POLSKA AKADEMIA NAUK * INSTYTUT NAUK PRAWNYCH

Zeszyt 4(170) 2006 STUDIA PRAWNICZE Warszawa 2007

PL ISSN 0039-3312

RYSZARD A. STEFAŃSKI

OSZUSTWA KOMPUTEROWE W PRAKTYCE POLSKICH ORGANÓW ŚCIGANIA

I. WPROWADZENIE

Analizą zostały objęte sprawy z całego kraju o oszustwa komputerowe (art. 287 k.k.), w których postępowania przygotowawcze zostały zakończone w 2002 r. i w I półroczu 2003 r. Wyboru spraw dokonali prokuratorzy rejonowi i okręgowi, do których kompetencji należy prowadzenie postępowań przygotowawczych lub nadzór nad dochodzeniami prowadzonymi w tych sprawach przez policję.

W ten sposób wyselekcjonowano 64 sprawy. Są to prawie wszystkie sprawy, które zostały zakończone w prokuraturach. Dane liczbowe – podawane niżej – dotyczą spraw, a nie przestępstw, gdyż lepiej obrazują one analizowane zjawisko, w wielu sprawach bowiem sprawcy dopuszczali się przestępstw, działając czynem ciągłym, działając tym samym sposobem i w związku z tym liczba faktycznie popełnionych czynów jest znacznie większa, obejmując niekiedy kilkadziesiąt czynów. Na przykład w jednej ze spraw sprawca zmienił zapisy komputerowe dotyczące 71 faktur (sprawa PR Szczecin-Zachód nr 6 Ds. 114/01), a w innej – 24 (sprawa PR w Lubinie nr 3 Ds. 1297/02).

Nie analizowano kar, gdyż wyroki zapadły w nielicznych sprawach, co – ze względu na małą liczbę spraw – uniemożliwiłoby wyciągnięcie poprawnych wniosków. Wskazać tylko można, że w 2001 r. polskie sądy skazały za przestępstwo oszustwa komputerowego (art. 287 § 1 i 2 k.k.) 29 osób, w tym na karę pozbawienia wolności – 24, karę ograniczenia wolności – 3, grzywnę – 2, a w stosunku do 2 osób postępowanie zostało warunkowo umorzone. Tylko 1 osoba została skazana na bezwzględną karę pozbawienia wolności.

II. RODZAJE ZACHOWAŃ PRZESTĘPNYCH

Sprawcy dopuszczali się różnorodnych zachowań przestępnych, a generalnie ich głównym celem było osiągnięcie korzyści majątkowej. Działania przestępne polegały na:

1) wystawianiu fikcyjnych faktur i fałszowaniu dokumentów księgowych – 10,
2) zmianie zapisów na rachunkach bankowych lub w innych dokumentach bankowych – 9,
3) przekonfigurowaniu połączenia z Internetem – 8,

4) usunięciu danych informatycznych – 6,
5) dokonywaniu zakupów przy użyciu numerów kart płatniczych innych osób – 3,
6) zniszczeniu strony internetowej – 3,
7) zmianie kodu dostępu – 3,
8) zakupie towarów po założeniu skrzynki pocztowej – 2,
9) uszkodzeniu danych lub oprogramowania – 2,
10) wprowadzeniu nowych zapisów – 2,
11) fałszowaniu kart telefonicznych – 2,
12) użyciu karty płatniczej w bankomacie – 2,
13) wprowadzeniu nieprawdziwych danych co do wykonanej pracy – 2,
14) zablokowaniu dostępu do stron na serwerze – 1,
15) podłączeniu się do sieci internetowej – 1,
16) zamówieniu za pomocą Internetu karty płatniczej na fałszywe nazwisko – 1,
17) zainstalowaniu wirusa Trojan – 1,
18) fałszowaniu liczników paliwa – 1,
19) używaniu zastrzeżonych kodów i haseł – 1,
20) kradzieży impulsów telefonicznych – 1.

Fałszowanie danych na komputerowym nośniku informacji polegało głównie na zmienianiu zapisanych danych po to, by przywłaszczyć towary lub pieniądze, np. fałszowano faktury i inne dokumenty finansowe (sprawa PR w Brodnicy nr Ds. 1657/01, PR w Lublińcu nr Ds. 205/02, PR w Ostrowcu Świętokrzyskim nr 1 Ds. 316/03, PR Poznań Nowe Miasto nr 1 Ds. 5448/02, PR Szczecin-Zachód nr 6 Ds. 114/01, PR Warszawa-Mokotów nr 5 Ds. 1068/02/IV i nr 5 Ds 722/02/IV, PR w Lubinie nr 5 Ds. 438/01).

