Rafał Kania, Adam Kotfasiński, Marcin Piotrowski

Zagrożenie przestępczością komputerową

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 4, 139-144

2010

Rafaģ KANIA
Adam KOTFASIÓSKI
Marcin PIOTROWSKI

ZAGROŁENIE PRZESTĘPCZOŚCIĄ KOMPUTEROWĄ

Streszczenie

W zakresie sugerowanych zmian w przepisach karnych, to autor postuluje zupeģnie odrębne uregulowanie w Kodeksie karnym przestępstw popeģnianych z wykorzystaniem elektronicznych instrumentów płatniczych. Wyzwaniem dla ustawodawcy jest takie sformuģowanie norm prawa karnego, aby nie pozwalały na wątpliwości interpretacyjne w zakresie podstawowych pojęć (tak jak to obecnie występuje np. jeżeli chodzi o pojęcie „karty płatniczej"). Kodeks karny nie wymienia karty płatniczej czy rachunku obciążeniowego jako przedmiotów czynności wykonawczej, lecz zalicza je do takich dóbr prawnych jak: mienie, dokument, dokument upoważniający do otrzymania sumy pieniężnej, środek płatniczy, kredyt czy nośnik informacji. Przepisy polskiego prawa karnego nie w peģni zabezpieczają ochronę obrotu z wykorzystaniem elektronicznych instrumentów płatniczych. Karta płatnicza stanowi bowiem specyficzny przedmiot ochrony, a realizowanie jej w ramach ujęcia syntetycznego może prowadzić do chwiejności i niejednolitości dokonywanych w praktyce kwalifikacji prawnych i wątpliwości, czy w ogóle w danym przypadku karta płatnicza i mechanizm zapłaty kartą są przedmiotem ochrony prawnej.

Summary – THE THREAT OF COMPUTER CRIMINALITY

The author postulates changes in criminal law. She suggests separate regulations in the Penal Code, in the field of crimes committed with the use of electronic payment devices. The challenge for the legislator is creating such norms of criminal law, which will not allow any ambiguities with respect to interpretation of the basic terms. This is nowadays the case with, for example, the term `payment cards`. The Penal Code does not see a payment card or a debiting account as subjects of enforcement , but includes them in such legal interests as property, documents, documents entitling to receiving an amount of money, currency, credit, or information carrier. The regulations of Polish criminal law do not fully ensure the safety of circulation with the use of electronic payment devices. A payment card requires special protection. Its synthetic realization may lead to instability and heterogeneity of the legal qualifications applied in practice, or even doubts, whether or not a payment card and transactions with its use are subjects to legal protection.

Wirusy, robaki internetowe, konie trojańskie, oszustwa związane z kartami kredytowymi i pranie brudnych pieniędzy - zagrożenia tego typu rozprzestrzeniają się wprost lawinowo, stanowiąc realne zagrożenie dla prawidģowego kształtowania się społeczeństwa informatycznego: zagrożenie dla bezpieczeństwa instytucji rządowych i finansowych, bezpiecznego obrotu gospodarczego. Według doniesień mediów opierających się na statystykach i danych policyjnych zdecydowana większość grup przestępczych szuka w sieci miejsca do rozwoju swojej działalności opanowując stopniowo Internet .Jak wynika z danych Komendy Gģównej Policji, w 2009 roku policja dostawała średnio 20 zgģoszeń dziennie o popeģnieniu cyber-

przestępstwa. Łącznie było ich 6351. To o ponad 30 proc. więcej niż rok wcześniej. W przypadku 2,2 tys. tych spraw policjantom udało się wszcząć postępowanie. To ponad dwa razy więcej takich przypadków niż w 2008 r. Cyberprzestępcy wyspecjalizowali się szczególnie w oszustwach i wyłudzaniu informacji. Taki proceder nazywa się fachowo phishingiem. Ataki pishingowe przeżyli w ub.r. klienci m.in. Allior Banku, Banku Zachodniego, WBK i Lukas Banku oraz telewizji kablowej UPC. Coraz częściej przestępstwa internetowe dotykają sprzedających i kupujących w sieci. Cyberprzestępcy, szczególnie w USA ,dokonują także na szeroką skalę manipulacji w urządzeniach odczytu kart płatniczych umieszczonych w automatach na stacjach benzynowych, aby w ten sposób wykradać dane o kartach. Do tej pory głównie tego typu ataki były stosowane raczej w przypadku bankomatów, w których przestępcy za pomocą nakładek do tzw. skimmingu umieszczanych przed otworem do umieszczania kart pobierali dane z pasków magnetycznych, aby następnie tworzyć kopie. Kody PIN były wykradane za pomocą ukrytych kamer albo specjalnych, dodatkowych nakładek na klawiatury bankomatów przykrywających właściwe pola z klawiszami. W nowo zaobserwowanych przypadkach urządzenia do skimmingu umieszczone na terminalach kolumn paliwowych za pośrednictwem łączy Bluetooth wysyłały dane do przestępców, ukrytych w okolicy. Ci z użyciem podrobionych kart mogli następnie pobierać gotówkę z automatów. Na chwilę obecną brak jest doniesień o tego typu atakach w naszym kraju, jednak prawdopodobieństwo ich się pojawienia w niedługim czasie wydaje się być bardzo wysokie. Stąd też szczególnie dużo uwagi wymaga badanie przedmiotowej problematyki, opracowywanie systemów zabezpieczeń i regulacji prawnych i gotowych do walki z tego typu przestępczością i gwarantujących bezpieczeństwo rozwoju społeczeństwa informatycznego.

