Informacja naukowa

Jan Hajdukiewicz

e – przestępczość, zagrożenia dla gospodarki

1. Wprowadzenie

Światowa rewolucja techniczna, jaką obserwujemy w ostatnim dziesięcioleciu, to rewolucja telekomunikacyjna, której przyczyną jest między innymi rozwój łączności satelitarnej i globalnej sieci internetowej. Możliwości utrzymywania stałego kontaktu pomiędzy ludźmi, dokonywania za pośrednictwem Internetu przelewów bankowych, zakupów - bez potrzeby wychodzenia z domu, muzyka i filmy oglądane z monitora komputera - wprowadziły w państwach o wyższym zaawansowaniu technicznym praktycznie nową jakość życia. Należy spodziewać się, i nie jest to wizja fantastów, że w niedługim czasie, w krajach reprezentujących nawet średni poziom zaawansowania w dziedzinie telekomunikacji, podstawowym, użytkowym sprzętem w domu będzie komputer działający w sieci Internetu.

Tak gwałtowny rozwój technik telekomunikacyjnych nie mógł zostać nie zauważony przez środowiska przestępcze, szczególnie te, które działają w sferze przestępczości gospodarczej. Sieci komputerowe, w których gromadzi się i przetwarza miliony danych są dziedziną szczególnie podatną na działalność przestępczą.

Przyczyny takiego stanu rzeczy są następujące:

- anonimowość działania, sprawca nie jest widziany przez swoje ofiary, co zapewnia mu znaczny komfort psychiczny,
- możliwość dokonania przestępstwa w jakimkolwiek miejscu na świecie, gdzie istnieje sieć internetowa, bez konieczności opuszczenia miejsca pobytu przestępcy,

- możliwość zdobycia ogromnych zasobów informacji i uzyskania dostępu do dokumentów, które w innych warunkach były by nieosiągalne,
- możliwość dosyć skutecznego zatarcia śladów przestępczej działalności,
- prowadzenie przestępczej działalności z kraju, na którego obszarze określona działalność jest dopuszczalna,

Szeroki zakres możliwości oddziaływania przestępczego na sieci informatyczne spowodował powołanie w latach osiemdziesiątych Komitetu Ekspertów ds. Przestępstw Komputerowych Rady Europy (the Select Committee of Experts on Computer - Related Crime of the Council of Europe), którego raport stał się podstawą rekomendacji nr R (89)9 Komitetu Ministrów Rady Europy i wskazał formy zachowań związanych z wykorzystaniem komputera i systemu komputerowego, które winny być skryminalizowane w systemach prawnych państw członkowskich. Zostały one skatalogowane w dwóch listach – pierwszej, tzw. minimalnej, która zawiera wykaz czynów wymagających kryminalizacji we wszystkich krajach członkowskich, a co za tym idzie ścisłej współpracy międzynarodowej, jednoznacznej ze zharmonizowaniem ustawodawstw krajowych w zakresie ścigania przestępczości transgranicznej oraz drugiej, tzw. fakultatywnej, która obejmuje zachowania o mniejszym stopniu szkodliwości i nie wymagające ścisłej współpracy międzynarodowej w zakresie ich ścigania.

Do najpoważniejszych przestępstw komputerowych Komitet Ekspertów Rady Europy zaliczył:

Oszustwo komputerowe

Przestępstwo to jest ubocznym skutkiem informatyzacji systemów bankowych i finansowo-księgowych, które coraz częściej opierają się na bezpapierowym obiegu dokumentów, teletransmisji danych i elektronicznym przelewie pieniądza. Celem działania przestępnego w takim przypadku jest nieuprawnione zdobycie środków finansowych.

Wskazana powyżej grupa przestępstw jest trudna do ścigania, gdyż wielokrotnie poszkodowany nie jest zainteresowany ujawnieniem słabości własnego systemu z uwagi na obawę utraty zaufania klientów.

