Problemy prawnokarne wirusów komputerowych.

Rozwijający się internet staje się środkiem masowego przekazu. Najnowsze prognozy wskazują, że w ciągu najbliższych dwóch do trzech lat ok. 14% ludności na świecie będzie miało dostęp do internetu. Dane szacunkowe mówią o około 1,3 miliarda wykonanych podłączeń do internetu do 2005 roku.[1]

Taki rozwój wymiany informacji na tak wielką skalę niesie za sobą wiele korzyści, ale i stwarza także wiele problemów. Jednym z nich jest zagadnienie rozprzestrzeniania się poprzez sieci połączeń komputerowych szkodliwych programów zwanych powszechnie wirusami komputerowymi. Pojęcie „wirus komputerowy" jeży włosy na głowie niejednemu użytkownikowi komputera czy firmie, której działalność opiera się na systemie komputerowym. Tymczasem jest to zwykły program, którego zadaniem jest niszczenie, uszkadzanie danych, zakłócenie pracy czy wreszcie spowodowanie anomalii w zachowywaniu się komputera.

Pierwszy raz w historii problemem wirusów komputerowych zajął się dr Frederick Cohen, który w swej pracy doktorskiej na Uniwersytecie w Dortmundzie sformułował ich definicję. Określił wirusa komputerowego jako kod programu, który rekursywnie replikuje kopię samego siebie w obrębie sieci. Definicja ta traktuje jednak rzecz wąsko, gdyż nie obejmuje wirusów polimorficznych, które same zmieniają swoją postać wraz z infekcją kolejnych plików.

Najnowsze definicje traktują wirusy jako programy komputerowe mające możliwość produkowania swych kopii w innych programach, mogących się wewnętrznie różnić, zmieniając jednocześnie kod tego programu, wykonując swój kod w określonym przez autora

[1] Komunikat pochodzący z badań Mummert & Partner – doradztwo dla przedsiębiorców, Hamburg

wirusa momencie. Ta definicja jest bardziej adekwatna do obecnej mnogiej twórczości autorów destrukcyjnych programów komputerowych.

W środowisku informatycznym można spotkać się z kilkoma podziałami wirusów komputerowych. Ja przytoczę jedno z najbardziej znanych zestawień.

Bomba logiczna— jest to kod umieszczony w programie, który uaktualnia się po spełnieniu określonych warunków, najczęściej spotykane są bomby czasowe (*tzw. time bomb*).

Koń trojański— jest to dowolny program, który zawiera kod realizujący funkcje inne od spodziewanych przez użytkownika.

Robak— ma zbliżone zasady funkcjonowania do wirusa, z pewnymi jednak odmiennościami. Działa w sieci przesyłając swoje kopie do różnych systemów. Jest samodzielnym programem wykonywalnym w środowisku systemu operacyjnego. W przeciwieństwie do wirusa nie potrzebuje nosiciela.

Królik— jest to program namnażający się aż do wyczerpania zasobów systemu.

Łańcuszek szczęścia— jest to replikant komunikatu wysyłanego pocztą elektroniczną lub przez krótkie wiadomości tekstowe SMS.

Muł trojański— jest to złośliwy kod komputerowy, który pobudza nieprawdziwe komunikaty, naśladujące normalny dialog z komputerem, bez właściwych efektów.[2]

Wirusy komputerowe posiadają zdolność oddziaływania na dowolny element systemu komputerowego, w szczególności przez:

☑ Wyświetlania nietypowych obrazów na ekranie (rysunków, znaków albo napisów),

[2] B. Fischer, Przestępstwa komputerowe i ochrona informacji, Zakamycze 2000 op. cit. s.42

- ☑ Zakłócania, zmieniania lub usuwania plików danych użytkownika (np. kasowania danych, oznaczanie miejsc na dysku jako „uszkodzone”, przez co zmniejsza się użyteczna przestrzeń dysku, uszkadzanie programów),
- ☑ Zakłócania lub oddziaływania na porty komunikacyjne (np. wymiana bajtów
- ☑ Zakłócanie danych w połączeniach modemowych, inicjowanie „fałszywych” połączeń telefonicznych, czy też zmiana położenia lub kierunku działania myszki),
- ☑ Spowalniania pracy systemu komputerowego (np. modyfikowanie przerwań sprzętowych),
- ☑ Powodowania fizycznych uszkodzeń podzespołów systemu komputerowego.

Nowe rodzaje wirusów pojawiły się wraz z ekspansją oprogramowania biurowego typu Microsoft Office. Pakiet ten został wzbogacony o tzw. makra, które to można napisać w ten sposób, aby realizowały procedury destrukcyjne i rozprzestrzeniały się zarażając kolejne dokumenty.