Zmiany danych w dokumentach bankowych stanowiły *modus operandi* wyłudzania pieniędzy od banków przez ich pracowników i polegały one na:
- podwyższaniu na komputerowym nośniku informacji limitu odnawialnego kredytu (sprawy PR w Kętrzynie nr Ds. 86/03, PR w Płocku nr 2 Ds. 1121/02),
- wprowadzaniu na nośnikach informacji fikcyjnych transakcji i kierowaniu środków finansowych na własne konto lub osoby najbliższej (sprawy PR w Katowicach-Wschód nr 1 Ds. 616/02/W, PR w Sulęcinie nr Ds. 1043/02, PR w Płocku nr 2 Ds. 1121/02, PR w Grodzisku Maz. nr 2 Ds. 1670/02),
- dokonywaniu przelewu pieniędzy na inne konta (sprawa PO w Poznaniu ośrodek w Koninie nr V Ds. 41/02),
- zwolnieniu blokady konta (sprawa PR w Płocku nr 2 Ds. 1121/02),
- przedłużeniu terminu spłaty kredytu (sprawa PR w Płocku nr 2 Ds. 1121/02),
- zarejestrowaniu fikcyjnej umowy kredytu bankowego (sprawa PR w Wałbrzychu nr 2 Ds. 146/03/4).

Sprawy dotyczące przekonfigurowania połączenia z Internetem były wszczynane z doniesień osób posiadających dostęp do Internetu za pośrednictwem łączy TP S.A. o zmianie ustawienia numeru dostępnego do Internetu na droższy numer komercyjny. Z ustaleń postępowań wynika, że nie jest możliwe korzystanie

w tym trybie z programów, z reguły erotycznych, bez wyrażenia zgody przez naciśnięcie odpowiedniego polecenia. Sprawy te zostały zakończone umorzeniem postępowania z powodu braku ustawowych znamion czynu zabronionego (np. sprawy PR w Lesznie nr Ds. 625/03, PR w Piasecznie nr 1 Ds. 634/01/YIII, PR Warszawa Praga-Południe nr 3 Ds. 492/03).

Usunięcia danych informatycznych dotyczyły różnych informacji o odmiennym znaczeniu, np. w jednej ze spraw usunięto zbiór biblioteczny (sprawa PR w Gorzowie Wlkp. Nr 1 Ds. 1063/03),

Numery kart płatniczych innych osób lub kart fikcyjnych wykorzystywano do dokonywania opłat za połączenia z firmami oferującymi programy erotyczne (np. w sprawie PR w Szczytnie nr Ds. 568/03).

Usunięcie hasła dostępu do konta internetowego miało na celu wprowadzenie w to miejsce własnego konta i wykorzystywanie go do fikcyjnego oferowania do sprzedaży w ramach licytacji internetowej różnych towarów (sprawa PR w Wodzisławiu Śląskim nr 2 Ds. 222/03).

Zainstalowanie wirusa podyktowane było chęcią wydłużenia czasu korzystania z komputera w kawiarence internetowej (sprawa PR w Nysie nr 1 Ds. 6/02).

Większość spraw dotyczyła przestępstw o niezbyt dużym ciężarze. Wyjątek stanowią:

- sprawa, w której sprawcy, działając w zorganizowanej grupie przestępczej, składającej się z obywateli Polski i Litwy, założyli spółkę na nieprawdziwe nazwisko i w jej pomieszczeniach zainstalowali terminale elektroniczne POS, wprowadzając do nich transakcje obciążające konta posiadaczy kart płatniczych wystawionych przez banki zagraniczne oraz przesyłając je za pośrednictwem linii telekomunikacyjnych do transmisji w Centrum Rozliczeniowym „PolCardu", w wyniku czego przeprowadzili 90 transakcji, wyłudzając kwotę ponad 540 tys. zł (sprawa PO w Szczecinie nr V Ds. 2/03/ Sp).
- sprawa uruchamiania impulsów telefonicznych na komercyjne numery telefoniczne wydzierżawione przez sprawców od providerów TP S.A. na szkodę różnych instytucji (sprawa PO w Warszawie nr V Ds. 33/01).

