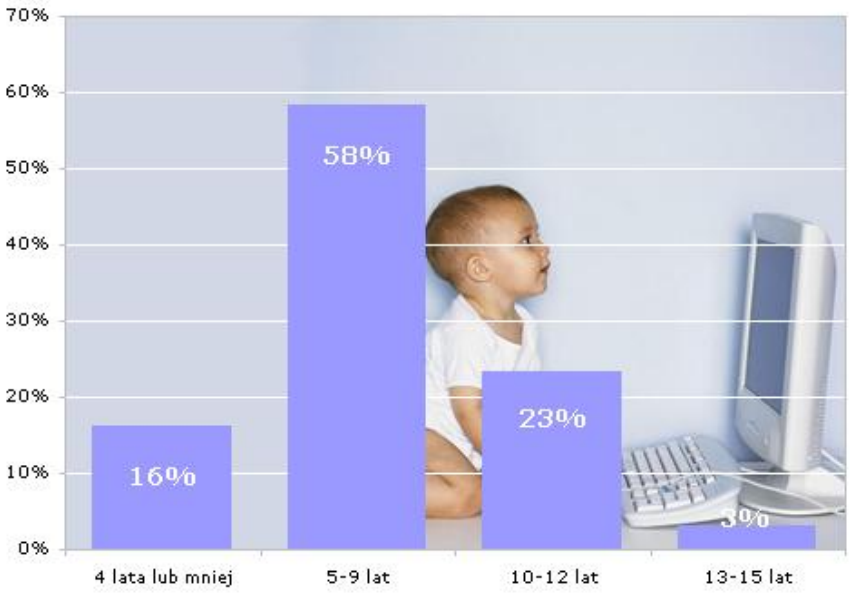
Wykorzystywanie Internetu przez dzieci i młodzież. Przeciwdziałania niebezpiecznym praktykom.

Do napisania tej t publikacji skłonił mnie udział w projekcie edukacyjnym „Bezpieczna szkoła" realizowanym przez firmę ArcaBit© oraz Fundację Dzieci Niczyje, którego celem jest edukacja pracowników oświaty w zakresie bezpieczeństwa dzieci i młodzieży w Internecie. Podczas opracowywania tego materiału, w dużej mierze korzystałam z materiałów pomocniczych otrzymanych podczas szkolenia oraz witryn: http://www.bezpiecznaszkola.com.pl/ i https://www.gemius.pl/. W niniejszym opracowaniu postaram się zwrócić szczególną uwagę na dwa zagadnienia: wykorzystywanie Internetu przez dzieci i młodzież oraz zagrożenia i sposoby zapobiegania i przeciwdziałania niebezpiecznym praktykom stosowanym przy wykorzystaniu sieci.

Historia Internetu zaczęła się 29 września 1969 roku, kiedy to na Uniwersytecie Kalifornijskim w Los Angeles (UCLA), a wkrótce potem w trzech następnych uniwersytetach zainstalowano w ramach eksperymentu pierwsze węzły sieci ARPANET – bezpośredniego przodka dzisiejszego Internetu. Eksperyment miał na celu zbadanie możliwość zbudowania sieci komputerowej bez wyróżnionego punktu centralnego, która mogłaby funkcjonować nawet pomimo uszkodzenia pewnej jej części. Wszystkie istniejące w tamtym czasie sieci zarządzane były przez jeden główny komputer, którego awaria pozbawiała możliwości pracy całą sieć.

Obecnie Internet objął swym zasięgiem całą Ziemię a w Polsce dostęp do niego posiada prawie każdy obywatel. Według badań Eurobarometr© z grudnia 2011 roku, w naszym kraju z Internetu korzysta około 90% dzieci w wieku od 6 do 17 lat. Większość z nich zaczyna korzystać z sieci będąc w wieku od 5 do 9 lat (58%), a co szóste z nich swoją przygodę z Internetem rozpoczyna jeszcze przed skończeniem 5-go roku życia (16,1%).[1]

