostocka, Wydział Informatyki, 15-351 Białystok, ul. Wiejska 45A, Tel. 85-746-90-50, Fax: 85-746-90-57, e-mail: e.buslowska@pb.edu.pl,
Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży, Instytut Informatyki i Automatyki, 18-400 Łomża, ul. Akademicka 14, Tel. 86-215-59-53, Fax: 86-215-66-01, ebuslowska@pwsip.edu.pl
[2] Politechnika Białostocka, Wydział Budownictwa i Inżynierii Środowiska, 15-351 Białystok, ul. Wiejska 45A, Tel. 85-746-90-50, Fax: 085-746-90-57, e-mail: agusia@pb.edu.pl
[3] Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży, Instytut Informatyki i Automatyki, 18-400 Łomża, ul. Akademicka 14, Tel. 86-215-59-53, Fax: 86-215-66-01, rkotowski@pwsip.edu.pl

śnie podjąć działania zapobiegające powstaniu niechcianych pewnych sytuacji. Informacja stanowi jeden z najbardziej strategicznych zasobów gospodarczych, naukowych i kulturowych.

Informacje są gromadzone nie tylko w postaci ogromnych baz danych lub baz wiedzy, ale przede wszystkim są przetwarzane. Podlegają szczegółowym analizom badawczym prowadzonym przez kadry zarządzające przedsiębiorstwem. Tak, więc bezpieczne gromadzenie danych, z bezpiecznym do nich dostępem, jest nieodzownym elementem dla każdej funkcjonującej firmy i stanowi podstawę jej funkcjonowania. Firma posiadając zasoby danych musi zmierzyć się z problematyką ich zabezpieczenia przed niepowołanymi działaniami. Postępująca na naszych oczach integracja życia społeczeństwa informacyjnego z Internetem sprawia, że komunikowanie się poprzez sieć stało się standardem, a informacje za jego pośrednictwem krążą od nadawców do odbiorców. Wszyscy uczestnicy wymiany danych ufają, że otrzymane informacje są wiarygodne.

2. ŚWIADOMOŚĆ ZAGROŻEŃ

Główny Urząd Statystyczny w 2010 przeprowadzając badania dotyczące wykorzystania technologii informacyjno-telekomunikacyjnych wśród osób fizycznych, sprawdził również, jaki jest ich pogląd na temat bezpieczeństwa w Internecie. Pytano osoby korzystające z Internetu w ciągu ostatniego roku o to, czy obawiają się zagrożeń wynikających z jego użytkowania. W badaniach poruszono osiem obszarów, które opisują niebezpieczeństwa związane z wykorzystaniem Internetu:

- „zarażenie" komputera wirusem – gdzie wirus może sam się powielać i modyfikować. Może być on przenoszony również pomiędzy komputerami, np. za pomocą przenośnej pamięci USB;
- pojawienie się konia trojańskiego, który służy hakerom do zdalnego dostępu do komputera danego użytkownika. Za jego pomocą można wykradać dane, instalować niechciane (np. szpiegowskie) oprogramowanie czy też manipulować czynnościami wykonywanymi przez komputer;
- pojawienie się oprogramowania szpiegującego, którego zadaniem jest monitorowanie czynności i aktywności użytkownika danego komputera;
- pojawianie się SPAM-u (niechcianych e-maili) – ponieważ SPAM zawierać może różnorodne treści, nie przyjmuje się jednoznacznej jego definicji i ocenę tego, co nim jest a co nie, pozostawia się respondentowi. Dana treść uznana za ciekawą przez jedną osobę, przez drugą może być postrzegana, jako zbędna;
- nadużycie danych osobowych lub innych informacji osobistych przesyłanych przez Internet albo inne naruszenie prywatności, np. poprzez nadużycie prywatnych informacji, zdjęć, filmów itp. umieszczonych w serwisach społecznościowych (np. Nasza-klasa, Grono, Facebook);
- straty finansowe powstałe na skutek otrzymania oszukańczego e-maila (phishing) lub przekierowania do fałszywej strony internetowej (udającej np. stronę banku), gdzie niczego niepodejrzewające osoby same podają poufne dane, takie jak identyfikatory i hasła (pharming);
- wyłudzenie nienależnych płatności za pomocą przesłanego przez Internet numeru karty kredytowej lub debetowej;