Fałszerstwo komputerowe

Występuje ono w dwóch formach:

- jako komputerowe fałszerstwo dokumentów, w których komputer, oprogramowanie i urządzenia zewnętrzne (skaner, drukarka itp.) są narzędziem

do fałszowania dokumentów klasycznych;

- jako fałszerstwo dokumentów elektronicznych, polegające na wprowadzaniu zmian w dokumentach elektronicznych (księgi handlowe i podatkowe, ewidencje magazynowe, kartoteki pojazdów itp.) lub też w innych elektronicznych nośnikach informacji (np. zmiana zapisu na ścieżce magnetycznej karty płatniczej czy identyfikacyjnej).

Jest to przestępstwo, którego wykrycie jest wielokrotnie utrudnione, z powodu niezauważalnych zmian, których ujawnienie wymaga specyficznej wiedzy i narzędzi. Sam proces fałszowania, kopiowania czy skanowania dokumentów może być, przy wykorzystaniu zaawansowanych technologii, praktycznie niezauważalny. W polskich warunkach pewnym ograniczeniem możliwości fałszerza jest m.in. obowiązek przechowywania wydruków na nośniku papierowym z dokumentu elektronicznego (na potrzeby organów podatkowych i ZUS).

Nieuprawnione wejście (włamanie) do systemu komputerowego - hacking

Przestępstwo polega na wejściu do systemu po pokonaniu zabezpieczeń w postaci kodów i haseł broniących dostępu do zgromadzonej i przetwarzanej informacji. Penetrowanie przez hackerów systemów informatycznych za pośrednictwem połączeń telekomunikacyjnych jest zjawiskiem o zasięgu międzynarodowym i jednocześnie najczęściej występującym przestępstwem komputerowym. Samo wejście do systemu jest w ustawodawstwie większości krajów czynem przestępczym. Na ogół jest ono również podstawą do dokonania innych czynów przestępczych.

Polska Policja ujawniła sprawców szeregu prób i udanych przypadków włamań, zgłaszanych przez polskich administratorów sieci komputerowych, a także próby włamań do systemów komputerowych w Polsce z terenu USA i innych krajów.

Niszczenie danych lub programów komputerowych

Do niszczenia programów komputerowych i zbiorów danych wykorzystywane są programy destrukcyjne, jak np. wirusy komputerowe, konie trojańskie, bomby logiczne i robaki komputerowe.

Dla użytkowników systemów komputerowych różnice te mogą nie mieć znaczenia, jednakże z punktu widzenia kryminologicznego są istotne. W przypadku ujawnienia bomby logicznej lub konia trojańskiego bez uprzedniego zawirusowania systemu komputerowego sprawcy należy szukać wśród osób uprawnionych do dokonywania zmian w oprogramowaniu, natomiast krąg

sprawców wprowadzenia wirusa lub robaka komputerowego może być praktycznie nieograniczony.

Sabotaż komputerowy

Sabotażem komputerowym nazywamy uszkodzenie lub zniszczenie systemu komputerowego i informacji, którego celem jest sparaliżowanie funkcjonowania systemu komputerowego lub telekomunikacyjnego. Może być dokonany w efekcie celowego zawirusowania systemu komputerowego albo w wyniku lekkomyślności i zaniedbania pracowników, np. zaniechania procedur nadzorujących sieć komputerową (monitoringu) przez pracownika odpowiedzialnego. Bardzo często sabotaż połączony jest z szantażem komputerowym, gdzie sprawca w zamian za spełnienie jego warunków, najczęściej finansowych, gotów jest odstąpić od sparaliżowania systemu komputerowego w sobie tylko znany sposób.

W Polsce takie sytuacje miały miejsce w związku ze zwolnieniami z pracy administratorów zakładowych sieci (zemsta i wymuszenie zapłaty za „pomoc" w usunięciu zagrożenia).

Nieuprawnione przechwycenie informacji - podsłuch komputerowy

Współczesne techniki przechwytywania informacji są poważnym zagrożeniem dla systemów informatycznych. Dane komputerowe można bowiem przejmować zarówno z transmisji teleinformatycznych jak i w wyniku analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy (komputery, monitory, przewody itp.) oraz fal akustycznych generowanych przez drukarki. Przy czym działania te mogą być zdalne i nie pozostawiające żadnych śladów. Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych.