Elektroniczne instrumenty płatnicze w polskim prawie karnym

Przepisy polskiego prawa karnego nie w pełni zabezpieczają ochronę obrotu z wykorzystaniem elektronicznych instrumentów płatniczych. Karta płatnicza stanowi bowiem specyficzny przedmiot ochrony, a realizowanie jej w ramach ujęcia syntetycznego może prowadzić do chwiejności i niejednolitości dokonywanych w praktyce kwalifikacji prawnych i wątpliwości, czy w ogóle w danym przypadku karta płatnicza i mechanizm zapłaty kartą są przedmiotem ochrony prawnej.

Kodeks karny nie wymienia karty płatniczej czy rachunku obciążeniowego jako przedmiotów czynności wykonawczej, lecz zalicza je do takich dóbr prawnych jak: mienie, dokument, dokument upoważniający do otrzymania sumy pieniężnej, środek płatniczy, kredyt czy nośnik informacji. Jednocześnie fundamentalna zasada prawa karnego „nullum crimen nulla poena sine lege poenali anteriora" bezwzględnie zakazuje analogii, zwłaszcza wykładni rozszerzającej. Z kolei ochrona systemu finansowego i bankowego oraz ochrona zaufania do systemu rozliczeń wymaga szczególnego potraktowania karty płatniczej. Obrót za pomocą kart płatniczych stanowi bowiem część składową obrotu gospodarczego, a zamach na środki tego obrotu pośrednio godzi w obrót gospodarczy, uderzając dotkliwie szerokie masy społeczeństwa i odbijając się na procesach gospodarczych.[1]

[1] Por. uchwała Sądu Najwyższego z dnia 29 czerwca 1972 roku, w sprawie III KR 105/72, OSNK w 1972, Nr 12, poz. 194

Jedynym miejscem w prawie karnym, gdzie odniesiono siń do elektronicznych instrumentów pğatniczych jest wprowadzony w rozdziale XXXV kodeksu karnego obejmujŃcym przestńpstwa przeciwko mieniu, w art. 278 § 5 k.k.,[2] penalizacji kradzieŻy karty uprawniajŃcej do podjńcia pieniŕdzy z bankomatu, jako odrńbnego typu przestńpstwa kradzieŻy. Motywów wyodrńbnienia tego przestńpstwa nie okreŚlono w uzasadnieniu projektu juŻ jednak w tak kategoryczny sposób, poprzestajŃc na stwierdzeniu, Że podobnie jak energiń potraktowano kradzieŻ karty magnetycznej sğuŻŃcej do pobierania gotówki z automatu bankowego, której nie moŻna porównaŕ z kradzieŻŃ ksiŃŻeczki oszczńdnoŚciowej.[3] Na uregulowanie to zareagowano w piŚmiennictwie zarówno zdziwieniem, Że w kodeksie zapewniono szczególna ochronń przed kradzieŻŃ, poprzez odrńbnŃ typizacjń, jednej tylko z odmian funkcjonujŃcych w obrocie gospodarczym kart, stosunkowo najmniej uŻytecznej,[4] jak i obawŃ aby celu tej regulacji nie przekreŚliğa zasada tzw. przepoğowienia kradzieŻy.[5] Zapis ten wywoğuje takŻe powaŻne trudnoŚci interpretacyjne. W odróŻnieniu od innych przedmiotów materialnych speğniajŃcych kryterium mienia (art. 44 k.c.), wartoŚci majŃtkowej karty pğatniczej nie moŻna utoŻsamiajŃc z kosztami jej wytworzenia. WiŃŻe siń ona bowiem z jej funkcjŃ i tkwi w zapisie znajdujŃcej siń na karcie informacji, która umoŻliwia dokonywanie zakupu dóbr i usğug bez potrzeby posğugiwania siń w tym celu gotówkŃ. Z chwilŃ wprowadzenia do obrotu pieniŕdza elektronicznego, wartoŚŕ majŃtkowa kart mikroprocesorowych bńdŃcych noŚnikiem Ąelektronicznej gotówkiò stanie siń jeszcze bardziej oczywista i wymierna, skoro w Ąelektronicznej portmonetceò nie bńdzie mogğo znajdowaŕ siń wiŕcej pieniŕdzy niŻ równowartoŚŕ w zğotych 150 euro.[6] ŚciganiePrzywğaszczenia karty spotka siń juŻ z niewŃtpliwym zarzutem analogii niedozwolonej w prawie karnym materialnym.[7]

