edukacja medialna

Złośliwe oprogramowanie

WIEDZA W PIGUŁCE

Przy korzystaniu z komputerów często zapominamy o ich bezpieczeństwie. W ten sposób narażamy je na zainfekowanie złośliwym oprogramowaniem. Wykorzystuje ono niedopatrzenia twórców aplikacji i systemów operacyjnych, z których korzystamy – po to, aby umożliwiać działania niezgodne z naszą wolą.

Pojęcie „**złośliwego oprogramowania**" obejmuje wiele programów o różnych metodach działania. Niektóre z nich mają na celu **przejęcie naszych danych**. Inne pozwalają na **obserwację działań wykonywanych w komputerze**, a nawet na przejęcie kontroli nad kamerą internetową. Złośliwe oprogramowanie **bywa wykorzystywane do wymuszenia pieniędzy** lub ich kradzieży, czego przykładami są oszustwa phishingowe czy tzw. ransomwear. Przy jego pomocy cyberprzestępcy szyfrują wszystkie pliki przechowywane na zainfekowanym dysku, a następnie żądają okupu za ich odszyfrowanie.

Pomimo różnorodności wirusów, **droga zakażenia komputera jest jednak zwykle taka sama – internet**, który zastąpił w tym dyskietki i inne nośniki danych. Mechanizm instalacji złośliwego oprogramowania może **ukrywać się w e-mailach lub ich załącznikach** × zwłaszcza tych w formacie PDF. Może też uruchomić się przy okazji **wgrywania programów, ściągniętych z niezaufanych źródeł**. Może wreszcie wykorzystywać luki przeglądarek internetowych i ich dodatków (np. wtyczki Flasha) × w tym wypadku instalacja wirusa rozpocznie się po **wejściu na podejrzaną stronę internetową**.

Ochronę przed atakiem cyberprzestępców zapewnia przestrzeganie kilku prostych zasad:

1. **Regularnie aktualizuj oprogramowanie.** Często naprawia to błędy, które mogły posłużyć do stworzenia wirusów.
2. Korzystaj z aktualnych, dobrych, starannie wybranych **programów antywirusowych.** Nie wyłączaj ich i nie ignoruj ich ostrzeżeń.
3. Instaluj tylko **programy pochodzące z zaufanych źródeł**. Uważaj, aby przy zgadzaniu się na kolejne etapy instalacji, nie zaakceptować nieświadomie czegoś niechcianego.
4. **Nie otwieraj podejrzanych e-maili**, a jeśli ci się to zdarzy, nie ściągaj na dysk i **nie otwieraj ich załączników**.
5. Im bardziej treść maila lub strony internetowej nakłania cię do podjęcia jakiś działań, tym dłużej zastanów się nad ich bezpieczeństwem.
6. **Nie instaluj przypadkowych rozszerzeń przeglądarek**.
7. Sprawdzaj zaufanie certyfikatów stron internetowych.

POMYSŁ NA LEKCJĘ

Na kilka dni przed zajęciami poproś, aby uczestnicy i uczestniczki założyli (nowe) konta mailowe. Zbierz adresy. Załóż własne, fikcyjne, nowe konto. W dniu, w którym odbywają się zajęcia, wyślij wszystkim mail z załącznikiem (**materiał pomocniczy A**). W temacie maila wpisz tytuł: Wiadomość od Poczty Polskiej, ważne. Na tej lekcji uczestnicy i uczestniczki dowiedzą się, w jaki sposób należy chronić komputer przed szkodliwym oprogramowaniem, poznają rodzaje takiego oprogramowania i typowe objawy tzw. infekcji.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, czym jest złośliwe oprogramowanie, komu i do czego może służyć;
- wiedzą, dlaczego należy się chronić przed działaniem złośliwego oprogramowania oraz wiedzą, jak to robić;
- umieją podać typowe przykłady działania złośliwego oprogramowania i typowe sposoby jego rozpowszechniania;
- wiedzą, że należy przed instalacją aplikacji zasięgnąć informacji, czy można ją uznać za godną zaufania (czy nie wykazuje cech złośliwego oprogramowania).

