

Raport Security

locos.pl

KONTROLE LEGALNOŚCI OPROGRAMOWANIA KOMPENDIUM WIEDZY.

W ostatnim okresie czasu zdecydowanie nasiliły się kontrole legalności oprogramowania, co wyraźnie widać w licznych doniesieniach prasowych o policyjnych przeszukaniach w firmach i mieszkaniach. Nie sposób też nie dostrzec tematu w codziennych dyskusjach, także tych na forach internetowych. Wokół tematu powstało wiele nieporozumień i mitów. Niniejszy artykuł jest próbą stworzenia kompendium wiedzy w tym zakresie i ma za zadanie wyjaśnić przynajmniej część wątpliwości pojawiającym się w związku z kontrolami legalności.

Piractwo komputerowe

Piractwo komputerowe jest według powszechnie przyjętej definicji działalnością polegającą na łamaniu praw autorskich poprzez nielegalne kopiowanie lub nielegalne posługiwanie się utworami, jakimi niewątpliwie są programy komputerowe. Owa „nielegalność” może oznaczać, iż program komputerowy kopiujemy lub posługujemy się nim bez zgody autora, wbrew warunkom udzielonej licencji lub bez uiszczenia stosownych opłat z tyt. tzw. praw autorskich.

Piractwo komputerowe przejawia się najczęściej poprzez:

- wykonanie nielegalnych kopii oraz fałszowanie nośników,
- niezgodne z udzieloną licencją:
 - preinstalacja oprogramowania,
 - wypożyczanie lub wynajem,
 - wykonywanie dodatkowych kopii (np. zapasowych),
 - brak wymaganych atrybutów legalności,
 - brak rejestracji,
 - wykorzystanie oprogramowania na większej liczbie stanowisk, niż przewiduje licencja, etc.

(BSA), Polska zajmuje drugie miejsce w rankingu największego zagrożenia piractwem komputerowym wśród państw Unii Europejskich. Blisko 60 proc. oprogramowania zainstalowanego w naszych komputerach jest nielegalne.

W polskim prawie znane są przestępstwa, które można określić mianem piractwa komputerowego. Podstawą prawną w tym zakresie jest ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. Nr 88, poz. 553 ze zm.) oraz ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. z 2006 r., Nr 90, poz. 631 ze zm.).

Kodeks karny przewiduje karę pozbawienia wolności od 3 miesięcy do 5 lat za uzyskanie cudzego programu komputerowego, bez zgody osoby uprawnionej, w celu osiągnięcia korzyści komputerowej (art. 278 § 2) oraz taką samą karę za nabycie, pomoc w zbyciu, przyjęcie lub pomoc w ukryciu bezprawnie uzyskanych cudzych programów komputerowych (art. 291 § 1).

autorskim i prawach pokrewnych, przewidują ona karę grzywny, karę ograniczenia wolności oraz karę pozbawienia wolności do 2 lat za rozpowszechnianie bez uprawnienia lub wbrew jego warunkom cudzych utworów w wersji oryginalnej albo w postaci opracowania, w tym programów komputerowych (art. 116 ust. 1). Jeśli czyn ten miał na celu osiągnięcie korzyści majątkowej, ustawa przewiduje karę pozbawienia wolności do lat 3 (art. 116 ust. 2). Dodatkowo na podstawie art. 79 ust. 1 twórca (producent), którego prawa naruszono może żądać m.in.: wydania uzyskanych korzyści oraz zapłaty 2 lub 3-krotnego wynagrodzenia oraz naprawienia szkody.

Kolejną kwestią, która wymaga rozstrzygnięcia odpowiedzialność personalna z tytułu posiadanego nielegalnego oprogramowania. Jak się okazuje, w praktyce odpowiedzialność może zostać przypisana:

- członkom zarządu spółek prawa handlowego,
- dyrektorom przedsiębiorstw i instytucji np. państwowych,
- osobom, które zajmują się administracją sieci komputerowych,
- osobom fizycznym prowadzącym działalność gospodarczą, zwłaszcza

w zakresie sprzedaży urządzeń komputerowych,
 • właścicielom komputerów (użytkownicy końcowi).

Popelnienie przestępstwa może polegać na podjęciu przez kierownictwo decyzji o nabyciu i korzystaniu z nielegalnego oprogramowania. Kierownictwo ma więc zamiar popelnienia czynu zabronionego (wina umyślna - działanie w zamiarze bezpośrednim). Naruszana jest więc dyspozycja art. 18 § 1 K.k. (sprawstwo kierownicze), który stanowi, że odpowiada za sprawstwo nie tylko ten, kto wykonuje czyn zabroniony sam albo wspólnie i w porozumieniu z inną osobą, ale także ten, kto kieruje wykonaniem czynu zabronionego przez inną osobę lub wykorzystując uzależnienie innej osoby od siebie, poleca jej wykonanie takiego czynu. Osoba zarządzająca firmą popelnia czyn zabroniony również wtedy, gdy przewidując możliwość jego popelnienia na to się godzi (wina umyślna - działanie w zamiarze ewentualnym).