Rozwój internetu i poczty elektronicznej spowodował istny nawał wirusów dołączonych do poczty elektronicznej. Wynikiem działania takiego wirusa jest samodzielne jego powielanie i rozsyłanie do adresatów z książki adresowej programu pocztowego. Przykładem wirusa pocztowego jest wirus Monopoly. Wirus pojawia się na komputerze 'ofiary' w postaci załącznika do listu elektronicznego zawierającego, niegroźną z pozoru aplikację wyświetlającą okienko dialogowe z tekstem: Bill Gates is guilty of monopoly. Here is the proof.:-) oraz obrazek przedstawiający Billa na planszy gry Monopoly.

Przechodząc do omówienia problemów stricte prawnokarnych nie sposób pominąć faktu, że mimo wielorakich rodzajów

przestępstw komputerowych wiele jest takich, które mogą być efektem działania wirusa komputerowego. Należy zaznaczyć, że żaden autor definicji wirusa nie wymienia faktu napisania wirusa ani wprowadzenia go do sieci jako przestępstwa komputerowego.

W obecnym stanie prawnym w Polsce karalne jest zarówno wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym programów dezintegrujących dane i system komputerowy[3] jak i posługiwanie się nimi w taki sposób, aby wypełnić znamiona kodeksowe czynu zabronionego. Nowelizacja Kodeksu Karnego z 2004 roku wniosła zmianę w postaci wprowadzenia karalności pisania wirusów komputerowych. Przestępstwo to zagrożone jest karą pozbawienia wolności do lat 3. W razie skazania sprawcy za to przestępstwo sąd obligatoryjnie orzeka o przepadku napisanego wirusa, a może orzec ich przepadek, jeżeli nie stanowił własności sprawcy – art. 269b§2 K.K.

Jednym z głównych zagadnień przestępstw przeciwko bezpieczeństwie danych i systemów komputerowych jest problem informacji jako przedmiotu ochrony prawnej. Z uwagi na ciągłe przetwarzanie danych w systemach komputerowych informacji, jako przedmiotowi ochrony prawnej należy zapewnić nie tylko należytą ochronę techniczną, ale i odpowiednią ochronę prawną. Chodzi więc o gwarancję należytej poufności danych przy zachowaniu ich dostępności.
Na ochronę informacji składają się trzy podstawowe składniki integralność, dostępność i poufność danych komputerowych. Wspólna ochrona tych trzech czynników jest warunkiem sine qua non należytej ochrony informacji. Brak ochrony któregokolwiek spowoduje bezużyteczność ochrony przez pozostałe. Postulatem jest więc ochrona informacji w sposób kompleksowy, w zakresie równym dla powyższych czynników.

[3] Art.269b§1 KK, Dz.U.nr 88, poz. 553

Przestępstwo nielegalnej ingerencji w dane i nielegalnej ingerencji w funkcjonowanie systemu komputerowego to dwa podstawowe typy przestępstw przeciwko bezpieczeństwu danych i systemów komputerowych. Czyny te są penalizowane przez państwa-sygnatariuszy Konwencji Rady Europy o cyberprzestępczości w art. 4 i 5 wspomnianego aktu. Zakaz dokonywania nieuprawnionych ingerencji w dane ma chronić integralność elektronicznego zapisu informacji, a tym samym zapewnić poprawność i kompletność przetwarzanych danych oraz kompatybilność funkcjonowania programów komputerowych. Nieuprawnione naruszenie integralności danych przechowywanych lub przetwarzanych w systemie informatycznym to często sprawka wirusów komputerowych o właściwościach destrukcyjnych, które modyfikują lub niszczą dane.[4]

Kodeks karny do nowelizacji w 2004 roku nie bardzo inkryminował tego rodzaju incydenty. Sam art. 268 § 2 kk nie był skutecznym narzędziem do ścigania przestępstw naruszenia integralności danych komputerowych z uwagi na to, że przepis dotyczył „informacji istotnej".

