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.

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.

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

Udostępniono na licencji Creative Commons Uznanie autorstwa - Na tych samych warunkach 3.0.

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.