[1] http://pliki.gemius.pl/Komunikaty/2008/2008_03_19_Gemius_SA_Dzieci_online



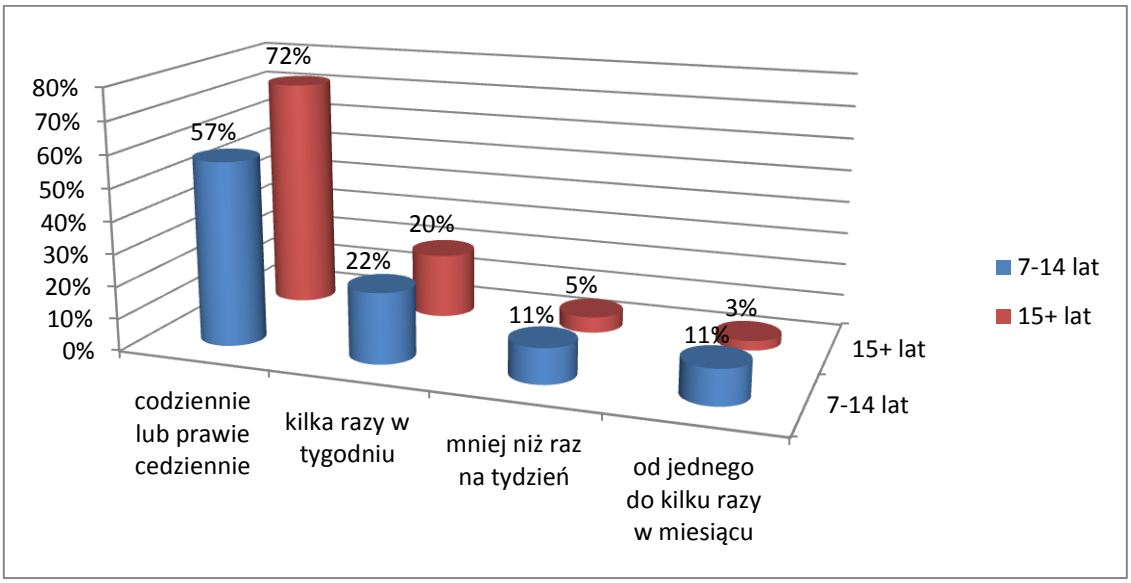
Rysunek 1. Wiek, w którym dziecko zaczęło korzystać z Internetu.

Aby skutecznie zadbać o bezpieczeństwo należy na początek zdać sobie sprawę z realności zagrożenia. Nie jest tajemnicą, że obecnie dzieci spędzają większość czasu przed komputerem. Nawet odrabianie lekcji, pisanie wypracować nader często polega na przeszukiwaniu sieci, wyszukiwaniu potrzebnych materiałów i niestety plagiatctwie. Niestety, dzieci o wiele sprawniej poruszają się w cyberprzestrzeni niż ich rodzice oraz posiadają większą wiedzę na temat rozwiązań informatycznych. Jest to zrozumiałe, ponieważ obecnie w szkołach realizuje się program nauczania technologii informatycznej. W latach szkolnych rodziców, kalkulator był szczytem osiągnięć informatycznych. Jest to podstawowa przyczyna braku skutecznego stosowania ochrony własnych dzieci przed zagrożeniami występującymi w Internecie.

Ostatnie, niestety nieliczne i przestarzałe badania pokazują, że wśród użytkowników w wieku 7-15 lat:

- Ponad połowa dzieci korzysta z Internetu codziennie lub prawie codziennie (57%). Co trzecie dziecko (33%) korzysta z Internetu raz na tydzień lub częściej.
- Dziewczynki spędzają w Internecie więcej czasu niż chłopcy. Średnio miesięcznie dziewczynki w wieku 7-15 lat (42,3% osób biorących udział w badaniu) surfują 31 godz. 43 min, a chłopcy (57,7% badanych) 30 godzin 22 min.
- Największą popularnością wśród dzieci cieszą się witryny z kategorii „Kultura i rozrywka” – średnio spędzają w serwisach tego typu 12 godz. 24 min miesięcznie. Kolejne kategorie tematyczne witryn odwiedzanych przez dzieci najczęściej to: „Wyszukiwarki i katalogi” (5 godz. 24 min) „Społeczności” (4 godz. 38 min) oraz witryny „Firmowe” (1 godz. 51 min).