Nielegalne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych chronionych prawem autorskim (piractwo komputerowe)

Piractwem komputerowym jest kopiowanie, reprodukowanie, używanie i wprowadzanie do obrotu bez zezwolenia właściciela praw produktu programowego chronionego przez prawo autorskie. Dotyka ono wszystkich producentów oprogramowania, niezależnie od ich wielkości oraz w efekcie końcowym także użytkowników. Legalni producenci ponoszą bowiem ogromne

koszty tworzenia oprogramowania, jego testowania, promocji itp., które następnie wliczają w cenę gotowego produktu. Nielegalny producent ponosi jedynie koszty zakupu sprzętu i nośników, nie inwestując w rozwój programu i nie płacąc podatków.

Dodatkowym rodzajem przestępczości, tworzącym nową jakość w dziedzinie piractwa intelektualnego jest wykorzystanie sprzętu komputerowego do produkcji i powielania płyt CD z nagranymi utworami fonograficznymi, skompresowanymi w systemie MP3, MP4, oraz filmami w systemie MPEG czy SV CD, umożliwiającymi projekcję bez konieczności stosowania dosyć jeszcze kosztownego systemu DVD.

Do nielegalnego kopiowania filmów czy muzyki na płytach CD nie jest potrzebne specjalistyczne studio, wystarczy komputer i nagrywarka do CD. Małe wymiary krążków CD ułatwiają ich przechowywanie, transport i dystrybucję, a także nienaruszalność zapisu. Wartość surowca (płyty CD-R) jest niższa od wartości czystej kasety wideo. Wszystkie te elementy powodują, że zysk uzyskiwany ze sprzedaży nagranej pirackiej płyty z filmem czy muzyką jest znacznie wyższy od zysku ze sprzedaży tradycyjnej kasety wideo czy płyty muzycznej. Skompresowanie plików dźwiękowych umożliwia umieszczenie na jednej płycie CD-R do 10 godzin muzyki. Muzyka odtwarzana jest w komputerach lub specjalnych odtwarzaczach, produkowanych profesjonalnie przez znane firmy. Możliwość przesyłania plików muzycznych i filmów za pośrednictwem łączy telekomunikacyjnych jest początkiem końca giełd komputerowych, zapowiedzią przejścia piractwa intelektualnego do nowej formy działalności i nowym wyzwaniem dla organów ścigania i wymiaru sprawiedliwości.

W lutym ub. roku w wyniku działań policyjnych zabezpieczono automatyczną kopiarkę polskiej produkcji, pozwalającą na wyprodukowanie 60 szt. kopii dowolnego nośnika z płyty CD na płytach CD-R, bez potrzeby jakiejkolwiek kontroli.

Bezprawne kopiowanie topografii półprzewodników

Przez topografię półprzewodnika rozumie się rozwiązanie polegające na przestrzennym, wyrażonym w dowolny sposób rozplanowaniu elementów, z których co najmniej jeden jest elementem aktywnym. W tym przypadku chodzi również o ochronę praw autorskich i patentowych związanych z przestrzennym rozplanowaniem elementów i wszystkich lub części połączeń układu scalonego.

Na liście fakultatywnej Komitetu Ekspertów Rady Europy znalazły się:

Modyfikacja danych lub programów komputerowych

Szpiegostwo komputerowe

Używanie komputera bez zezwolenia

Międzynarodowa Organizacja Policji Kryminalnych "Interpol" przestępczość komputerową definiuje jako przestępczość z użyciem komputerów i zalicza do niej czyny wymienione w raporcie Komitetu Ekspertów Rady Europy, a nadto przesyłanie za pomocą sieci komputerowych materiałów pornograficznych i rasistowskich oraz używanie sieci komputerowych do celów komunikacyjnych przez zorganizowane grupy przestępcze.

2. Działania polskiej Policji przeciwko e - przestępczości

Polska Policja zajmuje się zjawiskiem przestępczości komputerowej oraz przestępstw dokonywanych przy wykorzystaniu najnowszych technologii od 1990 r. Oprócz przestępstw w dziedzinie informatyki, podjęto skuteczne działania zmierzające do ograniczenia naruszeń praw własności intelektualnej i znaków towarowych.

