SYSTEMY OPERACYJNE

PRAWO AUTORSKIE I PRZESTĘPCZOŚĆ KOMPUTEROWA

PRAWO AUTORSKIE – PODSTAWA PRAWNA

W 1994 roku zostały uchwalone przez Sejm przepisy obejmujące ochronę programów komputerowych. Szczegóły możesz znaleźć w Dz. U. Nr 24 z 4.02.1994 r. - ustawa o prawie autorskim i prawach pokrewnych. Ochrona oprogramowania komputerowego gwarantuje twórcy autorskie prawa osobiste oraz prawo majątkowe. Twórca programu posiada wyłączne prawo do korzystania z utworu oraz rozporządzania nim.

PRAWO AUTORSKIE

Prawo autorskie zajmuje się ochroną twórczych produktów naszego intelektu, takiej jak utwory muzyczne, programy komputerowe, utwory literackie, plastyczne i inne.

Prawo autorskie chroni prawa twórców do ich utworów, podobnie jak prawo własności, chroni prawa właścicieli do ich rzeczy. Mówi się potocznie, że np. jakaś piosenka jest czyjąś własnością. Prawnicy określają to własnością intelektualną. Prawo własności dotyczy rzeczy materialnych, tj. samochodu, komputera, domu, natomiast prawo autorskie chroni przedmioty niematerialne; zajmuje się utworami jako dobrami intelektualnymi.

PRAWO AUTORSKIE

Prawo autorskie nie zajmuje się natomiast obrotem nośnikami, na których są zapisane dzieła. Sprzedaż płyt CD z muzyką reguluje prawo cywilne. Ale już kwestiami praw do wydania danego utworu w określonej formie, np. na płycie CD, zajmuje się prawo autorskie. Podobnie jest z programami zapisanymi na CD, DVD, dyskietkach.

CO TO JEST UTWÓR?

Utwór jest dobrem niematerialnym. Dla zaistnienia utworu wystarczy zapoznanie się z nim (inaczej ustalenie) w jakikolwiek sposób, przez co najmniej jedną osobę poza, oczywiście, twórcą.

Utwór – każdy uzewnętrzniony w jakikolwiek sposób przejaw działalności twórczej o indywidualnym charakterze np. utwór muzyczny, literacki, plastyczny, komputerowy (np. program).

Dobra niematerialne to twórcze produkty naszego intelektu, których istnienie nie jest zależne od fizycznego utrwalenia, np. zapisu na dysku w przypadku programu komputerowego.

CO TO JEST UTWÓR?

Zgodnie z polskim prawem autorskim, program komputerowy jest traktowany na równi z utworem muzycznym lub literackim. Prawo autorskie chroni utwory, w tym programy, już od momentu ich ustalenia, co niekoniecznie jest związane z utrwaleniem na jakimś fizycznym nośniku, takim jak kartka papieru czy CD. Nie ma znaczenia, na czym i czy w ogóle jest on zapisany. Wystarczy choćby „napisanie” takiego programu w głowie (sytuacja podobna do ułożenia w głowie wiersza) i „wyrecytowanie” go. Jeżeli z takim programem zapozna się (usłyszy go), choć jedna osoba, należy uznać go za ustalony. Oczywiście nie ma przeszkód, by to ustalenie nastąpiło przez spisanie programu na kartce lub wprowadzenie go do pamięci komputera, na dyskietkę, płytę CD.

Nie wszyscy zdajemy sobie sprawę, że kupując np. oryginalny Egzemplarz płyty CD z muzyką, nie „kupujemy” muzyki jako takiej. Nie nabywamy do niej samej praw autorskich,

KORZYSTANIE Z PROGRAMÓW OBJĘTYCH PRAWEM AUTORSKIM

Bez zezwolenia posiadacza praw autorskich do programu jego legalny użytkownik może:

- utworzyć jedną kopię zapasową jeżeli jest to niezbędne do korzystania z programu komputerowego
- zwielokrotniać kod, jeżeli jest to niezbędne do uzyskania informacji do osiągnięcia współdziałania niezależnie działającego programu

Autorskie prawa majątkowe obejmują:

