edukacja medialna

Korzyści i szkody z nadzorowania sieci

WIEDZA W PIGUŁCE

Internet wydaje się przestrzenią pełnej wolności tworzenia i zdobywania informacji. Często zapominamy o tym, że sieć nie mogłaby istnieć bez rzeszy opiekujących się nią osób. Ich działania nie ograniczają się tylko do takich oczywistych i widocznych działań, jak administrowanie forów czy dbanie o porządek na własnej stronie.

Monitorowanie sieci odbywa się również na wielką skalę. Nasze podróże po sieci pozostawiają po sobie ślady. Tropią je m.in. dostawcy usług internetowych. Przechowują oni informacje o działaniach w sieci swoich klientów co najmniej przez dwa lata! Takie bazy danych ułatwiają pracę poszukujących dowodów przestępstw policjantów. Mogą je przeszukiwać, jeśli prokuratura na to zezwoli.

Niemniej dane o działaniach internautów są zwykle zbierane w innych celach. Przede wszystkim — marketingowych. Być może zauważyłeś, że twoja historia przeglądania wpływa na spam wpadający do twojej skrzynki. Dzieje się tak dlatego, że internet jest jak system naczyń połączonych. Kiedy wejdziesz na stronę, na której wyświetlają się reklamy, serwis nimi zarządzający dostaje informację o twoich odwiedzinach. W tym serwisie wiadomo już, że interesuje cię treść danej strony. Jeśli reklamodawca pozyskał również twoje dane — może przesłać na maila reklamę, która prawdopodobnie cię zainteresuje.

Przed przepływem danych możemy bronić się poprzez instalację AdBlocka, NoScripta, FlashBlocka czy Cookie Monstera. Rozszerzenia te blokują niepożądane elementy stron. AdBlock nie tylko usunie denerwujące reklamy, lecz także ograniczy przepływ informacji o historii przeglądania.

Również wielu popularnych operatorów poczty elektronicznej wykorzystuje informacje internautów. Np. regulamin Gmaila zaznacza, że Google może niemal dowolnie dysponować listami swoich użytkowników. Niestety, choć wszyscy mamy prawo do tajemnicy korespondencji, trudno ją sobie zagwarantować w sieci. Google, tak jak wiele innych wyszukiwarek, wykorzystuje zbierane informacje, aby dostosowywać wyniki wyszukiwania do użytkownika. Dlatego też różnią się one w zależności od komputera.

W UE możliwości nadzoru sieci są mimo wszystko ograniczone. W innych krajach świata bywa stosowana państwowa cenzura internetu. Dzieje się tak np. w Chinach, gdzie zablokowanych jest m.in. wiele portali mediów z krajów demokratycznych.

POMYSŁ NA LEKCJĘ

Udział w grze **„Kto nas widzi w internecie"** uświadamia w uproszczony sposób, jak skomplikowane operacje kryją się za znalezieniem pożądanej informacji przez wyszukiwarkę internetową czy przez ile miejsc przechodzą wysłane przez nas e-maile i polecenia.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, że wiele podmiotów śledzi ruch internautów w sieci, zbierając o nich dane;
- znają pozytywne i negatywne strony nadzoru nad siecią — m.in. ułatwienie w wyszukiwaniu treści wobec ograniczania treści uznanych przez system za niepotrzebne;

- umieją ochronić się przed śledzeniem w internecie przy pomocy programów blokujących m.in. reklamy, ciasteczka, skrypty i pliki flash.

Przebieg zajęć

1.

Czas: 15 min
Forma: praca wgrupach
Pomoce: tablica i kreda lub papier dużego formatu i markery, kartki A4, wydruk **instrukcji do gry „Kto nas widzi w internecie"**

Poproś 8 osób o zgłoszenie się do udziału w grze. Rozdaj odpowiednie role gry z **instrukcji „Kto nas widzi w internecie"** i poleć przeczytanie instrukcji, wybranie sposobów i form ich realizacji (wybrane osoby mogą zaangażować innych do pomocy w przygotowaniu się do swojej roli). Miejscem „wyświatlania" treści w komputerze może być tablica lub papier dużego formatu. Maile i zapytania do wyszukiwarek mogą być pisane na mniejszych kartkach. Osoby symulujące „nieosobowe" działania, mogą zapisywać swoje „obserwacje" na kartkach.