Od 1998 r. w polskiej Policji, w Wydziale ds. Przestępczości Gospodarczej Biura Koordynacji Służby Kryminalnej KGP funkcjonuje Zespół, którego zadaniem jest zwalczanie przestępczości komputerowej i intelektualnej oraz koordynacja wszelkich działań policyjnych, mających na celu ograniczenie tego rodzaju patologii. Zespół zajmuje się praktycznie wszystkimi rodzajami wyżej wymienionych przestępstw komputerowych, a ponadto przestępstwami popełnianymi na szkodę operatorów telefonii komórkowej i przewodowej.

W większości Komend Wojewódzkich Policji powstały wyspecjalizowane komórki, które zajmują się omawianą problematyką. Zakłada się że w niedługim czasie we wszystkich Komendach Wojewódzkich Policji i Komendach Miejskich Policji w byłych miastach wojewódzkich zaczną funkcjonować specjalne komórki zajmujące się tym zagadnieniem.

Wyniki ujawniania i zwalczania e – przestępczości, uzyskane przez Zespół i koordynowane jednostki terenowe Policji

Specyfika polskiego rynku teleinformatycznego, ilość firm i instytucji korzystających z sieci Internetu mają zasadniczy wpływ na ilość i rodzaje ujawnionych przestępstw, do dokonania których sprawcy wykorzystywali sprzęt informatyczny. Tylko w I połowie 2000 r. ujawniono przestępczą działalność i ustalono:

- 15 obywateli polskich, którzy na stronach WWW oferowali do zakupienie pirackie filmy i gry komputerowe,
- sprawców dokonania włamania do 72 serwerów na terenie miasta To-

runia,

- osobę zamieszczającą propozycje pedofilskie,
- dwie oferty sprzedaży narkotyków,
- 2 przypadki wyłudzenia pieniędzy za zamówione za pośrednictwem Internetu wyroby, których nigdy nie dostarczono,
- 12 przypadków rozpowszechniania w Internecie pornografii z udziałem nieletnich i zwierząt, z czego w 8 przypadkach informacje o ustalonych sprawcach przekazano za granicę, do krajów w których działali (USA, RFN, Izrael),
- właściciela kont pocztowych z których wysyłane były groźby karalne do prezydenta Stanów Zjednoczonych.

W przypadku ścigania zjawiska piractwa programów komputerowych wyniki uwidoczniają skalę tego zjawiska, które narasta w miarę rozwoju sieci Internetowej. Aktualny stopień zagrożenia tą przestępczością przedstawia poniższa tablica.

W 1994 r. podaż pirackich programów komputerowych wynosiła 99% ogólnej ilości wprowadzonych do obrotu i spadła do ok. 55-65% w 1999 r. Według ocen Bussines Software Alliance – organizacji reprezentującej interesy największych światowych producentów programów komputerowych zagrożenie na takim poziomie jest jednym z najniższych w Europie.

Tablica 1. Wyniki ujawniania i zwalczania przestępstw związanych z komputerami

	1994	1995	1996	1997	1998	1999	2000
Liczba wszczętych postępowań przygotowawczych	15	71	151	279	267	522	815
Ilość zabezpieczonych nośników informatycznych	151.500	17.260	14.879	30.364	87.947	111. 858	195.914

3. Problemy i zjawiska przestępcze według oceny Policji

Poważnym problemem stało się udostępnianie publicznie poprzez siec komputerową wzorcowych opisów, wręcz algorytmów postępowania przestępczego oraz programów komputerowych mogących służyć do celów przestępczych. Na różnego rodzaju publicznych, polskojęzycznych listach dyskusyjnych niejednokrotnie pojawiają się ogłoszenia o sprzedaży towarów i przedmiotów pochodzących z przestępstwa, o sposobie produkcji lub zaży-

wania narkotyków oraz sposobach działania mogącego powodować naruszanie prawa. Rozpoznawanie tych zjawisk odbywa się poprzez typowe działania policyjne, zwłaszcza współpracę z dużymi dostawcami usług internetowych.