- trwałe lub czasowe zwielokrotnianie programu komputerowego
- dokonywanie jakichkolwiek zmian w programie
- rozpowszechnianie programu lub jego kopii

PRZYKŁADY NARUSZENIA PRAW AUTORSKICH

Naruszeniem praw autorskich (tzw. osobistych) będzie likwidacja podpisów zdjęć, udostępnianych (np. w ramach darmowej kolekcji) na stronie WWW, oraz tzw. cyfrowych „znaków wodnych", np. z logiem autora. Nawet gdy wymienione materiały są udostępniane darmowo, nie zwalnia nas to z respektowania osobistych praw autorskich twórcy. W tym wypadku jego prawa do oznaczenia swojego utworu. A zatem, skoro zdjęcia są „darmowe” (twórca zrezygnował z czerpania finansowych korzyści ze swoich praw majątkowych do utworu), to znaczy, że owszem – możemy wykorzystać je dla własnych celów, ale nadal musimy respektować prawa osobiste twórcy, bo skoro „podpisał” swoje dzieło, dał nam do zrozumienia, że sobie tego życzy.

PRZYKŁADY NARUSZENIA PRAW AUTORSKICH

Samowolne wprowadzanie utworu muzycznego do sieci w postaci pliku MP3, bez zgody osoby uprawnionej. Aby legalnie rozpowszechniać utwory w Internecie, należy zawsze uzyskać zgodę autora, producenta lub innej osoby uprawnionej do utworu. Dodatkowo zgoda ta musi określić, że chodzi o rozpowszechnianie utworów właśnie w sieci, a nie w inny sposób. Jeżeli bowiem ktoś nabył prawa do rozpowszechniania danego utworu – dajmy na to, na płytach CD i kasetach – może to robić legalnie, używając tylko tych nośników, a nie innych.

LICENCJE

Licencje to rodzaj umowy, w której autor utworu lub ktoś, kto ma do niego prawa autorskie (np. producent oprogramowania), określa na jakich prawach pozwala odbiorcy utworu (np. użytkownikowi programu) z niego korzystać. W przypadku programów komputerowych zawarcie umowy licencyjnej następuje przeważnie już przez samo otwarcie i odpieczętowanie pudełka z nośnikiem. A zatem zdarcie folii z dysków CD, które są zazwyczaj zapakowane wraz z książeczką licencyjną i certyfikatem autentyczności, jest równoznaczne z przyjęciem zasad licencji. W Internecie z kolei praktyką jest, że treść licencji zostaje wyświetlona na stronie WWW, a użytkownik potwierdza zgodę na jej warunki przez kliknięcie na odpowiedni przycisk ekranowy. W ten sposób godzimy się na przedstawione przez autora zasady korzystania ze strony Internetowej lub np. na warunki korzystania z zamieszczonych na niej programów do ściągnięcia. Ogólną zasadą jest posiadanie oddzielnych licencji programu komputerowego na każde stanowisko komputerowe. Nie można równocześnie instalować danego programu komputerowego z pojedynczą licencją na wielu komputerach.

PODSTAWOWE RODZAJE LICENCJI

Pełna wersja – program komercyjny bez żadnych ograniczeń. Jego rozprowadzanie w innych mediach (np. Internecie) jest niezgodne z prawem.

Freeware – określenie programu, którego można używać bezpłatnie i bez żadnych ograniczeń. Jego autor nie jest zainteresowany komercyjnym rozprowadzaniem swoich produktów, jednak jego prawa autorskie pozostają nadal w mocy. Nikt nie może np. wprowadzać żadnych zmian w tych programach. Aplikacje te nie nakładają na użytkownika obowiązku rejestracji, mogą być jednak rozpowszechniane wyłącznie w niezmienionej formie. W niektórych programach status Freeware dotyczy tylko użytkowników indywidualnych. W przypadku firm obowiązuje opłata licencyjna. Niektóre programy posiadają dodatkowo rozbudowaną wersję „Pro”, za którą już trzeba zapłacić.

PODSTAWOWE RODZAJE LICENCJI

Public domain – oprogramowanie oddawane darmowo na użytek ogółu, jako tzw. dobro publiczne. Dozwolona jest dalsza dystrybucja takich programów bez zgody autora.