Analiza ta wskazuje, że zamachy na zapisy na komputerowym nośniku informacji służyły przede wszystkim do przywłaszczania lub wyłudzania pieniędzy. Wskazuje na to stosunkowo duża liczba spraw o oszustwo komputerowe polegające na wystawianiu fikcyjnych faktur i fałszowaniu dokumentów księgowych oraz na fałszowaniu zapisów na rachunkach bankowych lub w innych dokumentach banku; stanowią one 29,6% badanych spraw, w tym w sektorze bankowym 14,0%. W sprawach tych zachowanie sprawców wyczerpywało znamiona przestępstwa przywłaszczenia (art. 284 § 1 k.k.) lub oszustwa zwykłego (art. 286 § 1 k.k.), a zmiany danych na komputerowym nośniku informacji były środkiem do osiągnięcia celu, jakim było przywłaszczenie gotówki. W takim też celu działali sprawcy kradzieży kwoty ponad 63 tys. zł pochodzącej ze sprzedanej benzyny na stacji benzynowej, którą zabrali, cofając liczniki dystrybutorów paliwa; w tym wypadku zachowania te zmierzały do ukrycia faktu kradzieży (sprawa PR w Ciechanowie nr 1 Ds. 1494/02). Do uzyskania wyższego wynagrodzenia za

pracę zmierzało wprowadzenie do bazy komputerowej nieprawdziwych danych o wykonanej pracy (sprawa PR w Wałbrzychu nr 1 Ds. 4253/01/1).

III. SPOSÓB ZAKOŃCZENIA POSTĘPOWAŃ

Analiza sposobów zakończenia postępowań przygotowawczych wskazuje na stosunkowo niską efektywność ścigania przestępstw oszustwa komputerowego. Na ogólną liczbę 64 spraw:

a) akty oskarżenia skierowano w 25 (39,0%) sprawach,

b) wnioski o warunkowe umorzenie postępowania w 4 (6,2%),

c) umorzono postępowania w 33 (51,6%), w tym z powodu niewykrycia sprawcy – 15 (23,4%), braku ustawowych znamion czynu zabronionego – 19 (29,7%), brak wniosku – 1 (1,5%),

d) zawieszono postępowanie w 2 (3,1%).

Stosunkowo duża jest liczba spraw umorzonych z powodu niewykrycia sprawców. Wiąże się to głównie z tym, że sprawcy korzystają z tzw. kawiarenek internetowych, w których nie jest prowadzona ewidencja korzystających z nich, jak i z poszczególnych komputerów, oraz nie ma możliwości ich monitorowania z serwera właściciela kawiarenki. Przykładem może być sprawa założenia skrzynki pocztowej na portalu internetowym Wirtualnej Polski na określoną osobę i zamawianie bez jej wiedzy różnych towarów (sprawa PR w Inowrocławiu nr 1 Ds. 984/02).

IV. WNIOSKI

Przeprowadzona analiza wykazała, że zamieszczanie danych na elektronicznych nośnikach informacji, których celem jest ułatwienie posługiwania się nimi, w tym wykonywanie pracy, jest wykorzystywane przez nieuczciwych pracowników jako środek do popełniania pospolitych przestępstw, zwłaszcza przywłaszczeń. Korzystanie z elektronicznych nośników informacji, zwłaszcza z Internetu, jest skutecznym środkiem do popełniania oszustw, a to głównie dlatego, że daje sprawcy gwarancję, że nie zostanie wykryty, zwłaszcza gdy korzysta z dostępu do Internetu w klubach lub kawiarenkach internetowych, gdzie nie rejestruje się osób korzystających z komputerów.

DEPUTY OF THE GENERAL PROSECUTOR COMPUTER FRAUD IN THE PRACTICE OF THE POLISH INYESTIGATION ORGANS

The analysis referred to 64 Polish cases of Computer fraud (Art. 287 of the PC) in which the preliminary proceedings were terminated in 2002 and first half of 2003. Relatively great number of cases consisted in issuing false invoices and falsifying accounting documents as well as falsifying bank accounts records and

other bank documents. Attacks on records on the Computer information carrier mainly served to appropriate and embezzle money. In these cases the behaviour of perpetrator fulfilled the features of the offence of misappropriation (Art. 284 § 1 of the PC) or common fraud (Art. 286 § 1 of the PC), and changes of data made on Computer information carrier constituted a means to reach the purpose, i.e. appropriation of money.