- niebezpieczeństwo uzyskania dostępu przez dzieci do nieodpowiednich stron internetowych lub nawiązania kontaktu z potencjalnie groźnymi osobami [1].

Badania dowiodły, że wszystkie badane grupy najczęściej obawiają się zarażenia komputera wirusem lub innym złośliwym programem powodującym utratę danych lub narażającym na stratę czasu. Największą świadomość zagrożenia, podczas korzystania z Internetu, mają ludzie młodzi, w wieku od 16 do 34 lat, osoby z wykształceniem wyższym oraz uczniowie i studenci. Najmniejsze obawy wykazują osoby starsze, dla których dominujący wskaźnik spośród wszystkich wskazanych zagrożeń wynosił 7% oraz emeryci i inni bierni zawodowo - 18%. Osoby z najniższym wykształceniem najmniej się obawiają zagrożeń. Tylko niespełna jedna trzecia tych osób obawia się zagrożenia zarażeniem komputera wirusem lub innym złośliwym programem powodującym utratę danych lub narażającym na stratę czasu. Małe zróżnicowanie widać w układzie rozpatrywanym pod względem miejsca zamieszkania. I tak wskaźnik dla najczęściej wskazywanego zagrożenia wyniósł w miastach dużych 58%, w miastach mniejszych 50%, na obszarach wiejskich 39%." [1]

3. ASPEKTY OCHRONY

Zagadnienia związane z ochroną danych stanowią bardzo ważną i prężnie rozwijającą się gałąź informatyki. Wiedza na temat bezpieczeństwa jest nieodzowna w dobie Internetu. Kontakty z kontrahentami i klientami, zakupy i operacje bankowe toczą się w sieciowym świecie. Z badań przeprowadzonych przez Główny Urząd Statystyczny w kwietniu 2010 roku, aż 95,8% przedsiębiorstw w Polsce ma dostęp do Internetu. Badaniom poddano prawie 14 tys. przedsiębiorstw, w których liczba zatrudnionych przekraczała 10 osób. Wśród korzystających z Internetu, 84,7% wykorzystuje technologie online łączenia się z systemami bankowymi i zarządzania finansami. Także 28,2% badanych przedsiębiorstw używa komputera z dostępem do sieci w celach edukacyjnych czy też szkoleniowych. Pokazuje to spory postęp w świadomości zastosowań Internetu w biznesie, który do niedawna nie był aż tak wykorzystywany przez polskich internautów.

Globalna sieć WWW potrafi być bardzo niebezpieczna. Coraz częściej poufne dane przechowywane są w postaci elektronicznej, prężne przedsiębiorstwa i instytucje zdając sobie sprawę z zagrożeń płynących ze strony hakerów czy niedoskonałości używanego systemu, angażują firmy specjalizujące się w ochronie bezpieczeństwa danych. Bezpieczeństwo danych polega na ich ochronie, czyli zagwarantowaniu dostępu tylko uprawnionym użytkownikom i zabronienie dostępu nieuprawnionym. Zabezpieczenie przed przypadkowym lub umyślnym ujawnieniem, aktualizacją lub zniszczeniem [2]. Wyróżniane są cztery podstawowe aspekty bezpieczeństwa:

- poufność,
- integralność,
- dostępność,
- spójność.

