Katarzyna Ciulkin-Sarnocińska[1]

Phishing – specyficzna forma pozyskiwania danych newralgicznych

W dobie powszechnej potęgi informatyzacji i rozwoju technologicznego, przestępstwa cybernetyczne są stawiane na równi z szeroko pojętym terroryzmem. Stają się one poważnym zagrożeniem nie tylko dla osób fizycznych czy prawnych, ale także zagrażają bezpieczeństwu całego państwa. Pomysłowość cyberterrorystów doprowadziła do powstania przestępstw dotąd nieznanych. Skala zagrożenia wzbudziła w ludziach realne obawy o to, że ich dobra, tj. poufne dane, dobra materialne oraz osobiste, mające dla nich najwyższą wartość, zostaną skradzione.

Zgodnie z najnowszymi badaniami przeprowadzonymi przez APWG[2] (*Anti Pee Wee Gaskins*) w trzecim kwartale 2013 roku, aż 31,88% komputerów z całego świata stało się celem cybernetycznego ataku. Chiny znalazły się na szczycie listy, osiągając 59,36%. Drugim w kolejności państwem jest Turcja (46,58%), następnie Peru (42,55%). Europa ma najniższe wskaźniki infekcji, jednakże w Polsce wskaźnik jest najwyższy, osiąga aż 35,45%. Dla porównania w Holandii wynosi on 19,19%, w Wielkiej Brytanii – 20,35%, w Niemczech – 20,60%. Australia znajduje się na 9. miejscu krajów o najniższej ilości zainfekowanych komputerów (26,67%). Niewiele więcej zainfekowanych komputerów mają: Japonia (26,84%), Wenezuela (27,82%), Kolumbia (29,14%), Stany Zjednoczone (30,58%) i Meksyk (31,49%).

Zgodnie z Raportem Norton 2013[3] (dawniej *Norton Cybercrime Report*) pomimo optymistycznych danych wskazujących, że spadła liczba dorosłych internautów padających ofiarą cyberprzestępców, to średni koszt ataku przypadający na ofiarę wzrósł o 50%. Obrazując skalę problemu w Polsce, należy zauważyć, iż w ciągu ostatnich 12 miesięcy ok. 6 mln Polaków padło ofiarą cyberprzestępców. W tym czasie koszt związany z działalnością przestępców internetowych wyniósł 6 mld zł.

Rozmiar przestępstw komputerowych doprowadził do konieczności wprowadzenia regulacji prawnych we wszystkich państwach. W polskim prawodawstwie, w celu zapewnienia bezpieczeństwa przetwarzania informacji w Internecie, wprowadzono liczne uregulowania w ustawach, m.in. w:

1 Uniwersytet w Białymstoku.

2 Phishing Activity Trends Report, 3rd Quarter 2013, APWG.

3 Norton Cybercrime Report, wrzesień 2012 r., s. 6, tekst dostępny pod adresem: http://www.norton.com/2012cybercrimereport (20.03.2014).

- kodeksie karnym[4],
- ustawie o ochronie danych osobowych[5],
- ustawie o ochronie informacji niejawnych[6],
- ustawie o dostępie do informacji publicznej[7],
- ustawie o prawie autorskim i prawach pokrewnych[8],
- ustawie o świadczeniu usług drogą elektroniczną[9].

Aktualnie cyberterroryzm nie sprowadza się tylko do umieszczenia złośliwego oprogramowania, które niszczy system, powodując miliardowe straty w gospodarce prywatnych przedsiębiorstw i instytucji państwowych. Przestępcy komputerowi (hackerzy, crackerzy, phisherzy) stają się coraz bardziej wyrafinowani, obierając za cel banki na całym świecie, w celu osiągnięcia korzyści majątkowej. Każdego roku w Polsce odnotowuje się coraz więcej kradzieży z internetowych kont bankowych. Przestępstwo to nosi nazwę phishing i polega na wyłudzaniu haseł do internetowych kont bankowych, PIN-ów kart kredytowych oraz okradaniu ich z pieniędzy właściciela. Przestępca w celu złamania haseł posługuje się techniką wyłudzania danych osobowych, które w wyniku jego działania, dzięki odpowiednio spreparowanym stronom internetowym, są dobrowolnie podawane przez oszukiwanych. Phisher podszywa się pod znaną poszkodowanemu instytucję, nie ujawniając własnej tożsamości. Działanie to wypełnia znamiona przestępstwa z art. 190a § 2 kk.

