POLSKA AKADEMIA NAUK * INSTYTUT NAUK PRAWNYCH

Zeszyt 4(170) 2006 STUDIA PRAWNICZE Warszawa 2007

PL ISSN 0039-3312

BARBARA ŚWIĄTKIEWICZ

OSZUSTWO KOMPUTEROWE – TECHNIKI DOCHODZENIOWE

Przestępstwo oszustwa komputerowego zostało wyodrębnione jako typ przestępstwa dopiero w kodeksie karnym z 1997 r.

Ustawowe znamiona tego przestępstwa opisane w art. 287 k.k. wyznaczają ramy tego artykułu.

Jest to przestępstwo skierowane przeciwko prawom majątkowym, których potwierdzeniem jest odpowiedni zapis w systemie gromadzonym, przetwarzającym lub przesyłającym automatycznie dane lub zapis na komputerowym nośniku informacji. Czynności sprawcze wymienione w tym przepisie mają charakter wyliczenia taksatywnego i poza przypadkami opisanymi przez ustawę może to przestępstwo być popełnione w innych formach. Liczba tego typu przestępstw wykrywanych przez policję rośnie.

W 1999 r. – 217 i w 2000 r. – 323, w 2001 r. – 279, w 2002 r. – 368, w 2003 r. – 168, w 2004 – 390, w 2005 – 568.

Najczęstszymi formami popełniania oszustwa komputerowego są:

- manipulacja danymi, polegająca na wprowadzeniu nieprawdziwych danych (najczęściej „martwych dusz") w celu uzyskania nienależnych korzyści majątkowych. Jest to najbardziej rozpowszechniona forma przestępstw pracowniczych, dokonywanych przeważnie przez operatorów, nie wymaga bowiem od sprawcy żadnej szczegółowej wiedzy lub umiejętności. Straty ponoszone przez instytucje w następstwie manipulacji danymi są większe niż na skutek innych rodzajów przestępczej działalności;
- manipulacja programem, tak aby program wykonywał określone czynności niezależnie od woli operatora. Jedną z odmian takich manipulacji jest metoda „salami", w której np. program bankowy przy rozliczaniu wkładów płatnych na każde żądanie samodzielnie dokonuje zmniejszania rachunku o minimalne kwoty i przekazuje je na uprzywilejowany rachunek sprawcy przestępstwa lub osoby przez niego wskazanej. Z uwagi na konieczność posiadania do realizacji tego przestępstwa specyficznej, fachowej wiedzy – sprawcy należy poszukać wśród twórców oprogramowania danej firmy, zatrudnionych informatyków lub włamywaczy komputerowych. Wśród policyjnych doświadczeń z tej dziedziny należy przypomnieć pierwszą sprawę z 1993 r., gdzie sprawca – pracownik banku – zainstalował program, który dokonywał automatycznego przelewu części odsetek z wybranych kont na jego prywatne konto;

– manipulacja urządzeniami wyjścia-wejścia, polegająca na wykorzystaniu ogólnie dostępnych peryferii komputerów i systemów w celu dokonania przestępstwa. Przykładem takich działań są przestępstwa dokonywane na szkodę banków i ich klientów za pomocą bankomatów, które są takimi terminalami[1].

Dość powszechne jest popełnianie oszustwa komputerowego za pomocą kart płatniczych.

Sczytywanie oryginalnych pasków magnetycznych (ang. *skimming)* i nanoszenie ich na inne karty stało się popularne wśród przestępców 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 grup międzynarodowych, czego przykładem może być zatrzymanie we Włoszech grupy przestępczej fałszującej paski magnetyczne, w której składzie byli obywatele polscy, a dane na pasek magnetyczny zbierane były w Polsce. Według danych pochodzących ze Związku Banków Polskich w Polsce może być 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 np. na 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[2].