2.

Czas: 20 min
Forma: gra
Pomoce: tablica i kreda lub papier dużego formatu i markery, kartki A4

Gdy wszyscy będą znali i rozumieli swoje role, a także przygotują się do ich wykonania, można zaczynać grę.

3.

Czas: 10 min
Forma: dyskusja
Pomoce: tablica i kreda lub papier dużego formatu i markery, kartki A4

Po wykonaniu poprzedniego ćwiczenia, każdy „nieosobowy" bohater gry pokazuje, jakie posiada dane o INTERNAUCIE. Zapytaj uczestników i uczestniczki, co ich zdziwiło albo zaskoczyło, czego nie byli świadomi. Przejdźcie jeszcze raz krok po kroku niezrozumiałe elementy gry, omawiając pokazane mechanizmy.

Zaznacz, że gra była bardzo uproszoną i przerysowaną symulacją działania internetu. W rzeczywistości komunikacja między serwerami, serwisami reklamowymi, tworzącymi statystyki i badającymi działania w internecie jest bardziej skomplikowana i zwielokrotniona.

Zapytaj uczestników i uczestniczki, jakie pozytywne i negatywne strony ma nadzór nad siecią. Czy wiedzą, w jaki sposób każdy może ograniczyć śledzenie w internecie przy pomocy rozszerzeń do przeglądarki blokujących m.in. ciasteczka, reklamy, skrypty i pliki flash? Zapisz najlepsze pomysły.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- mają świadomość, że wiele podmiotów śledzi ich ruch w sieci, zbierając o nich dane?
- znają pozytywne i negatywne strony nadzoru nad siecią?
- umieją ochronić się przed śledzeniem w internecie?

Opcje dodatkowe

Jeśli są do tego warunki (komputer połączony do internetu i rzutnik), można pokazać, gdzie różne strony internetowe wysyłają informacje o naszym wejściu na nie. Można skorzystać z wersji demonstracyjnej pod adresem http://www.mozilla.org/en-US/collusion/demo/ lub zainstalować rozszerzenie Collusion do przeglądarki Mozilla Firerox i oglądać reakcje dowolnych stron na żywo.

MATERIAŁY

Materiał pomocniczy „Kto nas widzi w internecie".

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Oznacz zdania jako prawdziwe lub fałszywe:

- Każdy jest śledzony w internecie. [rozwiązanie: prawda] [Prawda/Fałsz]
- Korzystanie z wyszukiwarki internetowej w każdym komputerze daje takie same rezultaty. [rozwiązanie: falsz] [Prawda/Fałsz]
- Zbieranie informacji o internautach zawsze oznacza złe intencje zbierającego. [rozwiązanie: falsz] [Prawda/Fałsz]
- Nie wiadomo, do jakich celów i przez kogo zostaną kiedyś użyte informacje zebrane na nasz temat. [rozwiązanie: prawda] [Prawda/Fałsz]

SŁOWNICZEK

- **AdBlock**: jedno z najpopularniejszych rozszerzeń do przeglądarek internetowych, automatycznie blokuje i usuwa reklamy ze stron internetowych. Zwiększa wygodę i bezpieczeństwo korzystania z sieci. Ogranicza przepływ informacji o historii przeglądania.
- **NoScript**: rozszerzenie do przeglądarek internetowych, automatycznie blokuje skrypty uruchamiane przez strony internetowe w przeglądarce.
- **FlashBlock**: rozszerzenie do przeglądarek internetowych domyślnie blokujące wszystkie filmiki typu flash na stronach internetowych, pozwalające je uruchomić jednym kliknięciem myszki.
- **CookieMonster**: rozszerzenie do przeglądarek internetowych, pozwala bardzo dokładnie kontrolować ciasteczka i to, jakie strony (i na jak długo) mogą je ustawiać.
- **cenzura internetu**: próby wprowadzenia odgórnego, kontrolowanego przez państwo, filtrowania treści w Internecie. W mniejszym lub większym stopniu wprowadzone w wielu krajach (Chiny, Iran, Włochy, Wielka Brytania).