Według oceny stanu zagrożenia oraz rodzajów przestępstw z jakimi Policja spotyka się na terenie naszego kraju, do najpoważniejszych problemów należą:

Pornografia i pedofilia w Internecie

Według badań statystycznych w Polsce obecnie jest około 2.000.000 stałych użytkowników sieci „Internet". Największą grupę użytkowników stanowią osoby w wieku 15-25 lat. Bardzo dużą grupę stanowią również dzieci do lat 15. Ze względu na specyfikę sieci „Internet" wszelkie treści znajdujące się w niej, dostępne są również dla tej najmłodszej grupy wiekowej. Treści, tak zdjęcia, jak i teksty oraz pliki video, propagujące przemoc i okrucieństwo są bardzo popularne i dostępne w sieci „Internet" bez ograniczeń. Jednakże ze względu na brak stosownych przepisów prawa penalizujących rozpowszechnianie tego typu treści, działania policji w tym zakresie muszą się ograniczać jedynie do monitorowania skali tego zjawiska.

Inaczej wygląda sytuacja z przestępstwami spenalizowanymi w polskich przepisach karnych, m.in. rozpowszechnianiem treści o charakterze pedofilskim. Dziedziny te są szeroko rozpoznawane oraz ścigane przez polską policję. Odnotowuje się stały wzrost ilości wszczętych postępowań przygotowawczych w takich sprawach. Jednakże podnoszenie się wiedzy informatycznej osób korzystających z Internetu w tym sprawców przestępstw, utrudnia w znacznym stopniu ich wykrywanie, ze względu na stosowanie coraz bardziej zaawansowanych technik ukrywania się.

Polskie przepisy prawne uniemożliwiają stosowanie technik operacyjnych powszechnie wykorzystywanych przez policje innych państw, w tym FBI w USA, w odniesieniu do ujawniania pedofilii, traktowanej jako bardzo poważne przestępstwo. Jest to po prostu prowokacja, polegająca na tym, że policjant udając np. ośmioletnią dziewczynkę odpowiada na oferty pedofilskie umieszczane w Internecie oraz poprzez sieć nawiązuje kontakt z konkretnym przestępcą. Zapisy zabezpieczone podczas tego kontaktu traktowane są w sądzie jako dowód.

Przestępstwa na szkodę bankowych systemów kart płatniczych

W chwili obecnej najbardziej rozwijającą się grupą fałszerstw są fałszerstwa kart płatniczych. Sczytywanie oryginalnych pasków magnetycznych (ang. skimming) i nanoszenie ich na inne karty stało się popularne wśród przestęp-

ców na przełomie 1997 i 1998 r. Podjęte wraz z pracownikami central rozliczeniowych działania policyjne przyniosły szereg pozytywnych rezultatów. W latach 1997 – 1999 zatrzymano w Polsce łącznie cztery grupy przestępcze dokonujące sczytywania pasków i nanoszenia danych na inne paski (KWP Poznań – 1 grupa, KSP – 3 grupy). Także i w tym przypadku stwierdzono działania międzynarodowe, czego przykładem może być zatrzymanie we Włoszech grupy przestępczej fałszującej paski magnetyczne, w składzie której byli obywatele polscy, a dane na pasek magnetyczny zbierane były w Polsce. Według danych pochodzących ze Związku Banków Polskich aktualnie w Polsce jest w obiegu ok. 4500 - 5000 szt. podrobionych, sfałszowanych i skradzionych kart płatniczych. Technologia fałszowania i podrabiania kart nie jest zbyt skomplikowana, a koszt niezbędnych do tego celu urządzeń (mieszczących się w średniej wielkości walizce) nie przekracza 4 - 5 tys. USD. Są to niewielkie koszty w porównaniu z nakładami na np. piracką produkcję fonografii - a zyski nieporównywalne, nie mówiąc o zagrożeniu ujawnienia działalności, jeżeli sprawca działa w obrębie bankomatów czy sklepów realizujących ten system opłat za usługi.

Działania na szkodę telekomunikacji

Coraz częściej zdarzają się przypadki kradzieży impulsów telefonicznych, dokonywane metodą przeprogramowania kart telefonicznych z 25 na 100 impulsów, lub nielegalnym „napełnianiem" kart wykorzystanych. Są one następnie wprowadzane do obrotu na targowiskach w dużych miastach lub środowiskach młodzieży szkolnej i studentów. Wysokość strat jakie ponosi TPSA jest praktycznie niemożliwa do oszacowania. Przedstawione zjawisko ma charakter narastający.