Przestępstwo to może polegać także na nieupoważnionym posługiwaniu się danymi z karty przy zamówieniach pocztowych, telefonicznych lub za pomocą sieci komputerowych (z angielska nazywanych także transakcjami MO/TO/IO)[3]. Dane dla sprawcy mogą pochodzić z autentycznych kart, dowodów transakcji, generowania fałszywych numerów itp. Ten typ przestępstwa będzie nabierał coraz większego znaczenia, wraz z rozpowszechnianiem się tej formy dokonywania transakcji w Polsce. W aktualnym stanie prawnym nie stanowi przestępstwa:

– nieuprawnione zbieranie numerów kart płatniczych i przyporządkowanych im kodów identyfikacyjnych bez użycia urządzeń specjalnych (w rozumieniu art. 267 k.k.), np. poprzez podglądanie i ręczne zapisywanie,
– przechowywanie numerów kart płatniczych i przyporządkowanych im kodów identyfikacyjnych w przypadku braku możliwości udowodnienia przygotowania do fałszerstwa w rozumieniu art. 310 § 4 k.k.

[1] K.J. Jakubski, *Współpraca organów ścigania karnego, przestępczość, efektywność procesu wykrywania* – materiały poseminaryjne pod red. K. Zajdera i J. Świerczewskiego, WSPol, Szczytno 2003.

[2] K.J. Jakubski, op. cit.

[3] Problematykę tę szeroko opisał K.J. Jakubski, *Wyłudzenia towarów i usług na podstawie numerów kart kredytowych przez Internet*, w: R. Skubisz (red.), *Internet 2000: Prawo – ekonomia – kultura*, Lublin 1999, s. 249–285 i K.J. Jakubski, *Bezpieczeństwo transakcji handlowych dokonywanych kartą płatniczą w Internecie*, „It Security Magazine" 2000, nr 3 (4) cz. 1, nr 4 (5) cz. 2.

W efekcie w polskiej sieci komputerowej rozwinęła się wymiana, a nawet handel numerami kart płatniczych, które następnie wykorzystywane są do nieuprawnionych zdalnych transakcji.

Tabela 1. Podstawowe dane dotyczące rynku bankowych kart płatniczych[4]

	1997	1998	1999
Liczba kart (min)	2,036	3,766	8,171
Liczba bankomatów (szt.)	1430	2006	3420
Liczba transakcji bankomatowych (min)	25,53	40,326	102,63
Wartość transakcji bankomatowych (mld PLN)	4,5	5,162	22,47
Liczba punktów akceptujących karty płatnicze (tys.)	38,7	52,4	71,2
Liczba transakcji płatniczych (min)	5,1	11,5	25,85
Liczba transakcji płatniczych (min PLN)	1,35	2,6	5,2

Trudno w krótkim artykule omówić techniki dochodzeniowe stosowane przy ściganiu przestępców dokonujących oszustwa komputerowego. Jest to przestępstwo skierowane przeciwko obrotowi gospodarczemu. W związku z tym stosowane są przy jego wykrywaniu techniki charakterystyczne dla ścigania tego typu przestępstw, czyli obserwacja i analiza oraz synteza danych. Często przestępstwo to jest wykrywane przy okazji rozpracowywania innych przestępstw, a nawet przypadkowo, np. kamery filmujące operacje dokonywane w bankomatach, tzw. „przykrywki", często wykrywa się przy wymianie świetlówki. Jest to także przestępstwo przeciwko mieniu. Mają wówczas zastosowanie techniki dochodzeniowe charakterystyczne dla ścigania przestępstwa skutkowego, które jest zgłoszone przez pokrzywdzonego, np. takiego jak kradzież karty i dokonanie za jej pomocą zakupów. Zgłoszenie przez pokrzywdzonego powoduje zastosowanie technik dochodzeniowych polegających na ustaleniu (przez informacje z banku), kiedy i w jakim sklepie dokonano zakupu, oraz przesłuchaniu obsługi sklepu, ustaleniu rysopisu sprawców. Są to bardzo typowe działania dochodzeniowe i niestety stosunkowo rzadko skuteczne. Specyfika formy popełnienia przestępstwa oszustwa komputerowego powoduje, że poza tradycyjnymi formami wykrywczymi stosowanymi przy ściganiu przestępstw przeciwko mieniu i przestępstw gospodarczych konieczne jest wypracowanie nowych form działań policji.