Zasadniczym elementem przesądzającym o istotności informacji będzie jej obiektywnie oceniane znaczenie dla podmiotu, którego informacja dotyczy. O istotności informacji decydować będą zatem przede wszystkim jej treść, waga i znaczenie. Podstawą oceny istotności jest w tym kontekście standard obowiązujący w danej dziedzinie, do której odnosi się informacja.[5]

Nowelizacja kodeksu karnego w 2004 roku wprowadziła kilka zmian odnośnie przestępstwa naruszenia integralności danych komputerowych. Dodanie art. 268a § 1 K.K. spowodowało penalizację

[4] A. Adamski, Buszujący w sieci, http://www.klub-odgik.org.pl/biuletyn/nov2003/bezkarne.htm
[5] P. Kardas, **Czasopismo Prawa Karnego i Nauk Penalnych, 2000/1/25 t.-6**

przestępstwa posługiwania się wirusami komputerowymi w celu niszczenia, uszkadzania, usuwania, zmieniania lub utrudniania dostępu do danych informatycznych albo w istotnym stopniu zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Czyn ten wg artykułu 268b zagrożony jest karą pozbawienia wolności do lat 3.

Kolejnym przestępstwem z zakresu bezpieczeństwa danych i systemów komputerowych jest nielegalna ingerencja w funkcjonowanie systemu. Jednym i zarazem najczęstszym sposobem dokonania tego czynu jest zainfekowanie systemu komputerowego ofiary programem odpowiednio przygotowanym w celu złamania zabezpieczeń chroniących dostęp do komputera, a następnie zatarcie śladów swojej działalności przez wprowadzenie do komputera wirusa, bomby logicznej lub robaka komputerowego w celu zatarcia śladów swojego zachowania.

Karalność sabotażu komputerowego przewiduje art. 269 k.k. Istota czyny zabronionego została określona jako zakłócenie lub uniemożliwienie automatycznego gromadzenia lub przekazywania *danych informatycznych* o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji publicznej, bądź też niszczenie, uszkadzanie, usuwanie lub zmienianie zapisu takich *danych informatycznych* albo urządzeń służących do ich gromadzenia albo przetwarzania.[6]

W znowelizowanym kodeksie wprowadzono art.269a którego zadaniem była kryminalizacja zniszczenia, usunięcia, uszkodzenia lub zmiany danych informatycznych, które w istotnym stopniu zakłócają pracę systemu komputerowego lub sieci teleinformatycznej. Określenia: "w istotnym stopniu zakłóca lub uniemożliwia automatyczne

[6] A. Adamski, Przestępczość w cyberprzestrzeni Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001, s. 33

przetwarzanie, gromadzenie lub przekazywanie danych" (art. 268a § 1 k.k. in fine) oraz "w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej" (art. 269a k.k.) są w gruncie rzeczy tożsame. Praca systemu komputerowego polega na przetwarzaniu, gromadzeniu lub przekazywaniu danych. Zakłócenie lub uniemożliwienie tych procesów odbija się na pracy systemu.[7] Takie rozwiązanie prawne budzi kontrowersje i brak spójności systemu prawnego. Obie te normy o bardzo podobnej formie mają różne zagrożenie karne. Art. 268a §1 przewiduje zagrożenie karą pozbawienia wolności do lat 3. Natomiast art. 269a przewiduje karę pozbawienia wolności od 3 miesięcy do lat 5.

W mojej opinii należy zmienić te zapisy formułując jeden art. 268 jako przestępstwo karalnej ingerencji w dane, § 1 powinien dotyczyć karalności ingerencji w dane komputerowe, natomiast kolejne paragrafy dotyczyłyby kwalifikowanych odmian tego przestępstwa. Karalna ingerencja w system komputerowy powinna zawarta być w artykule następnym i powinno zastosować się podobną technikę legislacyjną jak w odniesieniu do ingerencji w dane komputerowe. Typem podstawowym powinien być sabotaż komputerowy dotyczący każdego systemu komputerowego, natomiast typy kwalifikowane powinny penalizować pod wyższym zagrożeniem karnym sabotaż komputerowy przeciwko obronności kraju, bezpieczeństwu w komunikacji, funkcjonowaniu administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

Zakaz pisania programów działających destrukcyjnie na dane i system komputerowy zaczął obowiązywać wiele krajów zanim doszło do spektakularnych incydentów z kilkoma najbardziej znanymi wirusami. Jednym z najpopularniejszych był wirus Anna Kurnikowa, który

[7] A. Damski, Buszujący…

zaatakował w 2001 r. Autorem kodu okazał się 20 – letni mężczyzna z holenderskiej Fryzji. Podczas jego przesłuchania podejrzany stwierdził, że nie chciał nikomu zaszkodzić, powiedział także, że wykorzystał nieostrożność użytkowników, którzy otwierali wiadomości w skrzynkach e-mail.[8]

Rozpowszechnianie wirusów jest karalne we Włoszech, Izraelu, Szwajcarii, USA, Holandii, Federacji Rosyjskiej, