edukacja medialna

Bezpieczna komunikacja w sieci

WIEDZA W PIGUŁCE

Internet daje poczucie anonimowości. Wielu z nas żywi przekonanie, że komunikację w sieci łatwo zachować w tajemnicy. To poczucie jest jednak złudne. Jeśli porównać Internet do poczty, to można powiedzieć, że większość komunikatów nie przypomina listów osłoniętych kopertą przed wzrokiem postronnych, lecz pocztówki, do których ma wgląd nie tylko nadawca i adresat, ale choćby listonosz czy pracownicy sortowni listów. W przypadku sieci odpowiednikiem pracowników poczty może być np. dostawca łącza internetowego czy administrator strony internetowej.

Jeżeli korzystasz z niezabezpieczonej sieci Wi-Fi (np. w restauracji czy innym miejscu publicznym) Twoje dane — łącznie z hasłami do usług internetowych — mogą zostać przechwycone przez niepowołaną osobę. Aby zwiększyć swoje bezpieczeństwo, staraj się nie korzystać z takich sieci — a jeśli to niezbędne, pamiętaj, aby nie robić wówczas rzeczy szczególnie wrażliwych (np. nie logować się do konta bankowego!).

Nawet jeśli korzystasz z zabezpieczonej sieci, to przy wymianie danych za pomocą podstawowego protokołu HTTP do informacji takich, jak adres IP (liczba nadawana urządzeniu lub grupie urządzeń połączonych w jednej sieci), loginy i hasła, pliki zamieszczane w udostępnianej przestrzeni, mają dostęp osoby trzecie: Twój dostawca łącza internetowego, dostawca łącza internetowego dla serwera przeglądanej strony, administratorzy węzłów pośrednich w sieci, przez które przechodzi Twoja komunikacja, oraz administrator samej strony. W przypadku podejrzenia naruszeń prawa administrator systemu dostawcy oraz administrator strony mają obowiązek udostępnić Twoje dane podmiotom odpowiedzialnym za egzekwowanie prawa, tj. policji, prokuraturze; a w niektórych wypadkach również osobom fizycznym.

Aby ograniczyć dostęp do treści naszej komunikacji wyłącznie do nadawcy i adresata, warto zastosować protokół HTTPS. Spotykasz się z nim, korzystając z poczty elektronicznej, bankowości internetowej czy portali społecznościowych. Staje się on coraz powszechniejszy i powinien być stosowany na wszystkich stronach wymagających logowania (w niektórych przeglądarkach przed adresem strony widnieje wówczas zielona kłódka). Warto zainstalować wtyczkę HTTPS Everywhere, która automatycznie włącza protokół HTTPS tam, gdzie jest to możliwe.

Istnieją różne sposoby na to, by chronić swoją komunikację w sieci przed postronnymi osobami. Podstawę stanowi dbałość o odpowiednie ustawienia prywatności w serwisach, z których korzystasz. Niektóre narzędzia wymagają większych kompetencji — należy do nich TOR: specjalne oprogramowanie, które pomaga ukryć lokalizację (adres IP) oraz zapewnić poufność komunikacji w sieci. Ponieważ bywa on wykorzystywany do celów przestępczych (np. do dystrybucji wizerunków seksualnego wykorzystywania dzieci, tzw. pornografii dziecięcej), niektórzy poddają go krytyce. Warto jednak pamiętać, że to bardzo ważne i przydatne narzędzie, używane m. in. przez opozycję polityczną w Iranie.

Inną metodą uniemożliwiającą osobom postronnym śledzenie naszej aktywności w sieci jest choćby szyfrowanie poczty (np. z wykorzystaniem PGP/GPG). PGP (**Pretty Good Privacy**) to zaawansowany system kryptograficzny, GPG (**GNU Privacy Guard**) to jego odpowiednik udostępniany na wolnej licencji GPL. Szyfrowanie poczty jest szczególnie istotne, jeśli chcemy drogą elektroniczną przekazać poufne informacje.

POMYSŁ NA LEKCJĘ

Uczestnicy i uczestniczki zajęć zapoznają się z podstawowymi informacjami dotyczącymi przepływu danych w sieci. Odgrywając kilka scenek, będą mieli okazję poznać różnice między przepływem danych przy użyciu protokołu HTTPS, w sieci TOR i w sieci niezabezpieczonej.