- Co czwarte dziecko zagląda do serwisów erotycznych (25,67%). Miesięcznie dzieci spędzają na eksplorowaniu serwisów erotycznych średnio blisko półtorej godziny (1 godz. 28 min).
- 14% dzieci zagląda na strony związane z zakładami bukmacherskimi i kasynami internetowymi.
- Z serwisów randkowych korzysta 9% dzieci[2].



Rysunek 2. Częstość korzystania z Internetu.

Jak wynika z powyższego wykresu, codzienne korzystanie z Internetu przez dzieci powyżej 15-go roku życia jest nawet o 15% częstsze. Prezentowane dane zostały opracowane na podstawie badań przeprowadzonych w 2010 i 2011 roku. Wynika z nich, że dzieci w Internecie spędzały około jednej godziny dziennie, przy czym bardzo często bez kontroli rodzicielskiej. Obecnie, z pewną dozą prawdopodobieństwa można stwierdzić, że czas spędzony w sieci jest o wiele dłuższy, w większości trawiony na konsumpcję czyli przyjmowanie treści a nie na twórczą pracę i rozwój intelektualny poprzez generowanie nowych treści. Tę kategorię zagrożenia można zdefiniować jako **uzależnienie od Internetu**. Coraz większą popularnością wśród najmłodszych cieszą się też gry *online*, szczególnie sprzyjające uzależnieniu od Internetu. Sytuacja taka, często bagatelizowana przez dorosłych, powodować może poważne konsekwencje, jak wyobcowanie społeczne, problemy w nauce, czy problemy zdrowotne.

Jednak największym zagrożeniem występującym w Internecie jest treść informacji, jaka dociera do dzieci. Niestety, sieć wykorzystywana jest w dużej mierze

[2] http://www.google.pl/url?sa=t&rct=j&q=cz%C4%99sto%C5%9B%C4%87%20korzystania%20z%20internetu%20przez%20dzieci&source=web&cd=9&ved=0CFoQFjAI&url=http%3A%2F%2Fwww.bezpiecznaszkola.com.pl%2Ffolderbezpiecznaszkola.pdf&ei=B5umT4rLJuO90QWT_9jUCw&usg=AFQjCNEvlT7s8uFHbgw7ReVv6nWizLfQSg

przez środowiska pedofilskie w celach dystrybucji. Wymiany i produkcji treści o charakterze pornograficznym. Dużym odsetkiem tych treści są materiały i produkcje **pornografii dziecięcej**. Co roku ofiarami tego procederu na całym świecie padają tysiące dzieci, a do sieci trafiają niezliczone ilości materiałów pornograficznych z ich udziałem. Wraz z rozwojem serwisów komunikacyjnych problemem stało się również **uwodzenie dzieci** w Internecie, prowadzące często do wykorzystania seksualnego w rzeczywistym świecie. Dzieci coraz częściej wikłane są również w proceder **prostytucji** w sieci.

W ostatnim czasie poważną kwestią społeczną staje się również **przemoc,** której pewną odmianą jest **przemoc rówieśnicza** z użyciem mediów elektronicznych, określana mianem **cyberprzemocy**. Okazuje się, że tego typu przypadki to codzienność młodych ludzi - zjawisko wg różnych badań dotyczy od kilkunastu procent dzieci w Polsce do nawet 50%. Podstawowe formy tego zjawiska to:

- nękanie, straszenie, szantażowanie z użyciem sieci,
- publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci,
- podszywanie się w sieci pod kogoś wbrew jego woli.

Do działań tych wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne oraz serwisy SMS i MMS. W odróżnieniu od „tradycyjnej" przemocy zjawisko cyberprzemocy charakteryzuje wysoki poziom anonimowości sprawcy. Ponadto na znaczeniu traci przewaga fizyczna lub społeczna, a atutem sprawcy staje się biegłość w wykorzystywaniu możliwości niesionych przez media elektroniczne. Charakterystyczna dla tego problemu szybkość rozpowszechniania w sieci materiałów kierowanych przeciwko ofierze oraz ich powszechna dostępność sprawiają, że jest to zjawisko szczególnie niebezpieczne. Kompromitujące zdjęcia, filmy lub informacje mogą być w Internecie bardzo popularne i wielokrotnie powielane, a ich usunięcie jest często praktycznie niemożliwe. Pomimo tak dużego i narastającego problemu, polskie prawo nie zapewnia w pełni skutecznej ochrony. Wykorzystując istniejące regulacje prawne można w pewnym zakresie chronić małoletnie ofiary przemocy.