Oszustwo komputerowe jest najczęściej popełnione za pomocą komputera, co sprawia, że występuje konieczność stosowania technik wykrywczych innych niż tradycyjne. Sprawca jest na ogół daleko od miejsca wystąpienia skutku, a ustalenie jego danych wymaga możliwości prześledzenia operacji w sieci, co niejedno-

[4] Niestety nie mogę zaktualizować tych danych, pod koniec 2003 r. liczba kart płatniczych wydanych indywidualnym klientom przez PKO BP wynosiła 4 587 000, Pekao SA 2 271 000, ING Bank Śląski – 1 351 000, BPHPBK – 1 231 000, BZWBK – 1 113 000, Kredyt Bank – 860 000, BGŻ – 471 000, Bank Millenium – 462 000, mBank – 386 000 i Lukas Bank – 224 000 /źródło www.nbp.pl/. Tendencja rosnąca w emisji zarówno kart płatniczych, jak i kredytowych i obciążających jest faktem oczywistym.

krotnie jest bardzo utrudnione. Policjanci w związku z tym postulują wprowadzenie zmian ustawodawczych określających zasady pracy firm świadczących usługi telekomunikacyjne i internetowe polegających na:

- Nałożeniu na firmy obowiązku zbierania, czasowego magazynowania i przekazywania policji danych umożliwiających identyfikację sprawcy przestępstw dokonywanych przy użyciu serwerów. Stworzenie przepisów jednoznacznie określających obowiązki dostawców Internetu, co dawałoby większe możliwości wykrycia sprawcy. Obecnie podmioty świadczące usługi telekomunikacyjne w Polsce zobowiązane są do współpracy z organami ścigania w zakresie stosowania podsłuchu telekomunikacyjnego oraz wydawania w trybie art. 218 k.p.k. korespondencji elektronicznej. Ze względu jednak 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 do życzenia. Polskie przepisy prawne nie regulują okresów przechowywania zapisów dotyczących ruchu w sieciach teleinformacyjnych, co wielokrotnie uniemożliwia odtworzenie przebiegu sesji i odnalezienie sprawcy przestępstwa. Logi systemowe gromadzone są (lub nie) w zależności od woli operatora lub dostarczyciela usług.
- Ustaleniu jednoznacznej interpretacji ustawy o ochronie danych osobowych. Obecnie wielokrotnie stosuje się nadinterpretację tej ustawy, co jest przyczyną opóźnienia lub niemożliwości wszczęcia postępowania przeciwko sprawcy.

Ściganie i wykrywanie przestępstw komputerowych wymaga, aby policjant już podczas pierwszych czynności uzyskał jak najwięcej informacji na temat zdarzenia. Są to w szczególności:

- Informacje o podmiocie pokrzywdzonym oraz o wiedzy, jaką dysponuje zgłaszający zdarzenie (często się zdarza, że zgłoszenia dokonuje pokrzywdzony lub osoba upoważniona do jego reprezentowania, która nie ma wiedzy z zakresu informatycznego i nie jest w stanie udzielić informacji niezbędnych w dalszej fazie postępowania). Wówczas policjant powinien ustalić i przesłuchać osobę zajmującą się bezpośrednio obsługą sieci w pokrzywdzonej firmie.
- Dane na temat rodzaju zdarzenia, czy jest to przykładowo włamanie na stronę internetową, kradzież danych z komputera, czy oszustwo.
- Informacje na temat zaatakowanego komputera (sieci), np. jakie są używane systemy operacyjne i oprogramowanie, rodzaj (jeżeli jest) sieci, liczba użytkowników komputera (sieci) i zakres dostępu, istniejące zabezpieczenia itd.
- W zależności od systemu komputerowego zabezpieczenie wszelkich informacji o logach systemowych, dokonywanych przez intruza zmianach w systemie itp. Dane te mogą ulec zniszczeniu poprzez kolejne działania sprawcy lub pokrzywdzonego.
- W przypadku dysponowania przez pokrzywdzonego wiedzą wystarczającą do określenia źródła ataku na system należy to zawrzeć w protokole przesłuchania.