Poufność danych jest rozumiana, jako brak dostępu do danych dla użytkowników oraz aplikacji, które nie są uprawnione do jej odczytywania. Klauzulę bezpieczeństwa w postaci: ściśle tajne, tajne, poufne nadaje się danym newralgicznym z punktu widzenia instytucji. Naruszenie ich poufności wiązałoby się z dużymi kosztami oraz z punku widzenia funkcjonowania instytucji bardzo ryzykowne [2, 3].

Integralność danych oznacza pewność, że dane nie zostały podmienione, zniekształcone lub zmodyfikowane bez wiedzy ich właściciela. Stan danych pozostaje zgodny ze stanem wymaganym i oczekiwanym przez adresata, do którego są przesyłane. Naruszenie integralności następuje przy nieupoważnionym dostępie, potknięciach i zaniedbaniach użytkowników uprawnionych, nieposiadających odpowiedniego przygotowania lub przeszkolenia. Mogą również być spowodowane awariami sprzętu, zakłóceniami transmisji, błędami w oprogramowaniu lub wirusami. W systemach informatycznych integralność danych powinna być zapewniona podczas przechowywania danych ich przetwarzania i przesyłania [2, 3].

Dostępność danych polega na stworzeniu możliwości ciągłego korzystania z danych dla wszystkich upoważnionych użytkowników. Dostępność danych może naruszyć nieupoważniony użytkownik lub upoważniony, przez nieświadome działania. Dostępność może być ograniczona również przez awarie, zakłócenia w transmisji, błędy oprogramowania oraz przeciążenia sieci. W systemach informatycznych główny nacisk kładzie się na zwiększenie dostępności infrastruktury informatycznej, co optymalizuje koszty [2, 3].

Spójność dotyczy danych gromadzonych w bazie danych. Wszelkie zmiany w bazie danych stanowią proces dyskretny. Wprowadzane, aktualizowane i usuwane informacje muszą spełniać warunki narzucone na dane podczas definicji bazy danych tak, by baza była zgodna z modelowaną rzeczywistością. W każdym momencie czasu baza danych znajduje się w pewnym stanie. Stan nazywamy spójnym, jeżeli wszystkie wartości, które zawiera baza danych w tym stanie mogą zaistnieć w świecie rzeczywistym. Warunki spójności mogą być dynamicznymi lub statycznymi. Warunki dynamiczne różnią się od statycznych tym, że pamiętają poprzedni stan. Zachodzenie warunków spójności zapewnia poprawność bazy danych. Naruszenie spójności danych następuje w wyniku semantycznie niepoprawnych operacji, niewłaściwej synchronizacji działania transakcji współbieżnych lub w wyniku awarii systemu [2, 3].

Przez bezpieczeństwo informacji należy rozumieć również zachowanie rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Rozliczalność polega na zapewnieniu, że określone działania użytkownika mogą być przypisane w sposób jednoznaczny tylko jemu. Inaczej mówiąc brana jest odpowiedzialność za wykorzystanie systemu informacyjnego.

Autentyczność dotyczy użytkowników, procesów, i informacji. Autentyczność polega na sprawdzaniu tożsamości podmiotów i prawdziwości zasobów.

Niezaprzeczalność oznacza brak możliwości zaprzeczenia swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

Niezawodność gwarantuje spójność danych i systemu oraz oczekiwane jego zachowanie i spodziewane wyniki [2, 3, 4].

4. KATEGORIE ZAGROŻEŃ W INTERNECIE

W sieci bezpieczeństwo użytkowników i wykonywanych operacji jest najważniejsze. Niestety, nieświadomość zagrożeń wpływa na podatność utraty cennych danych. Wszyscy zdajemy sobie sprawę, że użytkownicy są najsłabszym ogniwem jakichkolwiek zabezpieczeń. Często brak wiedzy, bezmyślność lub lenistwo może doprowadzić do naruszenia bezpieczeństwa. Internet, jako najbardziej popularne medium pozwalające na łatwą i szybką wymianę informacji, jest narażony na wiele form nieuczciwości i naruszenia bezpieczeństwa danych.