Shareware – autorzy programów shareware'owych udostępniają bezpłatnie swoje dzieło do testów. Każdy przyszły nabywca, przed podjęciem decyzji o zakupie, może gruntownie sprawdzić w działaniu zazwyczaj w pełni funkcjonalną wersję. Część z tych programów ma jednak pewne ograniczenia, najczęściej jest to limitowany czas na testowanie takiej aplikacji.

Licencja GPL (General Public Licence) – zasady licencyjne określone przez konsorcjum Free Software Foundation, zakazujące redystrybucji oprogramowania w formie czysto binarnej. Jeżeli ktoś wprowadza do obiegu oprogramowanie zawierające jakąkolwiek część podlegającą licencji GPL, to musi udostępnić wraz z każdą dystrybucją binarną jej postać źródłową.

PODSTAWOWE RODZAJE LICENCJI

Licencja grupowa (Site licence) – określa, że zakupiony program może być użytkowany w sieci lub innym zestawie komputerów (np. szkolna pracownia) w określonej ilości, tzn. może być instalowany tylko na określonej maksymalnej liczbie stanowisk. Podobną zasadą określane są programy sprzedawane z licencją sieciową (Network licence).

Licencja jednostanowiskowa (One-site licence) – to licencja uprawniająca użytkownika do zainstalowania nabytego oprogramowania tylko na jednym stanowisku komputerowym. Użytkownikowi nie wolno udostępniać takiego oprogramowania w sieci ani używać więcej niż jednym komputerze w tym samym czasie. Zezwala natomiast na sporządzenie kopii zapasowej oprogramowania.

PODSTAWOWE RODZAJE LICENCJI

Licencja na obszar – to określenie umowy między producentem oprogramowania a nabywcą, uprawniająca go do sporządzenia określonej liczby kopii zakupionego oprogramowania na swój własny użytek. Takie rozwiązanie jest czasem stosowane przez firmy korzystające z sieci lokalnych LAN, umożliwia to wykorzystanie oprogramowania na wielu stanowiskach komputerowych ponosząc przy tym mniejsze koszty.

FORMY OGRANICZEŃ PROGRAMÓW

Trial – program po zainstalowaniu jest w pełni sprawny i działają jego wszystkie komponenty, ale tylko przez określoną ilość czasu od dnia jego zainstalowania w systemie. Po tym okresie, o ile użytkownik nie wprowadzi zakupionego u producenta kodu, program przestaje się uruchamiać i trzeba go odinstalować.

FORMY OGRANICZEŃ PROGRAMÓW

Demo – program po zainstalowaniu nie ma żadnych ograniczeń czasowych, ale za to część jego funkcji jest niedostępna, co pomniejsza jego wartość dla użytkownika. Zakupienie u producenta kodu rejestracyjnego odblokuje niedostępne opcje, czyniąc program w pełni użytecznym. Spotyka się również programy, które po zainstalowaniu są w pełni sprawne i bez ograniczeń czasowych, ale za to z limitem możliwych uruchomień, przeciętnie nie więcej niż 100. Następny program to taki, który po zainstalowaniu nie ma żadnych ograniczeń czasowych, funkcyjnych ani uruchomieniowych, ale za to każdorazowo w czasie startu aplikacji, jak i później w czasie korzystania z niej, samoczynnie wyświetla nachalne komunikaty, przypominające o konieczności rejestracji programu. Jeszcze inną wersją jest program, który nie ma żadnych ograniczeń czasowych, funkcyjnych ani uruchomieniowych. Autor zwyczajnie licząc na uczciwość użytkownika, oczekuje, że ten dostosuje się do regulaminu i we właściwym czasie zarejestruje program lub usunie go z systemu.

FORMY OGRANICZEŃ PROGRAMÓW

Adware – to programy, za których użytkowanie się nie płaci. Producenci czerpią z nich zyski przez umieszczanie w nich reklam. Jeśli użytkownik jest zadowolony z efektu pracy autorów programu, może im się odwdzięczyć wchodząc na reklamę sponsora. Większość autorów adware proponuje za niewielką opłatą także wersje bez reklam.

