Technologia informacyjna

Prawa autorskie, ochrona i bezpieczeństwo danych

Prawa autorskie

- Oprogramowanie zabezpieczone jest szeregiem warunków; najważniejsze z nich to:
  - ograniczenie liczby kopii;
  - zakaz udostępnienia oprog. osobom trzecim.
- Umowa licencyjna w szczególności może określać możliwości w zakresie:
  - zwielokrotniania programu (w całości lub w części)
  - modyfikowania programu (tłumaczenie, przystosowywanie. itp.)
  - rozpowszechniania programu (sprzedaż, dzierżawa, najem, itp.)
- Korzystanie z produktów w ramach umowy licencyjnej, może dotyczyć:
  - jednej kopii oprogramowania;
  - oprogramowania towarzyszącego (OEM);
  - oprogramowania Open Source.

Umowa licencyjna

Umowa licencyjna jest umową formalno-prawną zawieraną pomiędzy firmą tworzącą programy, posiadającą prawa autorskie do oprogramowania a osobą fizyczną lub firmą, która używa tego oprogramowania.

Licencja to w odniesieniu do oprogramowania regulacja prawna określająca warunki jego użytkowania i zasady odpłatności. Praktykuje się kilka rodzajów licencji określających zakres użytkowania oprogramowania i warunki uiszczania za nie opłaty.

Typy licencji oprogramowania

- **Shareware –** oprogramowanie jest udostępniane nieodpłatnie do testów. Darmowa wersja posiada spore ograniczenia funkcjonalne i służy jedynie do wypróbowania danego programu przed podjęciem decyzji o zakupie jego pełnej, komercyjnej edycji;
- **Trial –** programy mogą być użytkowane w niepełnym zakresie przez ograniczony czas, po czym stają się nieaktywne. Po upływie czasu, użytkownik powinien usunąć program z dysku twardego lub dokonać zakup pełnej wersji aplikacji;
- **Freeware (tzw. wolne oprogramowanie) –** oprogramowanie może być użytkowane i rozpowszechniane za darmo, jednak bez udostępnienia kodu źródłowego. Zwykle nie trzeba dokonywać rejestracji. Nieodpłatne korzystanie z programów na licencji Freeware może być ograniczone tylko do indywidualnych użytkowników, czyli osób prywatnych, które nie czerpią korzyści finansowych wykorzystując darmowy program;

Typy licencji oprogramowania

- **Open Source (tzw. otwarte oprogramowanie) –** licencja, która (podobnie jak programy typu Freeware) umożliwia bezpłatne użytkowanie i rozpowszechnianie oprogramowania. Jednak, w odróżnieniu od Freeware, Open Source pozwala na kopiowanie i dowolne modyfikacje kodu źródłowego danej aplikacji. Dzięki temu powstaje niezawodne oprogramowanie, chętnie wykorzystywane przez użytkowników.

5

Typy licencji oprogramowania

- **GNU GPL (General Public Licence)** – licencja wolnego i otwartego oprogramowania, pozwalająca użytkownikowi na korzystanie z programu w dowolnym celu, modyfikowanie jego kodu źródłowego w celu lepszego spełnienia własnych potrzeb, a także rozpowszechniania własnych ulepszeń z pożytkiem dla ogółu. W tym ostatnim przypadku dopuszcza się również czerpanie korzyści finansowych z udostępniania samodzielnie zmodyfikowanej kopii;
- **Abandonware –** licencja dotycząca oprogramowania porzuconego przez jego twórcę. Autor aplikacji nie pobiera już za nią wynagrodzenia, przez co nie gwarantuje też dla niej wsparcia (np. w postaci udostępniania aktualizacji czy naprawy błędów).

6

Typy licencji oprogramowania

- **Donationware** - jest jednym z typów licencji Otherware. Oprogramowanie na tej licencji może być dowolnie modyfikowane, kopiowane i dystrybuowane pod warunkiem, że licencjobiorca zapłaci autorowi symboliczną kwotę. Wielkość opłaty zależy od licencjobiorcy.
- **Adware** – Adware jest oprogramowaniem (zamkniętym) rozpowszechnianym za darmo, ale zawierającym funkcję wyświetlającą reklamy.

Licencja użytkownika EULA

- **EULA** (ang. End User License Agreement) – licencja nakładająca dodatkowe ograniczenia na użytkownika oprogramowania, np.:
  - możliwość instalacji określonej liczby kopii,
  - czy ilość użytkowników mogących używać danego oprogramowania.