Przebieg zajęć

1.

Czas: 5 min
Forma:
Pomoce: komputery z dostępem do internetu, zielone i czerwone kartki

Poproś uczestników i uczestniczki, aby otworzyli skrzynki mailowe i znaleźli list od „Poczty Polskiej". Sami/same muszą podjąć decyzję, czy otworzyć list czy go wyrzucić. Pozostaw minutę na podjęcie decyzji (uczestnicy i uczestniczki nie otwierają listów, a jedynie podejmują decyzję). Następnie podnoszą kartki koloru zielonego, gdy podjęli decyzję o otwarciu listu, lub czerwonego, gdy zdecydowali się go wyrzucić bez otwierania. Poinformuj, że osoby, które nie otworzyłyby listu, postąpiły słusznie, bo list jest „podejrzany" i pochodzi z niewiarygodnego, nieznanego źródła. Podaj temat lekcji.

2.

Czas: 10 min
Forma: rozmowa
Pomoce: komputery z dostępem do internetu

Poinformuj, że list tak naprawdę nie jest niebezpieczny i został wysłany przez Ciebie. Poproś, aby wszyscy go otworzyli. Wraz z uczestnikami i uczestniczkami przeanalizuj załącznik i wskaż elementy „podejrzane". Zwróć uwagę na to, że:

- Poczta Polska nie wysyła swoim klientom podobnych wiadomości,
- kod podany w mailu jest dość „tajemniczy",
- nie ma takiego prawa w Polsce, aby Poczta ubiegała się o zapłatę za przechowywanie przesyłki w kwocie 50 zł – jest to element straszenia, zawoalowanej groźby,
- twórca tego maila z wirusem ukradł logo Poczty Polskiej, by mail wyglądał autentycznie,
- aby się „wypisać", też należy kliknąć link
- jest to tzw. banker – oprogramowanie do wykradania danych rachunkowości bankowej/internetowej i podmiany kopiowanych do schowka numerów rachunków.

Źródło: http://niebezpiecznik.pl/post/falszywe-maile-od-poczty-polskiej-zaszyfruja-ci-dysk/

3.

Czas: 15 min
Forma: mapa myśli
Pomoce: **materiał pomocniczy B**, tablica, kolorowe mazaki/kolorowa kreda

Rozdaj **materiał pomocniczy B** (podział wirusów ze względu na sposób działania) i poproś o przeczytanie tekstu. Następnie stwórz z uczestniczkami i uczestnikami mapę myśli (rysowaną na tablicy przez młodzież), której środkowym elementem będą słowa: złośliwe oprogramowanie, a kolejnymi „odnogami" rodzaje wirusów z ich charakterystyką. Pamiętaj, że młodzież może uatrakcyjnić mapę myśli jakimiś znakami graficznymi, może użyć kolorowych mazaków (kredy) itp.

4.

Czas: 5 min
Forma: instrukcja
Pomoce: **instrukcja dla nauczyciela**

Podaj prawdopodobne objawy infekcji komputera (**instrukcja dla nauczyciela A**).

5.

Czas: 10 min
Forma:
Pomoce: **instrukcja dla nauczyciela B**

Podsumowanie: Wspólne tworzenie „dekalogu" zasad: Jak chronić komputer przed wirusami? (**instrukcja dla nauczyciela B**) Uczestnicy i uczestniczki zapisują „dekalog" w zeszytach.

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- rozumieją, że instalowanie oprogramowania ochronnego jest dziś koniecznością?
- potrafią rozpoznać „niebezpieczne" wiadomości e-mail i wiedzą, że nie należy ich otwierać?
- znają rodzaje wirusów?
- znają objawy infekcji komputera?