Najczęstszym celem phisherów są banki oraz aukcje internetowe. Zgodnie z policyjnymi danymi informacje zawarte w systemie informatycznym są najczęściej pozyskiwane w następujący sposób[10]:

- rozsyłanie sfałszowanych wiadomości e-mail, „udających" komunikaty z działu bezpieczeństwa bankowości elektronicznej, administratorów serwerów poczty elektronicznej lub serwisów aukcyjnych, z prośbą o przesłanie PIN-ów, haseł lub kodów jednorazowych w celu weryfikacji poprawności działania serwisu po np. pracach konserwacyjnych na serwerze,
- rozsyłanie fałszywych wiadomości e-mail z odnośnikami (linkami) do spreparowanej strony WWW e-banku, serwisu płatności elektronicznej, serwera poczty elektronicznej lub serwisu aukcyjnego,

4 Kodeks karny z dnia 6 czerwca 1997 r. (Dz.U. Nr 88, poz. 553, sprost.: Dz.U. z 1997 r. Nr 128, poz. 840).

5 Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883), t.j. z dnia 17 czerwca 2002 r. (Dz.U. Nr 101, poz. 926).

6 Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz.U. Nr 182, poz. 1228).

7 Ustawa o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz.U. Nr 112, poz. 1198).

8 Ustawa o prawie autorskim i prawach pokrewnych, z dnia 4 lutego 1994 r. (Dz.U. Nr 24, poz. 83), t.j. z dnia 1 sierpnia 2000 r. (Dz.U. Nr 80, poz. 904), t.j. z dnia 17 maja 2006 r. (Dz.U. Nr 90, poz. 631).

9 Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz.U. Nr 144, poz. 1204), t.j. z dnia 15 października 2013 r. (Dz.U. z 2013 r., poz. 1422).

10 Ochrona informatyczna danych – „Phishing" i kradzież tożsamości, Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Kryminalnego Komendy Głównej Policji, tekst dostępny pod adresem: http://www.policja.pl (20.04.2014).

- rozsyłanie złośliwego oprogramowania komputerowego (konie trojańskie, programy typu keylogger[11], oprogramowania szpiegujące spyware[12]),
- zmiany adresu IP (*Internet Protocol*) przedmiotowej strony na serwerze DNS i przekierowanie ruchu sieciowego na inny serwer, na którym „postawiono" wcześniej spreparowaną fałszywą stronę, np. banku,
- zmienianie pliku HOSTS[13] znajdującego się na komputerze ofiary, który jest odpowiedzialny za interpretację adresów IP i przypisanych im nazw domenowych.

Częstą praktyką cyberprzestępców jest rozsyłanie pocztą elektroniczną fałszywych wiadomości mających na celu imitację oficjalnych informacji z instytucji finansowych o dezaktywacji konta i konieczności ponownej jego aktywacji, np.:

- „Zanotowaliśmy próby logowania na Pańskie konto, prosimy o zalogowanie się w celu weryfikacji tożsamości".
- „Zostałeś wybrany spośród grupy klientów do wypełnienia krótkiej ankiety. W podziękowaniu za Twój czas przekażemy na Twoje konto 5$".