Zagrożenia w Internecie można podzielić na trzy główne kategorie:
- zagrożenia dla systemów i aplikacji webowych;
- zagrożenia dla prywatności;
- zagrożenia dla osób.

Rozwój mobilnych systemów operacyjnych pozwala na prostsze instalowanie zewnętrznych aplikacji, a co za tym idzie, pojawia się ryzyko infekcji szkodliwym oprogramowaniem. Systemy nieposiadające ścisłej kontroli aplikacji, np. Android firmy Google, narażone są na większe zagrożenie. System Android jest infekowany trojanem Trojan-SMS.AndroidOS.FakePlayer.b, który podszywa się pod odtwarzacz multimedialny. Strona z programem przekonuje użytkowników do instalacji obiecując obejrzenie filmu pornograficznego. Podczas instalacji użytkownik jest pytany o zgodę na wysyłanie wiadomości SMS, co jest niespotykane w przypadku odtwarzaczy multimedialnych i powinno wzbudzić podejrzenia. Po zainstalowaniu trojan wysyła wiadomości SMS na numery typu premium, a każda z nich obciąża konto użytkownika kwotą 6 dolarów. Ostatnio pojawiła się również aplikacja dostępna w serwisie Facebook, oferująca darmowe telefony iPhone, która wyrządziła już duże szkody [5].

Atakami skierowanymi przeciwko systemom są ataki typu odmowa usługi (ang. Denial of Service, DoS). Uniemożliwiają one dostarczanie usług swoim klientom i użytkownikom. Rozróżniamy ataki destrukcyjne oraz ataki obniżające sprawność systemu. Celem ataku destrukcyjnego jest całkowite odcięcie klientów od atakowanego serwisu. W przypadku ataków obniżających poziom konsumowana jest tylko pewna część zasobów ofiary.

Ataki DoS można również podzielić na skierowane przeciwko sieci oraz przeciwko systemom komputerowym. Ataki z pierwszej kategorii wykorzystują słabość ofiary wynikającą z ograniczonej przepustowości połączenia z Internetem. Łącza poszkodowanego są zalewane dużą ilością danych, przez co właściwa komunikacja zostaje bardzo utrudniona lub jest w ogóle niemożliwa.

W przypadku ataku skierowanego przeciwko systemowi, agresor może mieć na celu całkowite unieruchomienie serwera bądź też zablokowanie jednej z jego usług. Innym sposobem ataku na system komputerowy jest zajęcie jego zasobów. Ponieważ każdy komputer ma ograniczoną ilość zasobów potrzebnych do działania (pamięć operacyjną, moc obliczeniową procesora, przestrzeń dyskową itp.), atakujący może podjąć działania zmierzające do ich wyczerpania. Serwery WWW przestają udostępniać strony, serwery pocztowe nie odbierają i nie wysyłają wiadomości, a zablokowane rutery odcinają dostęp do Internetu.

Użytkownicy domowi oraz biurowi generalnie nie są zagrożeni, chociaż ich komputery mogą zostać wykorzystane do przeprowadzenia ataku. Do ofiar ataków DoS można zaliczyć także klientów zaatakowanych serwisów, którzy nie mogą korzystać z zablokowanych usług [6].

Aplikacje webowe (WWW) zyskują coraz większą popularność dzięki rozpoznawalnemu i powtarzalnemu interface'u użytkownika, wykorzystaniu hipertekstu, szybkości tworzenia nowych funkcjonalności, przenośności aplikacji pomiędzy platformami, centralne zarządzaniu aplikacją i możliwości użytkowania systemu z każdego miejsca w sieci**.** Zaletą aplikacji webowych jest działanie w Internecie lub w sieci lokalnej, przez co są narażone na niektóre zagrożenia [7].

Zwykle bezpieczeństwo aplikacji kojarzy się z ochroną przed bezpośrednimi atakami na dany system. Jako główne zagrożenia wymienia się: przejęcie, włamanie, kompromitacja

systemu, exploit. Trzeba jednak pamiętać o wielu innych możliwościach naruszenia bezpieczeństwa aplikacji. Na podkreślenie i uwagę zasługują następujące:
- zagrożenia wywołane nieprzewidywalną awarii sprzętu lub oprogramowania (np. awaria serwerów, problem roku 2000);
- błędy spowodowane czynnikiem ludzkim (np. pomyłki administratorów systemów);
- błędy proceduralne (np. nie wdrożenie procedury dostępu do kopii zapasowych danych przetwarzanych w aplikacji);
- kataklizmy (np. trzęsienia ziemi, zalanie serwerowni, ataki terrorystyczne) [8].

Zagrożeniem dla systemów i aplikacji są także aplikacje szpiegujące użytkowników pod pozorem wykonywania zupełnie innych zadań. Jak podaje firma F-Secure, program Tap Snake, będący odmianą znanej gry "wąż", okazał się aplikacją typu GPS Spy. Program przekazuje informacje o aktualnym miejscu pobytu użytkownika i jest aktywny nawet po wyłączeniu gry. Tap Snake jest programem komercyjnym i może być zakupiony i zainstalowany w telefonie osoby, którą chcemy śledzić. Pozwala na odtworzenie na mapie drogi, jaką przemierzyła szpiegowana osoba [9].

Podobnie jak oprogramowanie szpiegujące, funkcje śledzące może zawierać również oprogramowanie reklamowe. Do tej kategorii zaliczane są programy wyświetlające treści reklamowe, czyli aplikacje komputerowe utrzymujące się z reklam. Powodują one automatyczne otwieranie wyskakujących okienek zawierających reklamy lub zmianę strony głównej w przeglądarce internetowej. Jest ono zwykle dołączane do bezpłatnych programów, które umożliwiają autorom pokrycie kosztów tworzenia takich aplikacji. Oprogramowanie reklamowe samo w sobie nie jest niebezpieczne. Użytkowników zwykle bulwersują nachalnie wyświetlane reklamy [10].

Jeśli jesteśmy użytkownikami sieci przestajemy być anonimowi. Wykonywane przez nas czynności w większości przypadków pozostawiają ślady. Wysyłając wiadomość e-mail zachowana jest informacja o adresie IP komputera, z którego ją wysyłamy, odwiedzając strony internetowe serwery odczytują z jakiego IP łączymy się, itp. Obecne możliwości przeglądarek, takie jak: Cookies, ActiveX pozwalają na wyciągniecie poufnych danych o użytkowniku w postaci informacji o: nazwisku i imieniu, adresie e-mail, ostatnio odwiedzanych stronach i wyszukiwanych hasłach. Prywatność użytkowników jest również naruszana poprzez napływający spam, włamania do komputera czy programy śledzące działania użytkowników w sieci i wykradające poufne dane (spyware**)**. Zbieranie informacji na temat aktywności w sieci typu: zainteresowania, strony odwiedzane, pliki udostępniane pozwala na stworzenie profili zainteresowań. To może posłużyć do przesyłania nielegalnych treści, które mogą zainteresować użytkownika. Osobiste dane mogą być w wyniku ataku nawet modyfikowane, np. w wiadomości e-mail mogą być wprowadzone zmiany, może nastąpić kradzież pieniędzy z konta internetowego. Klienci organizacji finansowych są narażeni na atak z wykorzystanie trojana ZeuS. Do ataku wykorzystuje się tu phishing i elementy inżynierii socjalnej, ponieważ klient trafia na fałszywą stronę internetową sądząc, że jest na stronie swojego banku i podaje potrzebne dane. W ten sposób ZeuS mając login, hasło i możliwość odczytania kodu SMS-owego przesłanego na komórkę klienta, może dysponować kontem [11].

