



## **KONSPEKT LEKCJI**

**Przedmiot: Technologia informacyjna**

**Temat: Wirusy komputerowe - profilaktyka antywirusowa.**

Prowadzący: Tomasz Kindryk

### **Cele lekcji:**

- Uczeń wie, co to jest wirus komputerowy,
- Uczeń zna rodzaje wirusów komputerowych,
- Uczeń wie, jakie zagrożenia niosą za sobą wirusy komputerowe,
- Uczeń zna profilaktykę antywirusową.

### **Metody pracy:**

- Elementy wykładu,
- ćwiczenia,
- praca indywidualna.

### **Pomoce dydaktyczne:**

- Zestawy komputerowe z systemem operacyjnym Windows z dostępem do internetu,
- Przeglądarka internetowa,
- Oprogramowanie antywirusowe.

### **Przebieg lekcji:**

1. Czynności organizacyjne: sprawdzenie obecności, podanie tematu lekcji, zalogowanie się do sieci komputerowej.

2. Omówienie pojęcia wirus komputerowy.

Wirus komputerowy – najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy w przeciwieństwie do robaka komputerowego do swojej działalności wymaga nosiciela w postaci programu komputerowego, poczty elektronicznej itp. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników.

3. Omówienie różnych rodzajów wirusów:

- Wirusy towarzyszące - wirusy te zwykle tworzone są w językach wysokiego poziomu. Wykorzystują hierarchię stosowaną przez system DOS, dotyczącą kolejności uruchamiania programów o tych samych nazwach a innych rozszerzeniach. Jeśli w jednym katalogu jest kilka programów o tej samej nazwie ale o różnych rozszerzeniach (EXE, COM, BAT), to w przypadku podania nazwy programu bez rozszerzenia, w pierwszej kolejności poszukiwany jest plik o rozszerzeniu COM, potem EXE, a na końcu BAT.
- Wirusy plików wsadowych - są to tzw. batchviruses, gdyż pliki wsadowe to pliki o rozszerzeniu BAT. Wirusy te wykorzystują do transportu właśnie pliki BAT. Potrafią wbrew pozorom być bardzo niebezpieczne i infekować również pliki COM oraz EXE, a nawet tablice partycji dysku. Po uruchomieniu zainfekowanego pliku wsadowego tworzony jest plik uruchamialny COM lub EXE, który zawiera właściwy kod infekujący pliki BAT. Plik BAT jest następnie kasowany, a plik wykonywalny jest uruchamiany.
- Makrowirusy - nie zarażają programów uruchamialnych lecz dokonują destrukcji dzięki wykonywaniu swojego kodu zapisanego w plikach dokumentów Microsoft Office (doc, xls). W programie Microsoft Word jest to język WordBasic, a w programie Microsoft Excel jest to Visual Basic for Applications. Są to wirusy bardzo łatwo wykrywalne, a ponadto ich działanie może zostać zablokowane przez macierzyste aplikacje. Od chwili, gdy aplikacje Microsoft Office ostrzegają o istnieniu makr, wirusy tego typu nie są bardzo groźne, nie powstają także nowe. Wirusy tego typu mogą działać w programach Microsoft Office w środowisku Macintosh,

pojawiały się jeszcze w pierwszych latach XXI wieku, ale nie były szczególnie groźne ani powszechne.

- Generatory wirusów - istnieje wiele programów umożliwiających stworzenie własnego wirusa, nawet bez znajomości systemu czy mechanizmów wykorzystywanych przez wirusy. Można je bez problemu znaleźć w Internecie. Korzystają one z gotowych modułów w assemblerze i umożliwiają stworzenie wirusa o zadanych parametrach wybieranych zwykle przy pomocy przyjaznego użytkownikowi menu. Można w nim określić zakres infekowanych obiektów oraz rodzaj efektów które ma on wywoływać. Oprócz kodu wynikowego wirusa, generatory tworzą także źródła w assemblerze, co umożliwia zainteresowanemu pisaniem wirusów użytkownikowi dokończanie się w tej dziedzinie.
- Robak - programy, których działanie polega na tworzeniu własnych duplikatów. Nie atakują one żadnych obiektów jak to czynią wirusy, a jedynie same się powielają. Oprócz zajmowania miejsca na dysku niekiedy wywołują również negatywne skutki uboczne. Robaki są najbardziej popularne w sieciach, gdzie mają do dyspozycji różne protokoły transmisji sieciowej dzięki którym mogą się rozprzestrzeniać.
- Koń trojański - to określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementują niepożądaną, ukrytą przed użytkownikiem funkcjonalność (spyware, bomby logiczne, itp.). Nazwa pochodzi od mitologicznego konia trojańskiego.
- Bomba logiczna - fragment kodu programu komputerowego (często wirusa zawartego w zwykłym programie lub robaka), umieszczony w nim bez wiedzy użytkownika. Przykładowe warunki zaktywizowania bomby logicznej:

4. Omówienie zasady działania programów antywirusowych.

5. Rodzaje programów antywirusowych:

- Programy komercyjne,
- Programy darmowe,
- Skanery online.

6. Ćwiczenia:

- Instalacja oprogramowania antywirusowego,
- Aktualizacja bazy wirusów.

7. Omówienie dostępnych funkcji w programach antywirusowych.

8. Wylogowanie i wyłączenie komputerów.

**źródła:**

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy](http://pl.wikipedia.org/wiki/Wirus_komputerowy)

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy#Wirusy\\_towarzysz.C4.85ce](http://pl.wikipedia.org/wiki/Wirus_komputerowy#Wirusy_towarzysz.C4.85ce)

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy#Wirusy\\_towarzysz.C4.85ce](http://pl.wikipedia.org/wiki/Wirus_komputerowy#Wirusy_towarzysz.C4.85ce)

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy#Makrowirusy](http://pl.wikipedia.org/wiki/Wirus_komputerowy#Makrowirusy)

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy#Inne\\_programy\\_o\\_dzia.C5.82aniu\\_destrukcyjnym](http://pl.wikipedia.org/wiki/Wirus_komputerowy#Inne_programy_o_dzia.C5.82aniu_destrukcyjnym)

[http://pl.wikipedia.org/wiki/Wirus\\_komputerowy#Generatory\\_wirus.C3.B3w](http://pl.wikipedia.org/wiki/Wirus_komputerowy#Generatory_wirus.C3.B3w)

[http://pl.wikipedia.org/wiki/Ko%C5%84\\_troja%C5%84ski\\_\(informatyka\)](http://pl.wikipedia.org/wiki/Ko%C5%84_troja%C5%84ski_(informatyka))

[http://pl.wikipedia.org/wiki/Bomba\\_logiczna](http://pl.wikipedia.org/wiki/Bomba_logiczna)