Standardowym elementem niemal każdej licencji oprogramowania, jest klauzula, o **wyłączonej** odpowiedzialności producenta z tytułu używania oprogramowania przez użytkownika, czyli na braku jakiejkolwiek odpowiedzialności producentów oprogramowania za np. skutki błędów w programach.

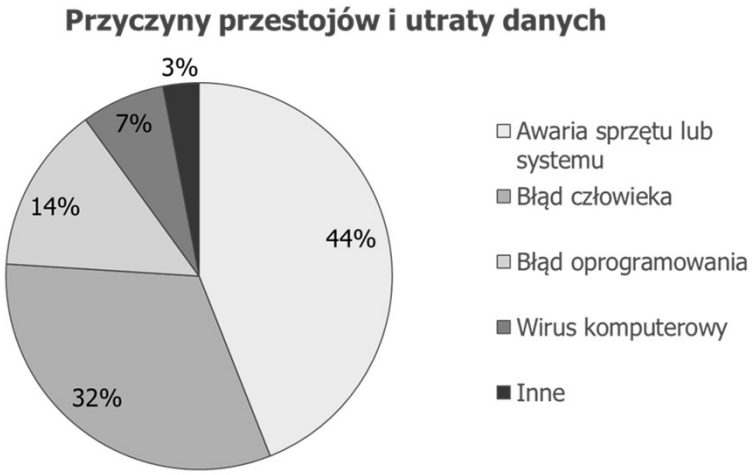
Rodzaje licencji komputerowych

- **jednostanowiskowa (one-site license) –** daje użytkownikowi prawo do instalacji danego programu na tylko jednym komputerze. Zgodnie z prawem, możliwe jest sporządzenie kopii zapasowej zakupionego programu. Program nie może być instalowana na kilku komputerach ani udostępniany za pośrednictwem Internetu innym użytkownikom;
- **grupowa (site license) –** licencja wielostanowiskowa, umożliwiająca korzystanie z oprogramowania przez większą liczbę użytkowników. Informacja na temat maksymalnej liczby osób uprawnionych do korzystania z programu jest uwzględniona w licencji;

Rodzaje licencji komputerowych

- **licencja sieciowa (network license) –** szczególna odmiana licencji grupowej, przeznaczona z myślą o określonej liczbie użytkowników, którzy mogą jednocześnie uruchomić program w ramach danej sieci komputerowej;
- **licencja firmware –** rodzaj licencji dotyczącej oprogramowania, zainstalowanego na stałe w urządzeniu, służącego do zarządzania nim.

Bezpieczeństwo w systemach informatycznych



28

Zagrożenia dla bezpieczeństwa systemów i użytkowników sieci Internet

- Podsłuch danych transmitowanych w sieci i dostęp nieuprawnionych osób do informacji zgromadzonych na dyskach. np. w bazach danych;
- Nieuprawnione korzystanie z zasobów systemu komputerowego, np. uruchomienie programu (wykorzystanie mocy procesora);
- Blokada usług systemu poprzez zlecenie serwerowi olbrzymiej liczby zadań powodujących takie obciążenie systemu, że kolejne zlecenia nie są obsługiwane lub czas ich realizacji znacząco wzrasta;

29

Zagrożenia dla bezpieczeństwa systemów i użytkowników sieci Internet

- Utrata danych na skutek złośliwego niszczenia zasobów informacyjnych systemu komputerowego, np. poprzez włamanie do systemu lub w wyniku działania wirusa komputerowego;
- Fałszowanie informacji lub/oraz podawanie się za innych użytkowników i działanie w ich imieniu i na ich rachunek. np. rozsyłanie poczty elektronicznej z cudzego konta pocztowego:
- Fizyczne odcięcie źródła informacji (serwera) od sieci komputerowej. np. awaria zasilania, kradzież komputera.

30

Wybrane metody zabezpieczenia informacji

- Urządzenia zastępcze
- Czynniki fizycznego bezpieczeństwa informacji
- Autoryzacja i uwierzytelnianie
- Szyfrowanie informacji
- Podpis elektroniczny

31

Szyfrowanie informacji

Systemy szyfrowania dzielą się ogólnie na dwa rodzaje:

- **symetryczne** - do szyfrowania i rozszyfrowania służy ten sam klucz, zwany także kluczem tajnym
- **asymetryczne** - używane są dwa różne klucze: publiczny do szyfrowania i tajny do rozszyfrowania.