W styczniu 2004 roku phisherzy rozesłali następującą wiadomość e-mail: „Drogi Kliencie, z przyjemnością informujemy, iż zakończyliśmy prace nad zintegrowanym serwisem bankowości internetowej. Wkrótce nowa platforma zastąpi obecny system, ale już teraz zachęcamy Cię do zapoznania się z możliwościami i udogodnieniami, jakie oferuje zintegrowany serwis. Prosimy o jak najszybsze zalogowanie się oraz sprawdzenie naszego nowego systemu. Zaloguj się http://www.online.citibank.pl". Witryna z wyglądu przypominała prawdziwą stronę internetową. Logując się na stronie internetowej banku, poszkodowani zostali przekierowani na fałszywą stronę stworzoną przez hackera. Ofiarami narażonymi na ataki cyberprzestępców są przede wszystkim osoby, które odwiedzają strony internetowe o określonych treściach (m.in. strony o tematyce porno, serwery FTP[14] z zasobami zawierającymi nielegalne oprogramowanie). Najczęściej to sama ofiara nieświadomie, z braku wiedzy, ściąga na swój komputer szkodliwe oprogramowanie.

Z pojęciem phishingu wiąże się również kradzież tożsamości, jako podstawowy aspekt naruszenia bezpieczeństwa danych informatycznych. Polega na podjęciu

11 Programy te działają na zasadzie przejęcia kontroli nad procedurami systemu operacyjnego służącymi do obsługi klawiatury. Każde wciśnięcie klawisza jest odnotowywane w specjalnym pliku. Opcjonalnie informacje o wciśniętych klawiszach poszerzone są o dodatkowe informacje, jak nazwa aktywnego programu lub okna. Funkcje chroniące przed ich wykryciem uniemożliwiają niedoświadczonej osobie wykrycie keyloggerów.

12 Programy te gromadzą informacje o użytkowniku i wysyłają je bez jego wiedzy i zgody autorowi programu.

13 Plik hosts jest jednym z modułów systemów operacyjnych, który wspomaga adresowanie w sieciach komputerowych. Jego zadaniem jest tłumaczenie przyjaznych użytkownikom nazw domenowych na ich numeryczne odpowiedniki (adresami IP), które identyfikują dany komputer w sieci.

14 FTP – serwer umożliwiający wymianę plików z odległymi komputerami za pomocą protokołu komunikacyjnego FTP.

czynności zmierzających do pozyskania prawdziwych danych realnie istniejących osób oraz ich wykorzystanie do popełniania innych przestępstw. Czyn zabroniony jest dokonywany przy użyciu środków technicznych, teleinformatycznych oraz socjotechnicznych w sposób niezgodny z obowiązującym prawem, w celu osiągnięcia korzyści majątkowej lub naruszenia dóbr osobistych[15]. Pojęcie danych osobowych na gruncie prawa polskiego jest zdefiniowane w ustawie o ochronie danych osobowych. Dane osobowe są „wszelkimi informacjami dotyczącymi zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przy czym osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne". Odpowiedzialność karną osoby dopuszczającej się kradzieży tożsamości reguluje kodeks karny w art. 190a § 2, który stanowi, że karze pozbawienia wolności do lat 3 podlega ten, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

Kradzież tożsamości może poprzedzać popełnienie przestępstwa oszustwa komputerowego uregulowanego w art. 287 kk., którego potrzeba wprowadzenia została uargumentowana tym, iż współcześnie pojęcie oszustwa tradycyjnego z art. 286 kk. jest niewystarczające. W myśl art. 287 kk. kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Powyższe przestępstwo można określić mianem manipulacji danymi informatycznymi w zakresie praw majątkowych[16]. Ustawodawca przy tworzeniu tego przepisu wzorował się na art. 8 Konwencji o cyberprzestępczości[17] z 23 listopada 2001 roku. Legalna definicja pojęcia danych informatycznych jest uregulowana w art. 1b Konwencji o cyberprzestępczości jako „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie informatycznym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"[18].

Artykuł 287 kk. chroni również informatyczne systemy przetwarzania, gromadzenia i przesyłania danych związanych z prawami majątkowymi oraz integralność,

15 Zgodnie z Komunikatem Komisji Wspólnot Europejskich „W kierunku ogólnej strategii zwalczania cyberprzestępczości" z 22 maja 2007, kradzież tożsamości jest definiowana jako „wykorzystywanie identyfikujących danych personalnych jako narzędzia do popełnienia innych przestępstw".