Włamania do systemów informatycznych

Problem włamań do systemów komputerowych wiąże się z koniecznością dostępu do informacji o takich zdarzeniach od poszkodowanych, jeżeli są oni zainteresowani ujawnieniem takiego przypadku (banki są raczej wstrzemięźliwe) i chcą ścigać sprawcę. Aktualnie – i jest tak również w innych krajach – policja informowana jest przez pokrzywdzonego o włamaniu do systemu jako ostatni organ, i to tylko w przypadku, gdy informatycy pokrzywdzonego nie mogą sobie sami dać rady z problemem, lub gdy wystąpiły tak duże straty, że sprawy nie da się ukryć. Nie ma tu możliwości działań prewencyjnych, czy operacyjnych. Policja jest powiadomiona o fakcie włamania do systemu lub nie - i nie ma na to wpływu. Polityka bezpieczeństwa sieci jest obszarem, gdzie

Policja może mieć jedynie rolę doradczą. W roku 1999 wszczęto w Polsce 2 sprawy o włamanie się do systemu informatycznego. W bieżącym roku do chwili obecnej uzyskaliśmy informacje od poszkodowanych o 3 włamaniach, w których ustalono ich sprawców. Ważnym czynnikiem wpływającym na skuteczność działania Zespołu jest jak najszybsze poinformowanie go o zaistniałym włamaniu i zabezpieczenie przez administratora systemu logów połączenia. Należy zakładać, że ten rodzaj przestępczości zajmie jedno z czołowych miejsc w e – przestępczości. Częste ugody podpisywane pomiędzy sprawcą i poszkodowanym są przyczyną marnotrawstwa pracy policji w związku z ujawnieniem hackera.

Zamieszczanie w Internecie niepożądanych treści (rasistowskich, obrażających godność, uczucia religijne itp.)

Od 1998 r. do chwili obecnej ujawniono jedynie kilka sporadycznych przypadków wygłaszania opinii rasistowskich na grupach dyskusyjnych, jednakże nie ujawniono stron WWW propagujących te opinie. Przykładem może być fakt, iż wśród ponad 9.000 stron o tematyce żydowskiej znajdujących się w zasobach polskiego Internetu, nie ujawniono dotychczas ani jednej propagującej treści antysemickie. Podyktowane może to być szeroko zakrojonymi działaniami prewencyjnymi, podjętymi przez pracowników Zespołu, w wyniku których nawiązano ścisłą współpracę z praktycznie wszystkimi większymi dostarczycielami usług Internetowych. W wyniku tej współpracy witryny WWW, zawierające treści niezgodne z etyką Internetową, są niezwłocznie usuwane a w przypadkach stwierdzenia naruszenia przepisów obowiązującego prawa zostają podjęte kroki zmierzające do ustalenia i ukarania sprawcy.

Powyższe działania spowodowały masowe przenoszenie stron WWW naruszających polskie przepisy na serwery znajdujące się poza granicami naszego kraju. W tych przypadkach ustalenia podejmowane są w oparciu o współpracę międzynarodową. Ze względu na specyfikę i rozległość sieci „Internet" nie można jednak stwierdzić, iż w polskich zasobach tej sieci w chwili obecnej nie ma ani jednej strony zawierającej treści rasistowskie czy obrażające określone grupy społeczne. Pracownicy Zespołu zwalczającego przestępczość komputerową są przygotowani aby w przypadku stwierdzenia tego typu nadużyć bezzwłocznie na nie zareagować i podjąć stosowne czynności wykrywcze. Przestępcy internetowi uaktywniają swoją działalność w tej dziedzinie w określonych sytuacjach, np. w okresie wyborów.