Cele operacyjne

Uczestnicy i uczestniczki:

- rozumieją, że dane przesyłane w sieci przechodzą przez wiele pośrednich urządzeń, które mogą mieć dostęp do ich treści i pozostają poza kontrolą użytkownika;
- rozumieją niebezpieczeństwa związane z logowaniem się do niezabezpieczonych sieci;
- wiedzą, że zachowanie prywatności i anonimowości w sieci jest bardzo trudne;
- potrafią podać przykłady narzędzi zwiększających bezpieczeństwo komunikacji w sieci;
- potrafią wyjaśnić korzyści, jakie daje HTTPS i TOR.

Pomysł na lekcję

1.

Czas: 5 min
Forma: rozmowa
Pomoce: Wiedza w pigułce

Korzystając z Wiedzy w pigułce, wprowadź uczestników i uczestniczki w temat zajęć — przedstaw metaforę Internetu jako poczty. Komunikat przesyłany w sieci można porównać do pocztówki, ale nie listu. Informacje, które wysyłamy, są dość łatwo dostępne dla innych. Powiedz, że na dzisiejszych zajęciach uczestnicy zapoznają się z funkcjonowaniem sieci i tym, jak informacje przepływają w sieci. Dowiedzą się, jakie informacje są dostępne w momencie logowania się do niezabezpieczonych sieci, do sieci TOR oraz przy wykorzystaniu protokołu HTTPS. Podczas ćwiczenia w grupie zobrazują przepływ informacji według 3 scenariuszy. Poproś uczestników i uczestniczki o zwrócenie uwagi, jakie korzyści użytkownikom daje logowanie się do sieci za pomocą HTTPS czy TOR.

2.

Czas: 30 min
Forma: praca wgrupach
Pomoce: nożyczki, **instrukcja dla grup „Działanie sieci"** i **materiał pomocniczy „Sieć"**

Podziel uczestników i uczestniczki na minimum 8-osobowe grupy. Każdej grupie rozdaj jedną **instrukcję dla grup „Działanie sieci"** i **materiał pomocniczy „Sieć"**. Poproś grupy o zapoznanie się z instrukcjami i wykonanie zadań. Monitoruj pracę grup i w razie potrzeby udziel wskazówek.

3.

Czas: 10 min
Forma: rozmowa

Zadaj uczestnikom i uczestniczkom pytanie:

1. Jakie dane ujawniamy, logując się do niezabezpieczonych sieci?
2. Jakie dane są o nas niedostępne, kiedy logujemy się do sieci z użyciem TOR i HTTPS?
3. Jakie korzyści daje HTTPS i TOR?

Podsumuj zwracając uwagę, że TOR jest narzędziem, które umożliwia działania internautów, np. w krajach, gdzie nie ma wolności słowa i gdzie aktywizm polityczny jest brutalnie tłumiony. Natomiast HTTPS jest narzędziem, które powinno być używane wszędzie, gdzie mamy do czynienia z logowaniem, na przykład w bankowości internetowej i sklepach internetowych.

Ewaluacja

Czy uczestnicy i uczestniczki po przeprowadzonych zajęciach:

- rozumieją mechanizm przepływu danych w sieci?
- rozumieją niebezpieczeństwa związane z logowaniem się do niezabezpieczonych sieci?
- wiedzą, że zachowanie prywatności i anonimowości w sieci jest bardzo trudne?
- potrafią podać przykłady narzędzi zwiększających bezpieczeństwo komunikacji w sieci?
- potrafią wyjaśnić korzyści, jakie daje HTTPS i TOR?

Opcje dodatkowe

Ćwiczenie 3 możesz rozwinąć o stworzenie listy rzeczy, których dla własnego bezpieczeństwa nie powinno się robić w sieci, kiedy jesteśmy zalogowani do niezabezpieczonych sieci.

Ćwiczenie 2 możesz podsumować, korzystając z interaktywnej grafiki tłumaczącej działanie HTTPS i TOR: https://www.eff.org/pages/tor-and-https.

MATERIAŁY

Instrukcja dla grup „Działanie sieci"
Materiał pomocniczy dla grup „Sieć"

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Zaznacz prawidłową odpowiedź (może być więcej niż jedna).