Przykładowo, jeżeli kierownictwo firmy ma świadomość, iż przy wykonywaniu określonych projektów niezbędne jest oprogramowanie specjalistyczne, a równocześnie wie lub podejrzewa, iż firma nie zakupiła takiego oprogramowania, to można mu przypisać winę za popelnienie przestępstwa paserstwa.

Innym przykładem takiego czynu jest wydanie dyspozycji pracownikom dowolnego kopiowania zakupionego przez firmę oprogramowania, bez zapoznania się z umową licencyjną wiążącą licencjobiorcę i licencjodawcę.

Jeśli chodzi o odpowiedzialność cywilną, można się w tym miejscu postłużyć analizą prawną uznaną kancelarii Sołtysiński, Kawecki & Szlęzak:

"Z tytułu odpowiedzialności cywilnej firmy ponoszą odpowiedzialność za działania podejmowane przez swoich pracowników. Odpowiedzialność osobistą, zarówno karną, jak i dyscyplinarną, a niekiedy nawet cywilną, za przestępstwa

związane z naruszeniem praw autorskich do oprogramowania mogą ponosić bezpośrednio osoby zarządzające: właściciele firm, członkowie zarządu spółek prawa handlowego, dyrektorzy przedsiębiorstw i instytucji państwowych oraz administratorzy sieci komputerowych. Osoby zarządzające mogą zmniejszyć ryzyko poniesienia takiej odpowiedzialności, jeżeli zatrudnią osobę na stanowisku np. administratora sieci, dyrektora lub specjalisty ds. IT, do którego obowiązków służbowych należy legalny zakup oprogramowania komputerowego lub/i dbanie o bezpieczeństwo systemów informatycznych. Dotkliwe kary grożą również przedsiębiorcom, którzy prowadzą działalność w zakresie sprzedaży urządzeń komputerowych, rozpowszechniając przy okazji oprogramowanie komputerowe w sposób nielegalny (np. instalując je na sprzedawanych przez siebie komputerach). Takie przestępstwo jest zagrożone między innymi karą pozbawienia wolności nawet do lat pięciu."

Kontrole legalności

Potocznie mówiąc o „kontrolach legalności” (popularnie nazywanych nalotami) mamy na myśli kontrole przeprowadzane przez Policję mające na celu wykrycie przypadków piractwa komputerowego. Należy jasno zaznaczyć, że organem uprawnionym do kontroli jest tylko i wyłącznie Prokurator lub Policja. Takie uprawnienie wynika z art. 220 § Kodeksu Postępowania Karnego z dnia 6 czerwca 1997 r. (Dz. U. Nr 89, poz. 555 ze zm.).

Nawiązując do przywołanych przepisów Policja może przybrać do czynności przeszukania specjalistów z zakresu informatyki, biegłego sądowego lub inną wskazaną osobę. W Policji sprawy związane z legalnością oprogramowania prowadzą wydziały/sekcje do walki z przestępczością gospodarczą.

W tym miejscu należy zaznaczyć, iż wbrew powszechnie panującemu przekonaniu kontroli legalności nie dokonują przedstawiciele organizacji działających w obronie praw autorskich czy pełnomocnicy producentów oprogramowania, a w szczególności nie dokonuje tego firma Microsoft. W związku z licznie pojawiającymi się błędnymi informacjami w tej sprawie firma Microsoft wydała nawet oświadczenie o następującej treści:



Należy zachować czujność, gdyż zdarzają się przypadki podszywania za funkcjonariuszy Policji czy też przedstawicieli firm softwareowych.

„W związku z docierającymi do nas informacjami o pojawieniu się w blokach mieszkalnych w kilku województwach ogłoszeń o planowanej kontroli legalności oprogramowania na prywatnych komputerach, chcielibyśmy poinformować, że akcja ta nie jest inicjatywą polskiego oddziału Microsoft i nie jest prowadzona w porozumieniu z nami. Nie jest nam również znane powiązanie jej inicjatorów z instytucjami zajmującymi się promocją i ochroną legalności oprogramowania komputerowego ani polskimi organami ścigania. Chcielibyśmy przestrzec użytkowników oprogramowania komputerowego przed wpuszczaniem

niem do prywatnych mieszkań osób podszywających się lub powołujących na firmę Microsoft. Osoby, które rozwieszają ogłoszenia i przeprowadzają „kontrolę” nie działają z polecenia firmy Microsoft i nie posiadają do tego żadnych pełnomocnictw. Prosimy jednocześnie, aby osoby, które spotkały się z tego typu akcją w swoim mieście, na swoim osiedlu lub w swoim bloku informowały o tym lokalne jednostki policji lub polski oddział Microsoft - e-mail: piratnie@microsoft.com.