Problematyka ataków wirusami komputerowymi nie była dotychczas przedmiotem szczególnego zainteresowania polskich organów ścigania. Spowodowane jest to stosunkowo wysokim stopniem świadomości użytkowników systemów komputerowych. Globalizacja „Internetu" powoduje jednak stałe zagrożenie. Wirus „I love you" nie spowodował poważniejszych dylematów w polskich systemach komputerowych, poza poważnymi i dotkliwymi problemami u jednego z największych polskich operatorów sieci telefonii komórkowej - ERA GSM. Przyczyną takiego stanu rzeczy mogło być dość szybkie nagłośnienie zagrożenia wywoływanego przez tego wirusa we wszystkich polskich mediach. Poważnym jednak utrudnieniem są licznie pojawiające się makrowirusy dotykające oprogramowanie biurowe produkcji firmy „Microsoft". Według opinii producenta polskiego programu antywirusowego „MKS-vir" nastąpił także spadek powstawania polskich mutacji wirusów na rzecz wirusów przybywających do Polski z zagranicy.

Piractwo w Internecie

Aktualnie obserwuje się zalew stron WWW wszelkiego rodzaju pirackimi ofertami, dotyczących zarówno muzyki skompresowanej w plikach MP3, filmów w plikach MPEG i DVD oraz użytkowych programów komputerowych. Z uwagi na pewną pracochłonność ustalania sprawców, znikomą dolegliwość kar zasądzanych za tego rodzaju przestępczość oraz zyski jakie osiągają przestępcy, należy liczyć się z rozwojem tej dziedziny przestępczości.

O tym, że piractwem parają się nie tylko informatycy, czy też młodzież i studenci może świadczyć przykład sprawy koordynowanej przez Zespół:

- w maju 1999 r. roku Zespół ds. Przestępczości Komputerowej Wydziału ds. Przestępczości Gospodarczej Biura Koordynacji Służby Kryminalnej KGP uzyskał informację, z której wynikało, że na witrynie internetowej WWW znajduje się oferta sprzedaży pirackich kopii programów komputerowych. Jak wynikało z wykonanych wstępnych ustaleń, stworzona została przez nieznaną osobę z terenu województwa zachodnio-pomorskiego,
- zamówienia na oprogramowanie komputerowe realizowane były za pośrednictwem skrzynki poczty elektronicznej oraz skrytki pocztowej znajdującej się na poczcie w miejscowości Łask. Pirackie programy komputerowe na płytach CD rozsyłane były do zamawiających drogą pocztową,
- w ramach podjętych czynności operacyjno-wykrywczych ustalono firmę odpowiedzialną za serwer WWW, na którym umieszczona została strona internetowa jak również ustalono, iż właścicielem skrytki pocztowej jest Bogusław G. - lat 50, z wykształcenia rolnik, zameldowany w Szczecinie, lecz w

sław G. - lat 50, z wykształcenia rolnik, zameldowany w Szczecinie, lecz w miejscu zameldowania nie przebywający. Ponadto ustalono, iż posiada on dom w miejscowości Wygon k. Łaska, jak również, że z UPT w Łasku nadał 21 paczek opłaconych przekazem pocztowym,

- na podstawie analizy połączeń telefonicznych wykonanych z miejsca stałego zameldowania w/w ustalono faktyczny adres jego zamieszkania. Natomiast badanie bilingów połączeń telefonicznych zrealizowanych z tymczasowego miejsca pobytu pozwoliło na ustalenie, że w lokalu tym znajduje się komputer, z którego w ciągu doby wykonywanych jest kilkanaście połączeń z siecią Internet,
- porównanie okresów i czasów połączeń z Internetem, z ustalonymi czasami aktualizacji witryny WWW, potwierdziło, iż założono ją przy wykorzystaniu komputera znajdującego się w mieszkaniu, w którym przebywał figurant,
- w wyniku przeprowadzonej obserwacji rozpracowywanego, potwierdzono jego przestępczą działalność, polegającą na sprzedaży nielegalnie powielonych programów komputerowych na płytach CD,
- w oparciu o zgromadzony materiał dowodowy, wszczęto postępowanie przygotowawcze, a Prokurator Rejonowy w Szczecinie wydał nakazy przeszukania serwera i mieszkań, z którymi miał związek sprawca,
- realizację sprawy przeprowadzono przy udziale biegłego z Laboratorium Kryminalistycznego,
- podczas przeszukań ujawniono i zabezpieczono: puste pudełka zbiorcze po płytach CD, komputer, komputerowe nośniki informacji, zawartość skrzynki e-mail oraz pliki, które posłużyły do założenia strony WWW.W trakcie zatrzymania Bogusław G. złamał posiadane przy sobie dwie 3,5 calowe dyskietki,
- w urzędzie pocztowym, przed którym go zatrzymano ujawniono dowody nadania przez figuranta 29 paczek,
- prowadzący postępowanie przygotowawcze zlecił przesłuchania ustalonych odbiorców „pirackich'' programów właściwym terytorialnie jednostkom. Wszyscy dotychczas przesłuchani odbiorcy potwierdzili dokonanie zakupu nielegalnie zwielokrotnionych programów,
- powołany biegły potwierdził, że z zabezpieczonego u figuranta komputera dokonywano aktualizacji witryny zamieszczonej w internecie, jak również odzyskał 180 listów e-mail z jednej z uszkodzonych dyskietek.