Do zagrożeń dla osób należą programy wymuszające zapłacenie okupu. Najczęściej za infekcje tego rodzaju programami odpowiadają serwisy erotyczne i pornograficzne. Użytkownik może być zachęcony do zainstalowania takiego programu lub też instalacja następuje poprzez luki w przeglądarce. Do najbardziej znanych tego typu programów należy

japoński wirus Kenzero. Po instalacji sprawdza historię stron przeglądanych przez użytkownika i jeśli użytkownik przeglądał serwisy pornograficzne, grozi opublikowaniem danych w Internecie. Żeby uniknąć publikacji proponowane jest opłacenie okupu w wysokości około 40 zł. Tego typu wirusy przede wszystkim infekowały komputery w Japonii. Obecnie doczekały się wspólnej nazwy – pornware [11].
W zagrożeniach dla osób fizycznych trzeba podkreślić również zagrożenia jakim podlegają korzystające z Internetu osoby nieletnie. Obecnie jednym z najnowszych zagrożeń są „Predators" – włamywacze do komputerów osób nieletnich, którzy mogą przejąć kontrolę nad kamerką internetową dziecka.

5. METODY OCHRONY PRZED ZAGROŻENIAMI

Większość firm wykorzystujących współczesne technologie teleinformatyczne do prowadzenia biznesu, stosuje mechanizmy zapewniające podstawowe bezpieczeństwo. Ze względu na występowanie różnych kategorii zagrożeń związanych z eksploatacją systemów informacyjnych muszą być podejmowane odpowiednie działania zabezpieczające. Ciągłe zmiany w pracujących systemach powodują, że pojedyncze zabezpieczenia nie są w stanie w pełni rozwiązać problemów bezpieczeństwa. Niezbędne jest wprowadzenie różnorodnych metod i narzędzi zabezpieczających. Zabezpieczenia sieci tylko za pomocą firewalli sieciowych okazują się niewystarczające. Aby skutecznie zapobiegać zagrożeniom poziomu systemu operacyjnego i aplikacji muszą być wprowadzone dodatkowe zabezpieczenia, przynajmniej w postaci oprogramowania antywirusowego. Należy pamiętać o ustawieniu automatycznej aktualizacji, np. Windows Update. Z systemu operacyjnego powinni korzystać tylko uprawnieni użytkownicy z bezpiecznym hasłem, inni użytkownicy powinni unikać pracy na koncie administratora. Dobrym rozwiązaniem jest zainstalowanie systemów wykrywania i blokowania włamań (IDS / IPS) i systemów antyspyware. Wysyłając pocztę należy korzystać z bezpiecznych i aktualizowanych klientów poczty e-mail. Dostęp do Internetu powinien mieć miejsce tylko z wykorzystaniem bezpiecznej i systematycznie aktualizowanej przeglądarki WWW. Można również korzystać z programów zapewniających kompleksową ochronę komputera oraz tożsamości użytkownika i plików.

Przechowywane w komputerze poufne dane należy chronić przed nieuprawnionym podglądaniem, wykradnięciem czy modyfikacją. Przy logowaniu do Internetu należy korzystać tylko z zabezpieczonych połączeń SSL[4] [12]. Można zastosować ochronę antywłamaniową przeciw próbom nieautoryzowanego dostępu do zasobów komputerowych, ochronę antywirusową przeciw napływowi złośliwego oprogramowania typu programy szpiegowskie, ochronę antyspamową przed napływem niepożądanych i szkodliwych treści. Przy korzystaniu z bankowości internetowej należy wybrać oferty banków zapewniających bezpieczne i silne uwierzytelnianie. Nie powinno się odbierać poczty e-mail od osób nieznanych, ani wiadomości na komunikatorach. Dbając o prywatność pamiętać trzeba o regularnym usuwaniu automatycznych zapisów w swoim komputerze, np. informacji o odwiedzanych stronach oraz innej aktywności w Internecie.