W piŚmiennictwie wyraŻany jest poglŃd, Że przedmiotem czynnoŚci wykonawczej przestńpstwa fağszowania pieniŕdzy i innych Ąrodków pğatniczych (art. 310 k.k.) nie moŻe byŕ karta bankomatowa, gdyŻ nie speğnia ona funkcji Ąrodka pğatniczego, o którym mowa w tym przepisie.[8] Interpretacja jeszcze dalej idŃca w tym kierunku, cağkowicie wyklucza moŻliwoŚŕ stosowania art. 310 k.k., jako podstawy kwalifikacji prawnej fağszerstw kart pğatniczych z tego powodu, Że definicja legalna Ąrodków pğatniczychò, jakŃ posğuguje siń ustawa prawo dewizowe (art. 2 ust. 1) nie zalicza (ze zrozumiağych skŃdinŃd powodów) kart pğatniczych do desygnatów tego pojńcia.[9]

InteresujŃca w tym kontekŚcie jest takŻe uchwağa peğnego skğadu Izby Karnej SŃdu NajwyŻszego z dnia 25 czerwca 1980 roku VII KZP 48/78, która pobranie

---

[2] Ustawa z dnia 06 czerwca 1997 roku Kodeks karny art. 278 § 5 (Dz. U. z 1997, Nr 88, poz. 553, z póŹn. zmianami)

[3] Nowe kodeksy karne z 1997 roku z uzasadnieniami. Wyd. Prawnicze. Warszawa 1997, s. 206

[4] B. Michalskiò Przestńpstwa przeciwko mieniu. Rozdz. XXXV Kodeksu karnego. Komentarz. Seria: Komentarze Karne Becka, CH Beck. Warszawa 1999, s. 79

[5] O. Górniok, S. Hoc, S.M. Przyjemski: Kodeks Karny, Komentarz, t. III, GdaŃsk 2001, s. 355

[6] Art. 58 ustawy z dnia 5 lipca 2002 roku o elektronicznych instrumentach pğatniczych

[7] S. Ğagodziński, Kontrowersje wokóğprzywğaszczenia (art. 284 k.k.), ĄProkuratura i Prawoò 2001, Nr 2

[8] J. Skorupka, Karta pğatnicza jako przedmiot czynnoŚci wykonawczej przestńpstwa z art. 310 § 1 k.k., ĄProkuratura i Prawoò 2001, nr 7-8; tenŻe Karnoprawna ochrona wierzycieli. ToruŃ 2001, s. 204

[9] Uchwağa SŃdu NajwyŻszego z dnia 30 wrzeŚnia 1998 roku, w sprawie I KZP 3/98, OSNKW 1998, Nr 9-10, poz. 41)

pieniędzy z bankomatu przy użyciu prawidłowego kodu identyfikacyjnego zakwalifikowania jako kradzież z włamaniem.