Jest to tylko jeden z przykładów spraw koordynowanych i przekazanych przez Zespół do jednostek terenowych. Dotychczasowe doświadczenia wskazują, że w „polskim" internecie szczególnie rozpowszechnione jest zamieszczanie ofert sprzedaży nielegalnego oprogramowania, płyt oraz plików audio,

przedmiotów pochodzących z kradzieży (szczególnie telefonów komórkowych i radioodtwarzaczy samochodowych) oraz rozpowszechnianie pornografii dziecięcej oraz ze zwierzętami.

4. Wnioski

Przedstawione problemy nie obejmują całości spraw z jakimi spotykają się polskie organy ścigania. Dla poprawy skuteczności działania Policji w zwalczaniu e – przestępczości niezbędne byłoby rozpatrzenie możliwości wprowadzenia pewnych zmian w ramach ustaw określających zasady pracy firm świadczących usługi telekomunikacyjne i internetowe.

Niezbędne było by obligatoryjne nałożenie na firmy obowiązku zbierania, czasowego magazynowania i przekazywania Policji danych umożliwiających identyfikację sprawcy przestępstw dokonywanych przy użyciu ich serwerów. Stworzenie przepisów jednoznacznie określających obowiązki dostawców Internetu, usprawniło by w dużej mierze proces wykrywczy. Aktualnie podmioty świadczące usługi telekomunikacyjne w Polsce są zobowiązane do współpracy z organami ścigania w zakresie stosowania podsłuchu telekomunikacyjnego oraz wydawania w trybie art. 218 k.p.k. korespondencji elektronicznej. Jednak ze względu na niedostosowanie przepisów kodeksu postępowania karnego do nowych form przekazu informacji oraz luk prawnych, jakie ujawniają się na styku przepisów tego kodeksu z art. 49 Konstytucji i ustawą - Prawo telekomunikacyjne, sposób i zakres tej współpracy pozostawia w chwili obecnej wiele wątpliwości. Polskie przepisy prawne nie regulują okresów przechowywania zapisów dotyczących ruchu w sieciach teleinformatycznych, co wielokrotnie uniemożliwia odtworzenie przebiegu sesji i odnalezienie sprawcy przestępstwa. Logi systemowe gromadzone są (lub nie) w zależności od woli operatora lub dostarczyciela usług. Może to być czasem powodem problemów z jakimi Policja spotka się w swojej pracy.

Konieczna jest jednoznaczna interpretacja ustawy o ochronie danych osobowych. Obecnie wielokrotnie stosuje się nadinterpretację tej ustawy, co jest przyczyną opóźnienia lub niemożliwości wszczęcia postępowania przeciwko sprawcy e – przestępczości.

Należy zastanowić się nad stworzeniem przepisów związanych z zakresem odpowiedzialności firm za treści zamieszczane na ich serwerach.

Należy liczyć się ze wzrostem zagrożenia przestępczością komputerową proporcjonalnym do szybkości rozwoju globalnej sieci internetowej i jej wpływu na wszystkie dziedziny gospodarki.

Należy już teraz zastanowić się nad funkcjonowaniem ustawy o prawie autorskim i prawach pokrewnych, uwzględniając wpływ Internetu na możliwość egzekwowania ich przepisów i prawdopodobieństwo utraty realnych zysków twórców, których dzieła nieodpłatnie będą udostępniane w sieci.