1. W przypadku logowania się w sieci bez użycia HTTPS, dostawca Internetu użytkownika zna:
   - ☑ numer IP użytkownika
   - ☑ dane, które użytkownik przesyła i odbiera
   - ☑ adresy stron, które odwiedza
   - ☑ loginy i hasła, z których korzysta

2. W przypadku logowania się w sieci z użyciem HTTPS, dostawca Internetu użytkownika zna:

   ☑ numer IP użytkownika
   ☐ loginy i hasła użytkownika
   ☐ dane, które użytkownik przesyła i odbiera
   ☑ adresy stron, które użytkownik odwiedza

3. W przypadku logowania się w ramach sieci TOR, dostawca Internetu użytkownika zna:

   ☑ numer IP użytkownika
   ☐ loginy i hasła użytkownika
   ☐ dane, które użytkownik przesyła i odbiera
   ☐ adresy stron, które użytkownik odwiedza.

SŁOWNICZEK

- **Protokół HTTP**:
- **Protokół HTTPS**:
- **TOR**: (ang. The Onion Router), specjalne oprogramowanie, które pomaga ukryć lokalizację (adres IP) oraz zapewnić poufność komunikacji w sieci.
- **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.
- **anonimowość**: brak możliwości zidentyfikowania osoby.
- **połączenie https://**: połączenie przeglądarki ze stroną internetową zapewniające szyfrowanie komunikacji, a tym samym znacznie utrudniające dostęp do treści osobom innym niż nadawca i odbiorca. Szyfrowanie niezbędne jest w bankowości elektronicznej i w innych sytuacjach, w których podajesz swoje prawdziwe dane. Korzystanie z połączenia https:// zaleca się każdorazowo przy logowaniu.
- **prywatność**: sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach (na przykład ze względu na bezpieczeństwo publiczne czy ochronę zdrowia).

CZYTELNIA

- Grzegorz Prujszczyk, Kamil Śliwowski, „**Komunikacja**" [dostęp: 13.06.2013]: `http://www.panoptykon.org/sites/panoptykon.org/files/panoptykon_poradnik_komunikacja.pdf`.
- Grzegorz Prujszczyk, Kamil Śliwowski, „**Bezpieczeństwo informacyjne w serwisach web 2.0**" [dostęp: 13.06.2013]: http://www.panoptykon.org/biblioteka/bezpieczenstwo-informacyjne-w-serwisach-web-20.
- **TOR and HTTPS**, EFF [dostęp: 13.06.2013]: https://www.eff.org/pages/tor-and-https.

Tekst: Urszula Dobrzańska, scenariusz: Weronika Paszewska, konsultacja merytoryczna: Wojciech Budzisz, Michał "rysiek" Woźniak, Kamil Śliwowski. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

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

Publikacja zrealizowana w ramach projektu „Świadomie i bezpiecznie w świecie mediów i informacji".

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.
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.
Treści nauczania
Bezpieczne posługiwanie się komputerem, jego oprogramowaniem i korzystanie z sieci komputerowej.
Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania zainteresowań, opisywanie zastosowań informatyki, ocena zagrożeń i ograniczeń, aspekty społeczne rozwoju i zastosowań informatyki.

Wiedza o społeczeństwie, IV poziom edukacyjny
Cele kształcenia
IV. Znajomość zasad i procedur demokracji.
Treści nauczania
Bezpieczeństwo.

Nowa podstawa programowa:

Informatyka, liceum i technikum
Treści nauczania
zapoznaje się z możliwościami nowych urządzeń cyfrowych i towarzyszącego im oprogramowania.
objaśnia funkcje innych niż komputer urządzeń cyfrowych i korzysta z ich możliwości.
rozwiązuje problemy korzystając z różnych systemów operacyjnych.
charakteryzuje sieć internet, jej ogólną budowę i usługi, opisuje podstawowe topologie sieci komputerowej, przedstawia i porównuje zasady działania i funkcjonowania sieci komputerowej typu klient-serwer, peer-to-peer, opisuje sposoby identyfikowania komputerów w sieci.
postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad.
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.

Wychowanie do życia w rodzinie, liceum i technikum
Treści nauczania
rozumie, na czym polega prawo człowieka do intymności i ochrona tego prawa.