Propozycje nowych rozwiązań i zmian legislacyjnych

Gospodarka globalna spowodowała pojawienie się nieznanych wcześniej zagrożeń. Zbyt często normy dotyczące ryzyka są dla wielu zarządów banków tylko listkiem figowym, a sam management nie zdaje sobie sprawy ze skali rozwoju cyberprzestępców. Świadomość ich istnienia wymaga stałego monitorowania systemów informatycznych w tej sytuacji pomocna dla kadry zarządzającej jest norma ISO 27005, która pomaga szacować ryzyka wynikające z niedostosowania lub zawodności transakcji bankowych przez zawodne systemy informatyczne, niefrasobliwość pracowników, błędy popełniane przez samych klientów banków. Dlatego system informatyczny banku musi mieć dostęp do informacji o pojawiających się ryzykach z innych branż. Najważniejsze w transakcji elektronicznej są procesy identyfikacji klienta.. dlatego bezpieczny identyfikator to główny problem transakcji elektronicznych. Aktualnie klienci banków zmuszeni są do zapamiętania około 20 identyfikatorów i minimum 2 haseł. Wynika to z faktu, że każdy bank stosuje inne identyfikatory zaprojektowane według własnych kryteriów i form identyfikacji klienta. Według normy ISO 21001 ŕ silne hasła do konta powinny być zmieniane co 30 dni, ale jest to nierealne, bo tego nie robią klienci banków. Dlatego lepszym rozwiązaniem są ŕmocne hasła ważne nawet przez 90 dni. I tu pojawia się główny problem, tj. brak jednolitego standardu wymiany informacji o bezpieczeństwie pomiędzy bankami. Płaci za to klient, który nie wie, co może, a czego mu nie wolno wpisywać do internetowych formularzy ze stron banków. Najczęściej stosowaną techniką do wyłudzania haseł jest phising. Na szczęście dość często jego słabością jest fatalna polszczyzna, spowodowana używaniem automatycznych translatorów z języka angielskiego. Ale statystyki pokazują, że cyberzłodzieje są wykazują coraz większe zainteresowanie naszym krajem. W dodatku przygotowane przez nich fałszywe formularze są coraz lepsze i trudne do wykrycia. Tymczasem banki nie zawsze wymieniają pomiędzy sobą informacje o takich atakach. Zbyt często ich klienci pozostawieni są samym sobie. Banki nie informują, jaki jest standard ich stron WWW, nie instruują na przykład jak korzystać z przeglądarek internetowych. Banki powinny edukować klienta o takich zagrożeniach i stworzyć do tego celu specjalna bazę danych. Tam, gdzie jest masowy klient transakcji elektronicznych , podstawowym problemem jest identyfikacja i uwierzytelnianie autoryzacji transakcji. Żaden z banków jednak nie wyda pieniędzy na biznes dający 100 % proc bezpieczeństwo. Jest to zbyt drogie, a przy masowym kliencie dodatkowo mało realne: system stawiałby przed nim zbyt duże wymagania, a zawsze najsłabszym ogniwem transakcji na odległość jest sam klient systemy bezpieczeństwa banków tworzą własne zasady, w konsekwencji rośnie portfel tożsamości elektronicznej. Jednak nikt nie wie jakie są standardy , a sami klienci nie maja świadomości, jak się tam przedstawiają. Tożsamość elektroniczna jest dodatkiem do usługi narzuconym przez bank internetowy.[10]

Błędem administracji rządowej jest z uporem od lat lansowany pomysł, aby podpis elektroniczny służył tylko do kontaktów z urzędami. Tymczasem chodzi o to,

[10] S. Brzeg-Wieluński, „Klient najsłabszym ogniwem", „Banki", Miesięcznik finansowy, Nr 3 (209) 2010, s. 90-92

Ůeby korzystaţ z niego nie tylko 250 tys. przedsiľbiorców, których paĆstwo zmusiţ do takiego kontaktowania siľ z ZUS-em. Tymczasem podpis elektroniczny ma wiele konkretnych zalet: jest uniwersalny, daje moŮliwoŚci nawiĹzania bezpiecznych relacji na odlegţoŚĺ. Ma tez atut trans graniczny w relacjach z UE. Np. pomaga w zaţatwieniu spraw w ojczyŹnie Polakom mieszkajĹcym na Wyspach Brytyjskich. W innych krajach unijnych nie ma debat, czy e-podpis jest zţy, czy dobry. Takie rozwiĹzanie dziaţa nawet w Chile. Jest duŮe zainteresowanie e-podpisem ze strony sţuŮby zdrowia. Wprowadzenie tej formy autoryzacji znacznie poprawiţby bezpieczeĆstwo równieŮ transakcji bankowych. Jednak w tym celu niezbľdne sĹ zmiany w przepisach regulujĹcych stosowanie podpisu elektronicznego, w szczególnoŚci rozszerzenie moŮliwoŚci posţugiwania siľ nim w innych niŮ tylko kontakt przedsiľbiorców z urzľdami, sferach aktywnoŚci obywateli.