W nieoficjalnych dyskusjach dotyczących tematu kontroli legalności, można było usłyszeć liczne opinie o braku fachowości Policji w kwestii samej czynności przeprowadzania przeszukania sprzętu komputerowego. Należy jednak zdementować takie opinie, gdyż umiejętności funkcjonariuszy Policji są stale podnoszone, a sami funkcjonariusze są coraz lepiej wyposażeni (także w oprogramowanie stricte audytorskie) oraz bardzo dobrze wyszkoleni.

Bardzo dobrym przykładem są działania Sekcji dw. z Przystępczością Gospodarczą Komendy Miejskiej Policji we Wrocławiu, którzy mogą pochwalić się jako jedyna jednostka w kraju, trzykrotnym zdobyciem nagrody „Złota Blacha”, za realizację spraw dotyczących kopiowania i rozpowszechniania pirackich nośników audiowizualnych.

Policja dokonuje przeszukania na podstawie nakazu sądu lub prokuratora. W sprawach niecierpiących zwłoki, jeśli uzyskanie takiego postanowienia w danej chwili nie było możliwe, wtedy przeszukanie może odbyć się za okazaniem nakazu kierownika jednostki (np. komisarzatu, komendy) lub legitymacji służbowej (art. 220 § 3 K. p. k.).

W tym momencie należy rozwiązać wszelkie wątpliwości dotyczące odpowiedzi na pytanie czy Polica

może przeprowadzić przeszukanie bez nakazu. Niewątpliwie, Polica posiada takie uprawnienia. W tym przypadku sąd lub prokurator musi w ciągu 7 dni zatwierdzić przeprowadzone przeszukanie. W praktyce, Polica często korzysta z tego przywileju. Przeprowadzając



Płyty zarekwirowane podczas nalotów
Źródło: <http://www.wroclaw.policja.gov.pl/>

„kontrolę” oprogramowania Policja tłumaczy, iż zgodnie z pozyskanymi informacjami przedmioty lub informacje stanowiące dowód mogły zostać zatarte lub usunięte (wykasowany program, wyniesiony komputer) i należało bezwzględnie podjąć czynności.

Skąd Policja zatem uzyskuje informacje o nielegalnym oprogramowaniu? Policja zapewnia, iż nie dokonuje przeszukań – szczególnie mieszkań - metodą „chybił-trafił”, jak się czasem nieoficjalnie spekuluje. W ogólnym ujęciu tematu, można mówić tu o zdobywaniu takiej wiedzy na drodze operacyjnej, co w praktyce oznacza informację przekazaną z infolinii antypirackich BSA (utrzymywaną m.in. przez firmę Microsoft), pozyskaną od informatora (np.: pracownik firmy) lub też z wiarygodnego zawiadomienia o popełnieniu przestępstwa. Oczywiście, do informacji operacyjnych mogą też zaliczać się donosy, np. konkurencji lub niezadowolonych pracowników.

Policja śledzi także popularne usługi wymiany plików P2P. W ten sposób mogą uzyskać numery IP osób, które logują się do sieci i ściągają nielegalne pliki. W takiej sytuacji

Policja uzyskuje dane osób od firm dostarczających Internet (ISP). W przypadku, w którym pod jednym adresem sieciowym występuje duża liczba użytkowników, łatwo jest wyłowić potencjalnych przestępców analizując logi systemowe (obserwacja wielkości transferów) lub obserwację udostępnionych w sieciach zasobów. Typowanie nie zawsze jest trafne i może się zdarzyć, że kontroli zostanie poddana osoba posiadająca legalne oprogramowanie natomiast znajdująca się w tej samej sieci co pirat (jest to bardzo częsty przypadek w tzw. sieciach osiedlowych).

Istnieją liczne wątpliwości, czy Policja ma także prawo przeszukiwać mieszkania prywatne.

W tym przypadku odpowiedź jest także twierdząca. Działając na podstawie art. 219 § 1 K.p.k. organ przeprowadzający czynności procesowe ma prawo do przeszukania mieszkania prywatnego - nawet za okazaniem legitymacji służbowej. Jednak w praktyce, przeszukania mieszkań Policja dokonuje za okazaniem nakazu stosownego prokuratora lub kierownika jednostki policji.

Przeszukanie obejmuje nie tylko same komputery, ale zgodnie z dyspozycją art. 236a K.p.k. może objąć dysponenta i użytkownika urządzenia zawierającego dane informatyczne, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.

W przypadku ujawnienia nielegalnego oprogramowania, Policja zabezpiecza nośnik oprogramowania jako dowód rzeczowy. W praktyce, zabezpieczenie oznacza zabranie przez Policję komputera, dysku twardego lub płyt CD.