16 A. Grześkowiak (red.), *Komentarz do art. 287 KK*, Legalis.

17 Council of Europe. European Treaty Series – No. 185, tekst dostępny pod adresem: http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf (20.03.2014).

18 Council of Europe. European Treaty Series – No. 185, art. 1b: „computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

poufność i dostępność tych danych[19]. Przestępstwo może zostać popełnione na dwa sposoby. Po pierwsze sprawca wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Stanowi to ingerencję w funkcje wykonywane przez system informatyczny. Natomiast w drugim przypadku sprawca zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, co stanowi ingerencję w zapisane dane informatyczne. W obu przypadkach mamy do czynienia z przestępstwem, jeśli sprawca działa bez wcześniejszego pozwolenia osoby uprawnionej. Ustawodawca uznał, iż zabronione jest każde działanie ze strony sprawcy, które wpływa na przebieg danych informatycznych[20]. Do wypełnienia znamion przestępstwa z art. 287 kk. wystarczy samo naruszenie zabezpieczenia danych informatycznych. W tym konkretnym przypadku jego czyn zostanie uznany za czyn współukarany uprzedni lub czyn ciągły. Sprawca czynu oddziałuje na urządzenie będące częścią systemu informatycznego funkcjonującego automatycznie lub na nośniku danych informatycznych. Zgodnie z utrwalonym orzecznictwem nie ma znaczenia, czy w wyniku przestępstwa powstanie szkoda i czy sprawca będzie miał zamiar przywłaszczenia danych informatycznych. Sąd Apelacyjny w Szczecinie w wyroku z dnia 14 października 2008 roku, II AKa 120/08[21] orzekł, iż: „Przestępstwo z art. 287 § 1 kk., dokonane jest już z chwilą wprowadzenia zmian lub innej opisanej w tym przepisie ingerencji w urządzenie lub system do gromadzenia, przetwarzania lub przesyłania informacji za pomocą techniki komputerowej. Efektywna szkoda nie należy zatem do jego znamion". Dane personalne ofiar, numery kart płatniczych, daty ich ważności oraz numery weryfikujące CVV (*Card Verification Number*) pozyskane w powyższy sposób pozwalają hackerom na dokonywanie elektronicznych transakcji finansowych bez wiedzy osoby uprawnionej.

Naruszenie prawa może przybrać formę ataku zmasowanego, polegającego na uzyskiwaniu danych poprzez wprowadzenie w błąd co do autentyczności portali internetowych. W efekcie tego dochodzi do wprowadzenia w błąd użytkowników co do autentyczności źródła wiadomości elektronicznych przekierowujących lub nakłaniających do odwiedzania fałszywych stron internetowych, a także uzyskiwania danych poprzez dokonywanie przekierowań automatycznych na fałszywe strony dzięki zmianom na serwerach DNS, system nazw domenowych (*Domain Name System*).

Ponadto naruszenie prawa może mieć również charakter ataku kierunkowego, polegającego na uzyskaniu informacji poprzez włamanie ukierunkowane na konkretną osobę, która wcześniej była obserwowana i podsłuchiwana. Przestępstwo to zostało uregulowane w art. 267 § 1 kk., który stanowi, że kto bez uprawnie-

19 Council of Europe. European Treaty Series – No. 185, art. 1a: „computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

20 M. Kulik, [w:] R. Zawłocki (red.), *System Prawa Karnego*, t. IX, *Przestępstwa przeciwko mieniu i gospodarcze*, Warszawa 2011, s. 334-335.

21 Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r. II AKa 120/08 OSA 2010 nr 12, poz. 57, s. 3, Legalis, KZS 2011, nr 2, poz. 55.

nia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega także ten, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Karze podlega również osoba, która w celu uzyskania informacji, do której nie jest uprawniona, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Penalizowane jest też ujawnienie innej osobie informacji uzyskanej w powyżej opisany sposób[22].