Inne zagrażające zjawisko, którego dzieci bywają zarówno ofiarami jak i sprawcami, to tzw. **cyberprzestępczość**, czyli przestępstwa związane z komputerem i Internetem ukierunkowane na systemy i dane komputerowe, takie jak: włamania do systemów komputerowych (hacking, cracking), nielegalne kopiowanie i rozpowszechnianie programów komputerowych (piractwo), nieuprawnione niszczenie danych komputerowych, itp. Należy podkreślić, że dzieci są bardzo często świadomymi lub nieświadomymi sprawcami przestępstw polegających na piractwie komputerowym. Najczęstszym przykładem tego typu przestępczości jest jednak kradzież tożsamości polegająca na gromadzeniu danych osobowych innej osoby w

celu podszywania się oraz uprawdopodobnienia np. podczas dokonywania zakupów internetowych na czyjeś konto, oczywiści bez płacenia rachunków.

Młodzi internauci często korzystają w sieci z narzędzi komunikacyjnych oraz serwisów społecznościowych za pomocą których zawierają w Internecie znajomości. Kontakty te mogą stanowić dla dzieci poważne zagrożenie, szczególnie w sytuacji kiedy prowadzą do spotkania w autentycznym świecie gdyż mogą być wykorzystane między innymi przez pedofili. Zjawisko uwodzenia dzieci online, określa terminem *child grooming*[3], dostrzeżone zostało już w latach dziewięćdziesiątych minionego stulecia, a skala problemu cały czas rośnie. Czasami udają rówieśnika potencjalnej ofiary, przynajmniej w pierwszym etapie relacji (psychomanipulacja). Jednak, wbrew stereotypowemu wyobrażeniu, przypadki takie należą do rzadkości, a sprawcy wykorzystywania seksualnego dzieci w kontaktach online najczęściej nie ukrywają przed dzieckiem ani swojego wieku, ani intencji, sprawnie manipulując ofiarą. Niestety, zdarza się, że kontakty seksualne pomiędzy nieletnim a dorosłym inicjowane są przez dziecko. Zjawisko kultu pieniądza oraz tendencja do społecznego wykluczania osób słabiej sytuowanych prowadzi młode osoby do chęci posiadania za wszelką cenę. Anonse młodych internautów wskazujące na gotowość do takiej relacji znaleźć można w serwisach randkowych czy czatowych (z informacją o oczekiwanej gratyfikacji). Należy podkreślić, że okoliczność taka w żadnym stopniu nie zwalnia sprawcy z moralnej i karnej odpowiedzialności za popełnione przestępstwo.

Odnotować także należy wykorzystywanie wspomnianych wcześniej serwisów do nakłaniania młodych internautów do wstępowania do rozmaitych sekt, organizacji subkultury a także do samobójstw. Tego typu działalność określana jest mianem *harmful content* i zawiera treści:

- materiały pornograficzne,
- materiały prezentujące przemoc,
- treści propagujące rasizm i ksenofobię,
- treści nawołujące do popełnienia przestępstwa,
- treści promujące faszystowski lub inny totalitarny ustrój państwa,
- treści zachęcające do działań autodestrukcyjnych (prostytucji, używania narkotyków itp.).

Trudno jednak precyzyjnie oszacować skalę problemu, ponieważ wykrywalność tego typu przestępstw jest trudno wykrywalna szczególnie jeżeli dochodzi do nich za przyzwoleniem ofiary. Na podstawie badań socjologicznych przeprowadzonych w

[3] Działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później je seksualnie wykorzystać. Jest to także mechanizm używany, by nakłonić dziecko do prostytucji czy udziału w pornografii dziecięcej. Potocznie poprzez *child grooming* rozumie się uwodzenie dzieci przez Internet.

2010 roku szacuje się, że około 7% badanych zawarło w Internecie znajomość, w wyniku której próbowano wykorzystać ich do celów seksualnych[4].

Jak zadbać o bezpieczeństwo dzieci w Internecie wykorzystując odpowiednie oprogramowanie?