Ochrona danych

Przyczyny utraty danych

- Przypadkowe skasowanie;
- Celowe skasowanie celem zacierania śladów lub jako efekt sabotażu;
- Działanie złośliwego oprogramowania (np. wirusa)
- Uszkodzenie w wyniku przerwy w dostawie energii elektrycznej lub skoku napięcia;
- Błędy oprogramowania korzystającego z danych lub je aktualizującego;
- Nieprawidłowe wyłączenie komputera;
- Uszkodzenie urządzenia pamiętającego;
- Uszkodzenie lub brak struktur systemu plików;
- Formatowanie.

Ochrona danych

Metody zabezpieczenia przed zniszczeniem

- Zapisywanie na możliwie niezawodnych urządzeniach pamięciowych;
- Zabezpieczenie przed dostępem niepowołanych osób:
- Zapisywanie w więcej niż jednym egzemplarzu, z których każdy zapisywany jest na innym urządzeniu, które z kolei są przechowywane w różnych lokalizacjach.

Ochrona sieci komputerowych

W ochronie punktów styku wyróżnić można następujące grupy rozwiązań:

Ochrona przed wirusami, robakami, trojanami:

- Rozwiązania dostępne w postaci dedykowanych urządzeń (appliance), oprogramowania zintegrowanego z bramką (proxy) lub z systemem zaporowym;
- System alertowania generujący komunikaty dla administratorów;
- Zaawansowane możliwości raportowania i zdalnego zarządzania.

Ochrona sieci komputerowych

W ochronie punktów styku wyróżnić można następujące grupy rozwiązań:

Kontrola niepożądanej treści:

- Rozwiązania pozwalające w sposób niezauważalny przez użytkowników monitorować ich działania w sieci Internet, tworzyć raporty, jak również w pełni zarządzać wykorzystaniem Internetu;
- Możliwość kategoryzacji stron internetowych oraz blokowania niepożądanych kategorii nie związanych z wykonywaną pracą (np.: strony pornograficzne) - zwiększa to produktywność oraz minimalizuje ryzyko powikłań prawnych dla firmy;
- Wbudowany system alertowania generujący powiadomienia dla administratorów;
- Zaawansowane możliwości raportowania i zdalnego zarządzania.

Rodzaje złośliwego oprogramowania

Dialer

- oprogramowanie służące do modyfikacji numeru z jakim łączy się modem w celu zwiększenia opłat za połączenie. Obecnie nie spotykane.

Worm (Robak)

- programy rozmnażające się tylko przez sieć. Nie potrzebują programu "żywiciela" tak jak typowe wirusy. Często powielają się pocztą elektroniczną.

Rodzaje złośliwego oprogramowania

Exploit

- oprogramowanie wykorzystujące luki w systemie lub tylko jednym z zainstalowanych programów najczęściej w celu przejęcia kontroli nad naszym komputerem i wykorzystania go do ataku na serwis internetowy.

39

Rodzaje złośliwego oprogramowania

SQL/URL injections

- Zapytanie SQL to żądanie wykonania jakiejś czynności w bazie danych, zwykle jest to zapytanie ze strony internetowej pytającej o nazwę użytkownika i hasło. Ponieważ jednak większość stron nie wymaga podania żadnych danych poza nazwami użytkownika i hasłami, haker może wykorzystać pola formularzy do wysyłania własnych żądań, tzn. wstrzykiwania kodu SQL do bazy danych. Tym sposobem hakerzy mogą tworzyć, odczytywać, aktualizować, modyfikować i usuwać dane przechowywane w bazach danych, zwykle w celu pozyskania poufnych informacji.

40

Rodzaje złośliwego oprogramowania

Wirusy

- program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika.
- ze względu na różne rodzaje infekcji wirusy dzielą się na:
  - wirusy **gnieżdżące** się w boot sektorze twardego dysku (boot sector viruses),
  - wirusy **pasożytnicze** (parasitic viruses),
  - wirusy **wieloczęściowe** (multi-partite viruses),
  - wirusy **towarzyszące** (companion viruses),
  - **makro** wirusy (macro viruses).