Celem powstania treści przepisu jest zabezpieczenie informacji przed dostępem ze strony osób nieuprawnionych. Przepis koreluje z art. 49 Konstytucji RP[23] i stanowi gwarancję zachowania wolności i ochrony tajemnicy komunikowania się. Przestępstwo polega na uzyskaniu dostępu do informacji nieprzeznaczonej dla sprawcy. Aktualne brzmienie przepisu pozwala na przypisanie odpowiedzialności karnej nie tylko, gdy sprawca zapoznał się z nią, lecz także gdy przejmuje władztwo nad nośnikiem informacji. Przełamanie albo ominięcie zabezpieczeń oznacza uzyskanie dostępu do treści chronionych. Znamię uzyskania dostępu do systemu informatycznego[24] może obejmować zarówno część, jak całość systemu.

Ustawa o ochronie informacji niejawnych w art. 2 pkt 6 zawiera odniesienie do legalnej definicji systemu informatycznego z art. 2 pkt 3 ustawy o świadczeniu usług drogą elektroniczną – jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy – Prawo telekomunikacyjne[25]. Za Włodzimierzem Wróblem należy przyjąć, że urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym jest wyłącznie takie urządzenie, które jest przysposobione do uzyskiwania informacji „w warunkach uniemożliwiających zapoznanie się z tą informacją przez osoby postronne"[26]. Sąd Najwyższy Izba Karna w wyroku z dnia 2 czerwca 2003 roku II KK 232/02[27] uznał, że „co prawda przepis art. 267 § 1 kk. nie zawiera charakterystycznego zwrotu, który redukowałby w stronie pod-

22 A. Grześkowiak (red.), *Komentarz do art. 267 KK*, Legalis.

23 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483) art. 49: Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

24 Definicja legalna systemu informatycznego jest uregulowana w art. 7 ustawy o ochronie danych osobowych, określając go jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

25 Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (Dz.U. Nr 171, poz. 1800), t.j. z dnia 10 stycznia 2014 r. (Dz.U. z 2014 r., poz. 243).

26 W. Wróbel, [w:] A. Zoll (red.), *Kodeks*, t. II, Kraków 2006, s. 1285-1286.

27 Wyrok Sądu Najwyższego z dnia 2 czerwca 2003 r. II KK 232/02, OSNwSK 2003 nr 1, Legalis.

miotowej umyślność do zamiaru bezpośredniego, to jednak cała konstrukcja tego typu przestępstwa, a w szczególności znamię czasownikowe »uzyskuje« i znamiona określające bliżej sposób owego uzyskania, eliminują w istocie możliwość popełnienia tego występku w zamiarze wynikowym".

W związku z walką z cyberprzestępczością instytucje finansowe wprowadziły następujące zabezpieczenia:

- listę haseł jednorazowych (np. mBank, Inteligo, Multibank),
- jednorazowe hasła SMS (BZ WBK S.A., mBank, Millennium Bank),
- token (np. BZ WBK S.A., Volkswagen Bank direct, BGŻ S.A., Lukas Bank S.A.),
- podpis cyfrowy (np. Bank BPH S.A., ING Bank Śląski S.A.),
- dodatkowe hasło (np. Kredyt Bank S.A.).

Na stronie internetowej poświęconej walce z phishingiem – *Anti-phishing Working Group*, znajduje się ostrzeżenie, aby z nieufnością traktować każdą wiadomość, w której żąda się podania poufnych informacji dotyczących finansów. Jeśli wiadomość nie została opatrzona elektronicznym podpisem, nie można być pewnym, czy faktycznie pochodzi ona od nadawcy widniejącego w nagłówku. Phisherzy zazwyczaj straszą jakimiś konsekwencjami, próbując wymóc na ofierze natychmiastową reakcję i domagają się osobistych informacji. Wiadomości mają z reguły charakter bezosobowy, podczas gdy większość informacji pochodzących z banków ma charakter spersonalizowany. *Anti-phishing Working Group*[28] przypomina o tym, aby nie używać linków zamieszczonych w wiadomościach e-mailowych.