- **ciasteczka**: (ang. cookie), małe pliki tekstowe zapisywane na dysku użytkownika podczas korzystania ze stron WWW, które zapamiętują określone informacje o ustawieniach przeglądarki (np. wybrany język strony WWW, dane logowania) lub przesyłają pewne informacje z powrotem na serwery danej strony (np. ustawienia zabezpieczeń lub produkty w koszyku w sklepie internetowym). Ciasteczka mogą narażać użytkownika na wiele zagrożeń, gdyż działają w sposób niewidoczny i mogą zapamiętywać wiele wrażliwych informacji. Nowelizacja prawa telekomunikacyjnego nałożyła na właścicieli stron WWW obowiązek zamieszczenia w widocznym miejscu informacji o tym, że witryna korzysta z ciasteczek, oraz wskazówek na temat tego, jak można wyłączyć ich obsługę.

- **cyfrowy ślad**: informacje na temat aktywności konkretnych osób w sieci, magazynowane na serwerach dostawców internetu i właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.

- **rozszerzenie**: (inaczej: wtyczka), dodatkowy moduł do programu komputerowego, który rozszerza jego możliwości. Stosowanie wtyczek jest coraz częstszym zabiegiem wśród twórców programów, a zwłaszcza tych tworzących otwarte oprogramowanie. Zaletą takiego rozwiązania jest to, że użytkownicy mogą wybierać pomiędzy funkcjami, które chcą mieć w programie, a których nie. Poza tym odciąża to autora od pisania całego kodu programu, a zrzuca część tego obowiązku na zewnętrznych programistów. Najpopularniejszymi programami oferującymi wtyczki są przeglądarki internetowe oraz programy pocztowe, np. Mozilla Firefox i Mozilla Thunderbird. W obu przypadkach dzięki wtyczkom można znacząco zwiększyć poziom bezpieczeństwa i prywatności komunikacji.

- **przeglądarka internetowa**: Program służący do pobierania i wyświetlania zawartości plików pobieranych z serwerów, czyli wyświetlania stron internetowych i plików multimedialnych. Współczesne przeglądarki mają możliwość komunikowania za pomocą wielu różnych protokołów, np. poczty e-mail, dzięki czemu mogą służyć rozbudowanym zadaniom. W systemie Windows domyślną przeglądarką jest Internet Explorer, w systemie Linuks najczęściej jest to Mozilla Firefox. Dodatkowo przeglądarki takie jak Mozilla Firefox, Opera oraz Chrome obsługują dodatkowe wtyczki, czyli małe programy rozbudowujące ich funkcjonalności, np. z zakresu bezpieczeństwa.

- **skrypt**: prosty program uruchamiany przez stronę internetową. Skrypty są zwykle używane do tworzenia animowanych menu i innych udogodnień, ale bywają też wykorzystywane do śledzenia internautów. Zdarza się, że zawierają złośliwy kod, który wykorzystuje luki w programie przeglądarki do infekowania komputerów użytkowników.

CZYTELNIA

- Prujszczyk Grzegorz, Śliwowski Kamil, **Browsing, wirtualne zagrożenia** [PDF], [dostęp: 22.11.2012], Dostępny w Internecie: http://www.ceo.org.pl/sites/default/files/library-files/browsing.pdf,licencja: CC-BY-NC-SA, s. 3–12.

Tekst: Urszula Dobrowolska, scenariusz: Jan Dąbkowski, konsultacja merytoryczna: Michał "rysiek" Woźniak. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/korzysci-i-szkody-z-nadzorowania-sieci/.

Publikacja zrealizowana w ramach projektu Cyfrowa Przyszłość, dofinansowanego ze środków Ministerstwa Kultury i Dziedzictwa Narodowego.

Podstawa programowa:

Informatyka, III poziom edukacyjny
Cele kształcenia
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Nowa podstawa programowa:

Wiedza o społeczeństwie, IV-VIII klasa
Treści nauczania
Uczeń przedstawia korzyści i zagrożenia wynikające z korzystania z zasobów internetu; rozpoznaje przemoc w cyberprzestrzeni i wyjaśnia, jak należy na nią reagować.

Informatyka, liceum i technikum
Treści nauczania
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.