Ochrona przed zagrożeniami internetowymi dla osób fizycznych to przede wszystkim świadomość, że w sieci nie jesteśmy sami. Powinniśmy być świadomi zagrożeń i informować właściwe instytucje oraz służby o przypadkach cyberprzemocy. Jeśli dzieci korzystają

[4] SSL – ang. Secure Socket Layer

z Internetu powinno być zainstalowane oprogramowanie zapewniające kontrolę rodzicielską. Kontrola rodzicielska pozwala na monitorowanie działań dzieci w Internecie, aby można było chronić je przed zagrożeniami pochodzącymi z sieci.

6. WNIOSKI

Zagadnienia związane z bezpieczeństwem rozwijają się w dynamiczny sposób. Istnieje nieustająca potrzeba tworzenia nowych rozwiązań i eliminowaniu słabych punktów systemu operacyjnego lub aplikacji wykorzystujących sieć internetową. W sposób zdecydowany trzeba powiedzieć, że bezpieczeństwo to nieustający proces, który musi być ciągle udoskonalany.

Jak podają eksperci z zespołu CERT Polska, w 2010 r. otrzymali ponad 12 mln zgłoszeń automatycznych dotyczących polskich sieci. Do najważniejszych zagrożeń, którymi byli nękani internauci należą: infekcja ZeuSem, robak Stuxnet, ataki na telefonię internetową, złośliwe pliki PDF. Szczegółową analizę można znaleźć w raporcie zespołu CERT Polska [13]. Jest to bardzo pouczająca lektura i polecana dla osób i instytucji, które problem bezpieczeństwa w dalszym ciągu traktują marginalnie mimo coraz częściej zdarzających się złożonych ataków i możliwości ochrony przed nimi [14].

7. BIBLIOGRAFIA

[1] http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_nts_spolecz_inform_w_polsce_2006-2010.pdf (z dnia 23.09.2011r).
[2] Stokłosa J., Bilski T., Pankowski T.: *Bezpieczeństwo danych w systemach informatycznych*, Warszawa, PWN 2001.
[3] Busłowska E.: *Narzędzia i technologie ochrony danych*, Logistyka nr 2. 2010.
[4] Pieprzyk J., Hardjono T., Seberry J.: *Teoria bezpieczeństwa systemów komputerowych*, Gliwice, Helion, 2005.
[5] http://www.pcworld.pl/artykuly/363638_4/10.zagrozen.czyhajacych.w.internecie.html.
[6] http://magazynt3.pl/Ataki-typu-DoS-Anatomia-zagrozenia-i-metody-obrony/ (z dnia 30.09.2011r).
[7] Renk R., Saganowski L., Holubowicz W.; Choras M.: *Intrusion Detection System Based on Matching Pursuit*, ITTI Ltd., Poznan Intelligent Networks and Intelligent Systems (ICINIS '08). First International Conference on Issue Date. Pages 213- 216, 2008.
[8] Sajdak M.: http://www.securitum.pl/baza-wiedzy/publikacje/audyt-bezpieczenstwa-aplikacji-www (z dnia 30.09.2011r).
[9] http://www.telix.pl/artykul/waz-atakuje-smartfony-na-platformie-android-3,36197.html (z dnia 29.09.2011r).
[10] http://www.esetnod32.com.pl/nod32/slowniczek/adware/3/ (z dnia 29.09.2011r).
[11] http://www.viruslist.pl/analysis.html?newsid=602 (z dnia 29.09.2011r).
[12] Schneier B.: *Kryptografia dla praktyków*, Warszawa, WNT, 1995.
[13] http://www.cert.pl/PDF/Raport_CP_2010.pdf (z dnia 30.09.2011r).
[14] Choraś M., Kozik R., Piotrowski R. Brzostek J., Hołubowicz W.: *Network Events Correlation for Federated Networks Protection System*, 4th European Conference, ServiceWave 2011, Springer 2011, ISBN 978-3-642-24754-52011.