Postcardware – to określenie pewnego statusu, pod jakim autor programu rozprowadza swoją aplikację. Wymaga on, aby użytkownik, chcący korzystać z programu, wysłał do autora (tytułem zapłaty) kartę pocztową z opinią na temat programu.

PRZESTĘPCZOŚĆ KOMPUTEROWA

Konwencja Rady Europy nr 185 określa przestępstwa komputerowe które powinny być zwalczane w krajach członkowskich Rady Europy i innych państw będących sygnatariuszami konwencji:

- Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów
  - nielegalny dostęp
  - nielegalne przechwytywanie danych
  - naruszenie integralności danych
  - naruszenie integralności systemu
  - niewłaściwe użycie urządzeń
- Przestępstwa komputerowe
  - fałszerstwo komputerowe
  - oszustwo komputerowe
- Przestępstwa ze względu na charakter zawartych informacji
  - przestępstwa związane z pornografią dziecięcą
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

PRZESTĘPCZOŚĆ KOMPUTEROWA

Piractwo komputerowe - to kopiowanie, reprodukowanie, używanie i wytwarzanie bez zezwolenia produktu chronionego przez prawo autorskie.

Piractwem komputerowym jest też:

- fałszowanie, używanie cracków i nr seryjnych w celu uzyskania dostępu do nieograniczonej wersji danego programu,
- umieszczanie na serwerach pełnych wersji oprogramowania w celu udostępniania innym, np. poprzez sieci p2p,
- wynajem oprogramowania.

HACKING

Hacking - włamywanie do systemów lub sieci komputerowych.

Haker – osoba włamująca się do systemów lub sieci komputerowych.

Hacker ponosi odpowiedzialność karną za zapoznanie się z treścią przechowywanej w systemie komputerowym informacji, pod warunkiem że uzyska do niej dostęp na skutek przełamania zabezpieczeń. Nie ma znaczenia, czy pozyskaną informację wykorzysta, zniszczy, usunie czy ujawni. Hakerzy naruszają min. art. 267 §1 Kodeksu karnego.

HACKING

Hakerem nie jest osoba, która wykorzystuje lukę w systemie i dzięki niej uzyskuje informację, jeżeli

- wykorzystanie luki nie wymaga ingerencji w zapis znajdujący się na komputerowym nośniku informacji ani korzystania ze specjalnego oprogramowania.
- uzyskuje dostęp do systemu informatycznego w celu wykazania, że system ma błędy umożliwiające taki dostęp i jeżeli w wyniku dostępu nie zapozna się z żadnymi danymi znajdującymi się w systemie.

HACKING

Typy hakerów:

- **white hat hacker** (haker w białym kapeluszu). Osoba mająca wiedzę i umiejętności do włamania się do systemu ale robi to na użytek jakiegoś podmiotu, np. przedsiębiorstwa w celu testowania bezpieczeństwa sieci.
- **black hat hacker** (haker w czarnym kapeluszu). Osoba mająca wiedzę i umiejętności do włamania się do systemu w celach 'nieetycznych', np. kradzieży.
- **gray hat hacker** (haker w szarym kapeluszu). Haker w białym kapeluszu, który czasami jest hakerem w czarnym kapeluszu.
- **phreaker**. Haker systemów telekomunikacyjnych.
- **script kiddy**. Osoba os małych umiejętnościach hakerskich wykorzystująca dostępne narzędzia hakerskie (nie tworzy własnych narzędzi).
- **hacktivist**. Haker włamujący się do systemów (np. na serwery WWW) z powodów politycznych.
- **computer security hacker**. Haker posiadający wiedzę i umiejętności do włamywania się do sieciowych systemów bezpieczeństwa.
- **academic hacker**. Haker wykorzystujący zasoby uczelni (sprzęt komputerowy, oprogramowanie) do tworzenia i stosowania programów hakerskich.
- **hobby hacker**. Haker wykorzystujący swoje umiejętności do modyfikowania systemu z którego korzysta w domu.

SNIFFING

Sniffing – podsłuchiwanie pakietów w sieci.

Skanowanie sieci (network scanning) – jest to wykorzystanie specyfiki implementacji protokołów do sondowania urządzeń w sieci, aplikacji.