Przestrzeń wirtualna pod względem zagrożeń nie różni się od naszej zwykłej codzienności. Na każdym kroku czai się wiele zagrożeń, na które narażone są dzieci i młodzież. Internet na dobre stał się elementem codziennego aktywności życiowej. Często jest to narzędzie pracy, a w przypadku młodszych użytkowników znacznie częściej nauki i zabawy. Tyle, że zabawa ta niestety nie zawsze może być beztroska. Podłączony do Internetu komputer jest celem wielu zagrożeń, których nie można pozostawić samym sobie.

Codziennie powstaje mnóstwo szkodliwych kodów, którymi może zostać zainfekowane oprogramowanie naszego komputera w celu spamowania, uszkadzania systemu operacyjnego, niszczenia plików, kradzieży danych itp. Należą do nich:

wirusy komputerowe

Program powielający się bez zgody i wiedzy użytkownika. Jego funkcjonowanie na komputerze może przynosić różnego rodzaju niepowołane działania o różnej szkodliwości, jak spowalnianie pracy systemu, wyświetlanie różnych okienek, bądź usuwanie plików. Potocznie często mówi się wirusy na wszystkie rodzaje szkodliwego oprogramowania.

konie trojańskie (trojany)

Najbardziej rozpowszechniony obecnie rodzaj złośliwego oprogramowania. Trojany przemycają do komputera różne funkcje, których użytkownik nie jest świadomy. Mogą one następnie prowadzić szkodliwą działalność jak rozsyłanie spamu.

programy szpiegujące (spyware)

Oprogramowanie mające na celu szpiegowanie aktywności użytkownika, może wykradać ważne

robaki

Wyjątkowo złośliwy rodzaj szkodliwego oprogramowania. Często w sieci zdarzają się epidemie, w czasie trwania których zarażane są tysiące komputerów. Do infekcji robakami często dochodzi przez pocztę email, bądź porty USB obsługujące pamięci przenośne.

[4] „Wiktymizacja dzieci i młodzieży w Polsce" Gemius S.A., FDN, wrzesień 2009, badani: 15-18 lat - N=1000

rogueware

Fałszywe oprogramowanie antywirusowe, zamiast chronić komputer może prowadzić do infekcji innymi szkodliwymi programami. Dlatego warto instalować oprogramowanie zaufanych dostawców.

phishing

Coraz bardziej popularne zjawisko wyłudzania ważnych danych. Próby wyłudzeń mają miejsce poprzez spreparowane, fałszywe strony internetowe, na które kierowany jest użytkownik, aby podać dane, jak np. login i hasło.

W trosce o zapewnienie bezpieczeństwa dzieci w Internecie opiekunowie mogą wspomagać się rozwiązaniami technologicznymi. Mowa tutaj o filtrach, monitoringu aktywności i regulacji czasu dostępu do komputera. Najczęściej takie mechanizmy są elementem pakietu zabezpieczającego komputer i należy je odpowiednio skonfigurować, aby mogły pełnić swoją funkcję. Pakiety takie dostępne są na rynku i w zależności od ich skuteczności i zakresu działania, ceny wahają się od całkowicie darmowych do kilkuset złotych za roczną licencję. W zależności od wybranego pakietu, moduły kontroli rodzicielskiej najczęściej oferują następujące funkcje:

Przeglądanie stron Internetowych

Filtrowanie treści

Moduł ten ma za zadanie ochronę dzieci przed nieodpowiednią zawartością stron internetowych. Pozwala w wygodny sposób, za pomocą określonych reguł, określić do jakich treści użytkownik powinien mieć dostęp, a do jakich nie. Użytkownik może definiować treści za pomocą tzw. białych i czarnych list (spis konkretnych dopuszczanych i blokowanych adresów) oraz posiadających szeroki zakres słów kluczowych określających niedozwoloną tematykę, np. przemoc, narkotyki itd. Ponadto podczas każdej aktualizacji moduł wzbogacany jest o nowe, nieodpowiednie strony zdefiniowane przez laboratorium analityczne. Filtrowanie treści może być wykorzystywane nie tylko przez opiekunów, ale również przez wychowawców w ramach zajęć z edukacji informatycznej.