41

Rodzaje złośliwego oprogramowania

Trojany

- nie rozmnażają się jak wirusy, ale ich działanie jest równie szkodliwe. Ukrywają się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika np. otwiera port komputera, przez który może być dokonany atak hakera.

42

Rodzaje złośliwego oprogramowania

Wabbit/Fork bomb

- powoduje samoreplikację aż do wyczerpania zasobów komputera. Takie działanie powoduje kompletne zablokowanie komputera.

Backdoor

- trojan otwierający „drzwi” do naszego komputera w celu wykorzystania go do nielegalnej działalności w sieci jako tak zwane zombie PC.

Rodzaje złośliwego oprogramowania

Rootkit

- zestaw narzędzi umożliwiający podszywanie się pod administratora systemu w celu uzyskania jego uprawnień i przeprowadzenia szkodliwych działań w naszym komputerze. Nazwa wzięła się od słów Root – określenie administratora w systemach typu Unix oraz kit – zestaw.

Rodzaje złośliwego oprogramowania

Spyware

- oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody. Występuje często jako dodatkowe i ukryte komponenty większego programu, odporne na usuwanie i ingerencję użytkownika. Spyware zmienia wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Potrafi pobierać i uruchamiać pliki pobrane z sieci.

Rodzaje złośliwego oprogramowania

Scumware

- to ogólnie każde oprogramowanie, konkretnie, pobrane z Internetu bez naszej wiedzy. Coraz częściej są to nielegalne pliki Cookie, które magazynują nasze preferencje w sieci.

Adware

- jeden z najczęstszych złośliwych programów jaki spotyka każdego użytkownika Internetu. Często instaluje się bez naszej wiedzy i ciężko go usunąć. Wyświetla nam dodatkowe reklamy, których niejednokrotnie nie można zamknąć.

Rodzaje złośliwego oprogramowania

Keylogger

- występuje w dwóch postaciach: programowej i sprzętowej. Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody, cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe keyloggery były widoczne w środowisku operacyjnym użytkownika. Teraz coraz częściej są procesami niewidocznymi dla administratora.

Hijacker BHO

- Browser Hijacker Object (porywacz przeglądarek) modyfikuje ustawienia przeglądarki internetowej użytkownika. Może to oznaczać zmianę domyślnej strony startowej, przekierowanie na niechciane strony WWW, dodanie niechcianych zakładek lub generowanie niechcianych okien wyskakujących.

47

Rodzaje złośliwego oprogramowania

Stealware

- Pod tym pojęciem kryje się rożne oprogramowanie, które bez naszej wiedzy wykrada nasze dane i wysyła do osób trzecich

Hoaxes

- fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (ang. hoaxes), także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe z wysokim poziomem skanowania heurystycznego. Żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

48

Dodatkowe zagrożenia w sieci

Phishing

- metoda oszustwa, która polega na podszywaniu się pod inną osobę, czy też instytucję. Działanie to podjęte jest w celu wyłudzenia informacji, bądź nakłonienia ofiary do konkretnego działania.

Pharming

- jedna z najbardziej niebezpiecznych dla potencjalnego użytkownika form phishingu. Nawet jeżeli wpiszemy właściwy adres strony, zostaniemy przekierowani na fałszywą. Wygląda ona identycznie jak oryginalna strona www, jednak jej celem jest przejęcie danych logowania, haseł lub numerów kart kredytowych.

Ochrona przed szkodliwym oprogramowaniem

- stosowanie programów antywirusowych, których celem jest rozpoznawanie i eliminowanie wirusów,
- stosowanie programów usuwających adware oraz spyware, które mogły nie zostać wykryte przez program antywirusowy lub na których instalację użytkownik zgodził się nieświadomie,
- stosowanie dodatków blokujących reklamy,
- wykonywania kopii zapasowych najważniejszych plików lub całych dysków
- możliwości przechowywania plików online, w tak zwanej „chmurze”,

Ochrona przed szkodliwym oprogramowaniem

- uważnie czytać komunikaty, które pojawiają się w czasie instalacji programów,
- pobierać programy i aplikacje jedynie z zaufanych stron internetowych,
- regularnie aktualizować zainstalowane oprogramowanie, a przede wszystkim system operacyjny,
- regularnie skanować dyski programem antywirusowym
- nie otwierać załączników wiadomości e-mail od nieznanych nadawców,
- nie klikać w pojawiające się reklamy i informacje o wygranych.