Opcje dodatkowe

Jeśli masz więcej czasu, opowiedz o nieodpłatnym oprogramowaniu chroniącym przed działaniem złośliwego oprogramowania.

MATERIAŁY

- **materiał pomocniczy A**
- **materiał pomocniczy B**
- **instrukcja dla osoby prowadzącej A**
- **instrukcja dla osoby prowadzącej B**

ZADANIE DLA UCZNIA

Zadanie 1.

Oznacz zdania jako prawdę lub fałsz.

- Robaki to programy, które wykorzystują luki w systemach operacyjnych. [rozwiązanie: prawda] [Prawda/Fałsz]
- Robaki rozsyłają się za zgodą właściciela komputera. [rozwiązanie: falsz] [Prawda/Fałsz]
- Wirusy, jak nazwa wskazuje, infekują inne pliki. [rozwiązanie: prawda] [Prawda/Fałsz]
- Trojan to plik dołączony do „normalnego" programu. [rozwiązanie: prawda] [Prawda/Fałsz]
- Trojan zawsze zbiera poufne dane i wykorzystuje je przeciwko właścicielowi komputera. [rozwiązanie: prawda] [Prawda/Fałsz]
- Adware gromadzi dane. [rozwiązanie: prawda] [Prawda/Fałsz]
- Adware jest całkowicie nieszkodliwy. [rozwiązanie: falsz] [Prawda/Fałsz]
- Spyware jest szpiegiem. [rozwiązanie: prawda] [Prawda/Fałsz]
- Rootkity blokują działanie antywirusa. [rozwiązanie: prawda] [Prawda/Fałsz]

SŁOWNICZEK

- **złośliwe oprogramowanie**: wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera.
- **ransomware**: (ang. ransom – okup) – rodzaj oprogramowania używanego w przestępczości internetowej. Jego działanie polega na zaszyfrowaniu danych należących do użytkownika. Następnie program wymusza wyświetlenie notatki od przestępcy, informującej o tym, co musi zrobić właściciel plików, aby je odzyskać (zwykle chodzi o przelew określonej kwoty pieniędzy).
- **phishing**: (in. spoofing) wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przezpodszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne (np. Twój bank). Jest to rodzaj ataku opartego na inżynierii społecznej, tzn. wykorzystujący naszą nieuwagę, zaufanie do danej instytucji i często odruchowe działania.
- **certyfikat strony**: elektroniczny podpis strony internetowej, niezbędny do nawiązania połączenia https://.
- **program antywirusowy**: program komputerowy, którego celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.

CZYTELNIA

- **Złośliwe oprogramowanie udaje akta „afery podsłuchowej"** [online], [dostęp: 04.08.2015], dostępny w Internecie: http://www.cert.pl/news/10324/langswitch_lang/pl
- **Wieloetapowy phishing, który zaczyna się od prawdziwych odnośników: Marvin The Robot** [online], [dostęp 04.08.2015], dostępny w Internecie: https://plblog.kaspersky.com/wieloetapowy-phishing-ktory-zaczyna-sie-od-prawdziwych-odnosnikow/3038/
- **Makro wirus atakuje polskich klientów banku PKO BP**, [online], [dostęp: 04.08.2015], dostępne w Internecie: http://avlab.pl/aktualizacja-makro-wirus-atakuje-polskich-klientow-banku-pko-bp

Tekst: Urszula Dobrowolska, scenariusz: Małgorzata Bazan, konsultacja merytoryczna: Wojciech Budzisz. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/zlosliwe-oprogramowanie/.

Publikacja dofinansowana ze środków Ministerstwa Kultury i Dziedzictwa Narodowego

Podstawa programowa:

Informatyka: stosuje profilaktykę antywirusową

Nowa podstawa programowa:

Informatyka, VII-VIII klasa
Treści nauczania
Uczeń opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją.
Uczeń postępuje etycznie w pracy z informacjami.

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.