JednakŮe najprostszym i najskuteczniejszym pomysţem na w zrost bezpieczeĆstwa transakcji elektronicznych jest tzw. biometria. Klient nie musi pamiľtaĺ hasţa, moŮe dokonaĺ autoryzacji transakcji gţosem, przez odcisk palca lub skanowanie soczewki oka. Ale najlepszym rozwiĹzaniem jest skanowanie naczyĆ krwionoŚnych . to skuteczne rozwiĹzanie, bo wiele osób ma nieczytelne linie papilarne. Pamiľtaĺ jednak naleŮy, Ůe jest moŮliwa kradzieŮ danych biometrycznych z sejfów banków. Klienci banków w związku z tym boja siľ, Ůe ktoŚ moŮe wykorzystaĺ ich palec lub siatkówkľ oka do kradzieŮy pieniľdzy z konta. Dlatego teŮ biometria musi byĺ wspomagana przez kryptograficzne certyfikaty.

Biometryczne uwierzytelnianie transakcji sprawia, Ůe kradzieŮ karty lub danych z karty staje siľ bezcelowa. Zabezpieczenie takie moŮna stosowaĺ np. w przypadku uŮycia nowoczesnych multiaplikacyjnych kart z chipem (MULTOS). Pobrany przez bankomat skan biometryczny porównywany jest wówczas przez kartľ z zapisanym na niej wzorcem. KradzieŮ tego rodzaju informacji, jak i nieautoryzowane jej uŮycie jest niemoŮliwe, gdyŮ obraz ten przechowywany jest w zaszyfrowanej formie. Poza tym jest on sam z siebie bezuŮyteczny ď stanowi jedynie materiaţ porównawczy.

Poza wymienionych modelem porównawczym skanów biometrycznych na karcie (match on card) moŮe siľ ono odbyĺ na samym czytniku (match on device). W tej sytuacji zaszyfrowany wzór biometryczny pobierany jest z serwera, po uprzedniej rejestracji klienta w banku. Nastľpnie porównywany jest ze skanem pobranym przez bankomat podczas transakcji. JeŚli oba skany pasujĹ do siebie, wypţata dochodzi do skutku. Taki model wykorzystany zostanie do wypţat zasiţków społecznych z bankomatu. Technologia biometrycznego uwierzytelniania transakcji umoŮliwia równieŮ realizacjľ wypţat z bankomatu bez uŮycia karty w trybie off-line (bez udziału hosta autoryzacyjnego). W tym celu wykorzystywany jest bezpoŚrednio interfejs systemu bankowego, dziľki czemu transakcje ksiľgowane sĹ na rachunku on ď line.[11]

Bank decydujĹc siľ na wdroŮenie biometrycznego uwierzytelniania transakcji, zwiľkszy swojĹ innowacyjnoŚĺ w sensie marketingowym i procesowym. NajwiľkszĹ zaletĹ takiego systemu jest znaczne zwiľkszenie bezpieczeĆstwa transakcji bankomatowych (spadek liczby nieautoryzowanych transakcji).

[11] J. Koszel, „Biometryczne uwierzytelnianie transakcji w technologii Finger Vein", „Bank", Miesiľcznik finansowy, Nr 3 (209) 2010, s. 93

Zakresie sugerowanych zmian w przepisach karnych, to autor postuluje zupełnie odrębne uregulowanie w Kodeksie karnym przestępstw popełnianych z wykorzystaniem elektronicznych instrumentów płatniczych. Wyzwaniem dla ustawodawcy jest takie sformułowanie norm prawa karnego, aby nie pozwalały na wątpliwości interpretacyjne w zakresie podstawowych pojęć (tak jak to obecnie występuje np. jeżeli chodzi o pojęcie „karty płatniczej). Kodeks karny nie wymienia karty płatniczej czy rachunku obciążeniowego jako przedmiotów czynności wykonawczej, lecz zalicza je do takich dóbr prawnych jak: mienie, dokument, dokument uprawniający do otrzymania sumy pieniężnej, środek płatniczy, kredyt czy nośnik informacji. Przepisy polskiego prawa karnego nie w pełni zabezpieczają ochronę obrotu z wykorzystaniem elektronicznych instrumentów płatniczych. Karta płatnicza stanowi bowiem specyficzny przedmiot ochrony, a realizowanie jej w ramach ujęcia syntetycznego może prowadzić do chwiejności i niejednolitości dokonywanych w praktyce kwalifikacji prawnych i wątpliwości, czy w ogóle w danym przypadku karta płatnicza i mechanizm zapłaty kartą są przedmiotem ochrony prawnej.