Pokrzywdzony może w tym wypadku znacznie pomóc w procesie wykrywczym[5].

Problematyka ścigania włamań do systemów komputerowych wiąże się z koniecznością uzyskiwania informacji o takich zdarzeniach od poszkodowanych, jeżeli są oni zainteresowani ujawnieniem takiego przypadku. Praktyka wskazuje, że banki są w tym zakresie raczej wstrzemięźliwe. Obecnie policja jest informowana przez pokrzywdzonego o włamaniu do systemu jako ostatnia i to tylko wtedy, gdy informatycy pokrzywdzonego nie mogą sobie poradzić z problemem lub gdy wystąpiły tak duże straty, że sprawy nie da się ukryć. Powoduje to brak możliwości podjęcia działań prewencyjnych czy operacyjnych. Policja nie ma wpływu na to, czy zostanie powiadomiona o włamaniu do systemu czy nie. Polityka bezpieczeństwa sieci jest obszarem, gdzie policja ma jedynie rolę doradczą. W roku 1999 wszczęto w Polsce 2 sprawy o włamanie do systemu informatycznego, w 2000 r. w 3 sprawach udało się ustalić sprawców i to tylko dzięki informacjom uzyskanym od poszkodowanych. Aby policja mogła skutecznie ścigać sprawców oszustw komputerowych, powinna być jak najszybciej informowana o zaistniałym włamaniu, powinna natychmiast móc zabezpieczyć logi połączeń. Brak powiadomień, próby własnych dochodzeń, częste ugody podpisywane pomiędzy sprawcą i poszkodowanym negatywnie wpływają na skuteczność działań wykrywczych oszustw komputerowych. Brak pełnej informacji o sprawcach tych przestępstw ma wpływ także na ściganie tej przestępczości w ogóle, a nie tylko w konkretnych sprawach.

Polska policja zjawiskiem przestępczości komputerowej oraz przestępstw dokonywanych przy wykorzystaniu najnowszych technologii zajmuje się od 1990 r. Od 1998 r. działa w Wydziale ds. przestępczości Gospodarczej Biura Służby Kryminalnej KGP wyspecjalizowany 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 zajmujące się omawianą problematyką. Obecnie powstają takie komórki także w komendach miejskich i powiatowych.

Dodać należy, że w zakresie ścigania przestępstwa oszustwa komputerowego popełnianego za pomocą kart płatniczych znaczną rolę odgrywają techniki kryminalistyczne, których nawet pobieżne omówienie wymagałoby odrębnego referatu.

Konkluzja podsumowująca powyższe wywody nie napawa optymizmem. Polska policja ma świadomość dużego zagrożenia przestępczością oszustwa komputerowego i jednocześnie własnej bezsilności, wynikającej zarówno z uregulowań prawnych obowiązujących w Polsce, jak i postawy pokrzywdzonych.

[5] Por. J. Kosiński, *Przestępczość komputerowa w statystyce policyjnej*, w: T. Zasępa, R. Chmura (red.), *Internet i nowe technologie ku społeczeństwu przyszłości*, Łódź 2003.

THE COMPUTER CRIMES AND INVESTIGATION METHODS

The article is about basie detection principles used for work against Computer crimes, particularly crimes which used computers and credits cards. It shows also which changes in the legislation are necessary in the opinion of Polish Police.