Narzędzia służące do skanowania i analizy pakietów w sieci

- nmap
- wireshark,
- tcpdump,

Skanowanie sieci jest naruszeniem art. 267 § 2 Kodeksu karnego.

PHREAKING

Phreaking, czyli podłączania się domowo wykonanymi urządzeniami elektronicznymi do sieci telefonicznej w celu podsłuchiwania rozmów.

HIJACKING

Session hijacking - polega na uzyskiwaniu nieuprawnionego dostępu do systemów poprzez przechwycenie sesji legalnego użytkownika.

Session hijacking - przejmowanie połączeń poprzez „wstrzelenie” odpowiednio dobranych pakietów – wymaga dostępu do uprzednio legalnie zestawionego połączenia TCP (wazniak.mimuw.edu.pl).

Browser hijacker - oprogramowanie, które modyfikuje ustawienia przeglądarki internetowej użytkownika.

Hijacking jest naruszeniem art. 267 § 2 Kodeksu karnego.

SPOOFING

Spoofing – podszywanie się pod innego użytkownika w sieci.

IP spoofing – rodzaj ataku w którym adres IP napastnika rozpoznawany jest jako adres zaufany.

TCP spoofing – podszywanie bazujące na oszukaniu mechanizmu generowania numerów ISN; wykorzystanie ataku np. w celu oszukania mechanizmów uwierzytelniania usług.

UDP spoofing – modyfikacja pakietów w celu atakowania usług i protokołów wykorzystujących protokół UDP, np. DNS.

Przykład 1.

W celu ochrony sesji BGP przed podszywaniem się pod nadawcę lub odbiorcę danych (spoofing) wprowadzono podpis MD5 dla nagłówka protokołu TCP, RFC 2385.

CRACKING

Cracking – łamanie zabezpieczeń programów komputerowych, dostępu do systemów, usług sieciowych.

Cracker – osoba zajmująca się wyszukiwaniem i usuwaniem zabezpieczeń w oprogramowaniu komputerowym.

„Krakowanie” programów jest naruszeniem art. 268 § 1, art. 269 § 1 Kodeksu karnego.

PHISHING

Phishing (password fishing) - metoda uzyskiwania haseł dostępu do zasobów internetowych (kont bankowych użytkownika) za pośrednictwem e-maili. Atakujący podszywa się pod przedstawiciela instytucji finansowej próbując nakłonić odbiorców e-maili do przesłania im haseł oraz innych danych osobowych (np. poprzez fałszowanie stron WWW).

PHARMING

Pharming, zatruwanie DNS. Metoda uzyskiwania haseł dostępu do zasobów internetowych poprzez fałszowanie stron WWW. Z powodu ingerencji w zasoby systemu DNS nawet wpisanie poprawnego adresu URL w przeglądarce może spowodować pojawienie się fałszywej strony WWW.

POISONING

ARP spoofing/poisoning – modyfikowanie nagłówka protokołu ARP, w celu zdalnej modyfikacji tablic ARP systemów operacyjnych, przełączników, lub przepełniania tablic ARP.

DNS cache poisoning (pharming, birthday attack) – modyfikacja informacji o domenach w pamięci resolvera DNS.

ICMP redirect – wykorzystanie ICMP do zmiany trasy routingu dla wybranych adresów sieciowych.

SKANOWANIE PORTÓW

Proces wysyłania wiadomości do hostów na konkretne porty, aby sprawdzić, czy są otwarte.

WARDRIVING

Wardriving - polega na jeżdżeniu po mieście, aby zlokalizować bezprzewodowe punkty dostępowe, w celu zdobycia nieautoryzowanego dostępu do niezabezpieczonych sieci bezprzewodowych.

VISHING

Metoda oszustwa, polegająca na wykorzystaniu telefonii internetowej w celu podszycia się pod instytucję finansową.

Jedną z metod jest rozsyłanie spamów, w których podawane są numery 0-800, pod którymi odbiorca e-maila powinien zaktualizować swoje dane przy koncie bankowym.

Po wykręceniu podanego numeru włącza się automat, który prosi ofiarę o podanie konkretnychdanych dostępowych do konta.