edukacja medialna

Nadzór w sieci

WIEDZA W PIGUŁCE

Pewnie nieraz w internecie pokazał ci się baner reklamowy proponujący zakupy w sklepie niedawno przez ciebie odwiedzanym. To powszechne zjawisko jest efektem tzw. cyfrowego śladu, pozostawianego przez każdego użytkownika sieci. Składają się na niego nie tylko informacje świadomie przez nas udostępniane, lecz także przekazywane automatycznie (np. ciasteczka, informacje o adresie IP hosta odwiedzającego stronę itp.).

Bardzo często nie uświadamiamy sobie skali przepływu informacji o naszej aktywności w sieci. Wystarczy być zalogowanym do Facebooka lub do serwisów Google (np. Gmaila lub YouTube), aby historie naszych wyszukiwań i odwiedzanych stron z innych kart były udostępniane tym przedsiębiorstwom. Nie musisz nawet mieć otwartej strony Facebooka – wystarczy, że nie wylogowałeś się po ostatnich odwiedzinach.

Niektórzy w trosce o bezpieczeństwo informacji o sobie unikają portali społecznościowych. Zwykle jednak nawet i oni nie są zupełnie anonimowi dla Facebooka. Osoby korzystające z aplikacji Facebooka na smartfony udostępniają mu wszystkie swoje kontakty – numery telefonów i nazwiska swoich znajomych, w tym również tych, którzy nie mają konta na portalu.

Nigdy nie mamy pełnej kontroli nad informacjami, które udostępniliśmy – a często, gdy trafiają one w niepowołane ręce, prowokują do popełnienia przestępstwa. Na przykład o charakterze finansowym: niebacznie udostępniony numer dowodu wraz z naszym imieniem i nazwiskiem wystarczą, aby ktoś obciążył nas kredytem. Z drugiej strony łatwy dostęp do naszych danych może ułatwić wielokanałowy stalking. Umożliwia też przestępcom podszywanie się, które może służyć m.in. wyłudzaniu pieniędzy czy informacji o tobie od członka twojej rodziny.

Informacje o aktywności użytkowników w sieci mogą w mocy prawa być pozyskiwane przez instytucje państwowe. Zwykle służy to tropieniu cyberprzestępców. Często jednak masy informacji zagarniane przez oddziały śledcze dotyczą nie tylko przestępców, lecz także obejmują wielką ilość przypadkowych osób. Na przykład ABW ma prawo zażądać od administratora obserwowanej strony wszystkich treści oraz danych o użytkownikach czy listy adresów IP odwiedzających stronę. Może nawet uzyskać zdalny, bieżący dostęp do wszystkich aktywności dziejących się na niej. Zatem nawet jeśli nie jesteś internetowym przestępcą, możesz być obserwowany.

Pewnie zastanawiasz się, czy można jakoś zaradzić niekontrolowanemu przepływowi informacji o tobie? Podczas twojej sieciowej aktywności warto kierować się zasadą informacyjnego minimalizmu: im mniej możesz przekazać informacji, tym dla ciebie lepiej. Za każdym razem zastanów się, czy na pewno coś zyskasz, udostępniając kolejne zdjęcie czy materiał o sobie. Pomyśl, czy ktoś mógłby wykorzystać je jakoś wbrew twojej woli. Możesz również zrezygnować z wielu usług, które wymagają przekazywania zbyt wielu danych. Wybierz raczej podobne, ale o mniejszych wymaganiach. Rozważ również podawanie fikcyjnych danych, jeśli uważasz, że to uzasadnione.

SŁOWNICZEK

- **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.

- **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.
- **adres IP**: IP to protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych. Adres IP to liczba, która jest nadawana każdemu urządzeniu lub grupie urządzeń połączonych w sieci. Służy on ich identyfikacji. Jeden adres publiczny może być współdzielony przez wiele komputerów połączonych w podsieć. W takiej sytuacji każdy komputer w podsieci ma adres z puli adresów prywatnych. Większość komputerów korzysta z adresów IP przydzielanych dynamicznie, tylko w czasie podłączenia komputera do sieci. Po jego wyłączeniu dany adres IP może zostać przypisany innemu urządzeniu.
- **host**: dowolna maszyna (np. komputer), która posiada własny adres IP oraz uczestniczy w wymianie danych lub udostępnia usługi sieciowe poprzez sieć komputerową.

Tekst: Urszula Dobrowolska, scenariusz: Monika Prus-Głaszczka, konsultacja merytoryczna: Wojciech Klicki. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/nadzor-w-sieci/.

Publikacja zrealizowana w ramach projektu "Cybernauci - kompleksowy projekt kształtowania bezpiecznych zachowań w sieci", finansowanego ze środków Ministra Edukacji Narodowej.

Podstawa programowa:

Informatyka, IV poziom edukacyjny
Cele kształcenia
I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

Wiedza o społeczeństwie, IV poziom edukacyjny
Cele kształcenia
II. Rozpoznawanie i rozwiązywanie problemów.