Harmonogramy dostępu

Jest to przejrzyste narzędzie pozwalające na prostym schemacie ustawić odpowiednie parametry dostępu do Internetu. Harmonogramy powinny pozwalać zarówno na określenie godzin dostępu do sieci, jak również do samego komputera, co pozwala sprawować dużą kontrolę nad aktywnością najmłodszych w wirtualnym świecie. Uzupełnieniem opisanych mechanizmów jest obserwowanie ruchów dziecka w Internecie, nie przeszkadzające w surfowaniu po wirtualnym świecie, ale powiadamiające w szybki sposób o niepowołanych zachowaniach. Nielimitowany dostęp do sieci może również niekorzystnie wpływać na rozwój dziecka. Marginalnym skutkiem może okazać się wtedy

uzależnienie od Internetu. Tutaj pomocne mogą okazać się harmonogramy dostępu, będące elementem pakietów zabezpieczających.

Monitor aktywności i powiadomienia

Moduł monitoruje ruchy dziecka w Internecie i w prostych komunikatach e-mail informuje rodzica o próbach wejścia na nieodpowiednie strony itp.

Pobieranie danych.

Podczas pobierania danych z Internetu może dojść również do infekcji szkodliwym kodem, co następnie może prowadzić do kradzieży danych. Warto wiedzieć, że dane pobieramy nie tylko podczas zapisywania dokumentów, programów, czy multimediów, ale również podczas zwykłego otwierania stron internetowych. Dzieci rzadko zwracają uwagę, czy dana strona jest podejrzana. Dlatego dobrze jest chronić komputer już z poziomu zapory sieciowej (firewall), która będzie nas ostrzegać przed niebezpiecznymi połączeniami oraz posiadać aktualne oprogramowanie antywirusowe chroniące system przed infekcją złośliwym oprogramowaniem.

Uzależnienia

Internet, to również problem uzależnienia. Z dostępnych badań wynika, że dzieci spędzają w sieci coraz więcej czasu. Przy tym, często pozbawione są kontroli rodzicielskiej. Coraz większą popularnością wśród najmłodszych cieszą się też gry *online*, szczególnie sprzyjające uzależnieniu od Internetu. Sytuacja taka, często bagatelizowana przez dorosłych, powodować może poważne konsekwencje, jak dezadaptacja społeczna, problemy w nauce, czy problemy zdrowotne.

Aspekty prawne

Prawo nie reguluje sytuacji uzależnienia w kontekście odpowiedzialności uzależnionego, o ile nie popełnił on przestępstwa. Przede wszystkim dziecku powinna być udzielona pomoc psychologiczna. Odpowiedzialni za dostarczenie tej pomocy są rodzice/opiekunowie prawni. Profesjonalista, który stwierdza, że dziecko jest uzależnione od Internetu, a rodzice ignorują problem i nie działają dla dobra dziecka, winien powiadomić o tym sąd rodzinny i nieletnich. Sąd może zobowiązać rodziców do działania w interesie dziecka.

Na koniec przypomnę Internetowy dekalog, którego przestrzeganie
może nie uchroni przed przestępstwem komputerowym,
ale na pewno utrudni sprawcy jego popełnienie:

1. Pamiętaj, że w Internecie nie wiesz z kim tak naprawdę rozmawiasz.
2. Nie przeglądaj stron oznaczonych ostrzeżeniami o nieodpowiedniej treści.

3. Nie podawaj danych osobowych na podejrzanych stronach.
4. Nie klikaj w podejrzane linki.
5. Pamiętaj swoje hasła i ich nie udostępniaj osobom trzecim.
6. Nie ignoruj ostrzeżeń zapory sieciowej.
7. Przestrzegaj ostrzeżeń programu antywirusowego.
8. Pobieraj tylko legalne pliki.
9. Nie udostępniaj dokumentów nie należących do Ciebie.
10. Pamiętaj o przestrzeganiu zasad dobrego wychowania kiedy surfujesz po Internecie.

PAMIĘTAJ!

TUTAJ UZYSKASZ POMOC!

Od 1 sierpnia 2013 godziny działania Helpline.org.pl zmieniły się z 11.00-17.00 na 12.00-18.00 . Dzięki temu linia 800 100 100 oraz czat są dostępne dłużej w godzinach popołudniowych.

Przydatne strony:
www.dzieckowsieci.pl
www.sieciaki.pl

Opracowanie:

mgr Ilona Wierzbicka