Przed atakami hackerów można ustrzec się, nie logując się na strony banków przez podejrzane wiadomości e-mail i nie podając swych szczegółowych danych. Adres strony internetowej instytucji bankowej należy wpisać samodzielnie. Ważne jest, by przy łączeniu się z wirtualną bankowością nie korzystać z ogólnodostępnych komputerów, np. w kafejkach internetowych. Ponadto należy odpowiednio zabezpieczyć przed wirusami swój własny komputer programami antywirusowymi. Dodatkowo można zwrócić uwagę, czy strona internetowa instytucji bankowej jest zabezpieczona protokołem SSL (*Secure Socket Layer*). Bezpieczne strony korzystają z bezpiecznego połączenia, o którym świadczy symbol zamkniętej kłódki w przeglądarce i https:// w pasku adresu. Dzięki nowelizacji prawa karnego i wprowadzeniu przepisów dotyczących oszustwa komputerowego mamy realne instrumenty, którymi możemy posłużyć się w walce z hackerami. Każde uzasadnione podejrzenie co do fałszywej strony internetowej należy zgłosić Policji lub prokuraturze oraz pracownikom instytucji finansowych, pod którą podszywają się przestępcy. Istnieje również możliwość zgłoszenia przestępstwa na wspomnianej stronie internetowej instytu-

28 Oficjalna strona internetowa *Anti-phishing Working Group*, informacje dostępne pod adresem: http://www.antiphishing.org (10.03.2014).

cji poświęconej walce z cyberprzestępczością, *Anti-phishing Working Group*. Stosując się do powyższych zaleceń, można ustrzec się przed potencjalnymi atakami cyberprzestępców oraz uniemożliwić atak hackerów na przyszłość.

Literatura

Adamski A., *Przestępstwa komputerowe w nowym kodeksie karnym. Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze*, zeszyt 17. Ministerstwo Sprawiedliwości, Departament Kadr i Szkolenia, Warszawa 1998.

Grześkowiak A. (red.), *Komentarz do art. 287 KK*, Legalis.

Grześkowiak A. (red.), *Komentarz do art. 267 KK*, Legalis.

Phishing Activity Trends Report, Anti-Phishing Working Group, February 2006.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, 2010.

Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji, Biuro Bezpieczeństwa Narodowego, Warszawa 2009.

Źródła prawa

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883) t.j. z dnia 17 czerwca 2002 r. (Dz.U. Nr 101, poz. 926).

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz.U. Nr 182, poz. 1228).

Ustawa o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz.U. Nr 112, poz. 1198).

Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (Dz.U. Nr 24, poz. 83), t.j. z dnia 1 sierpnia 2000 r. (Dz.U. Nr 80, poz. 904), t.j. z dnia 17 maja 2006 r. (Dz.U. Nr 90, poz. 631).

Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz.U. Nr 144, poz. 1204), t.j. z dnia 15 października 2013 r. (Dz.U. z 2013 r., poz. 1422).

Kodeks karny z dnia 6 czerwca 1997 r. (Dz.U. Nr 88, poz. 553, sprost.: Dz.U. z 1997 r. Nr 128, poz. 840).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483).

Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (Dz.U. Nr 171, poz. 1800), t.j. z dnia 10 stycznia 2014 r. (Dz.U. z 2014 r., poz. 243).

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r. W kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM(2007) 267 wersja ostateczna.

Council of Europe. European Treaty Series – No. 185.

Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318 105th Congress.

Orzecznictwo

Wyrok Sądu Apelacyjnego w Szczecinie z dnia 14 października 2008 r. II AKa 120/08.

Wyrok Sądu Najwyższego z dnia 2 czerwca 2003 r. II KK 232/02.

Źródła internetowe

http://www.aol.com
http://www.policja.pl
http://eur-lex.europa.eu
http://www.gpo.gov
http://cs.brown.edu
http://www.antiphishing.org
http://www.norton.com
http://blog-daneosobowe.pl
http://www.oszustwsieci.pl
http://serwisy.gazetaprawna.pl
http://haker.nie-spamuj.eu
http://www.microsoft.com
http://www.bbn.gov.pl
http://www.nato.int
http://wiadomosci.dziennik.pl