W przypadku zabezpieczenia rzeczy, osoba, która rzecz wydała po-

winna niezwłocznie złożyć wniosek o sporządzenie i doręczenie jej postanowienia sądu lub prokuratora o zatwierdzeniu zatrzymania, czym musi być pouczone. Zgodnie z art. 217 § 4 K.p.k. doręczenie powinno nastąpić w terminie 14 dni od zatrzymania rzeczy.

Zatrzymanie takich przedmiotów jakimi są komputery, serwery czy media, w większości przypadków mogą prowadzić do ogromnych komplikacji w działalności firmy czy instytucji. W niektórych przypadkach jednostka może w ogóle zostać pozbawiona sprzętu komputerowego, który traktowany jest jako narzędzie do popełnienia przestępstwa. Dlatego w szczególnych przypadkach funkcjonariusz prowadzący przesłuchanie lub prokurator może zezwolić na skopiowanie ważnych danych, np. danych księgowych niezbędnych do funkcjonowania jednostki. Policja zobligowana treścią art. 227 K.p.k. musi zachować umiar i poszanowanie godności osób oraz nie wyrządzać niepotrzebnych szkód

i dolegliwości przy stosowaniu takich środków przymusu jak przesłuchanie i zatrzymanie

Tutaj pojawia się pytanie, czy Policja przeszukując mieszkanie prywatne, gdy odnajdzie służbowy komputer (laptopa), może go skontrolować, względnie zatrzymać? Odpowiedź po raz kolejny jest



twierdząca - Policja jak najbardziej może taki laptop skontrolować i zabezpieczyć. W takiej sytuacji obowiązkiem przedstawiciela firmy (np. administratora) jest przedstawienie odpowiednich licencji czy

atributów legalności aby udowodnić, że zainstalowane na służbowym sprzęcie oprogramowanie jest legalne.

Na koniec kilka słów o organizacji Business Software Alliance. BSA jest organizacją, której oficjalnym celem jest promowanie bezpieczeństwa i poszanowania prawa w społeczeństwie informacyjnym oraz reprezentowanie wobec instytucji publicznych, jak i na rynku międzynarodowym, interesów producentów oprogramowania komputerowego oraz ich partnerów produkujących sprzęt komputerowy. W swoich celach reprezentuje potentatów świata softwareowego, m.in. takie firmy jak Microsoft, Adobe, Autodesk, McAfee, SAP, Symantec, Sybase i inne. W praktyce BSA prowadzi linię antypiracką, występuje przed sądem w imieniu swoich członków, zbiera i przeprowadza analizę informacji dotyczących piractwa oraz zajmuje się szeroko pojętą promocją i edukacją w tym zakresie.



Przykładowa akcja edukacyjna BSA
Źródło: <http://www.bsa.org/>

W przeszłości, na temat BSA krążyło wiele spekulacji, głównie odnośnie działań o charakterze lobbystycznym z zakresu ochrony prawa autorskiego. BSA słynie też ze swoich filmów edukacyjnych, w których przedstawiają scenariusze policyjnych „nalotów” – wszystko to okraszane dramaturgią rodem z filmów Hitchcocka. Reasumując, działania BSA były i nadal są kontrowersyjne, natomiast nie można odmówić organizacji wysokiej skuteczności w realizacji zamierzonych celów.

Zobacz także:

- Ochrona własności intelektualnej”, Microsoft , <http://www.microsoft.com/poland/>
- Business Software Alliance, www.bsa.org/poland
- „Trzykrotne zdobycie prestiżowej nagrody Złota Błacha”, Komenda Miejska Policji we Wrocławiu, <http://www.wroclaw.policja.gov.pl/>
- Eliza Głowicka, Michał Gigolla, „Policja toczy wojnę z piratami”, Słowo Polskie – Gazeta Wroclawska, 19.01.2007
- „Ochrona własności intelektualnej”, Dziennik ONLINE, <http://www.dziennik.pl/Default.aspx?TabId=14&ShowArticleId=27940>
- Przemysław Gamdzik, „Przestępstwa na dysku”, Computerworld Online, 2.04.2002, <http://www.computerworld.pl/artykuly/21961.html>

OPRACOWANIE

Na podstawie zgromadzonych materiałów:
Piotr Błaszczek, Tadeusz Calanca

O autorach:

Piotr Błaszczek - specjalista ds. bezpieczeństwa IT, audytor systemów IT, biegły sądowy, na co dzień Główny Specjalista Bezpieczeństwa w jednej z agencji rządowych i administrator sieci, członek ISACA International.

Tadeusz Calanca - specjalista ds. bezpieczeństwa IT, audytor IT, biegły sądowy, na co dzień administrator systemów informatycznych oraz administrator bezpieczeństwa informacji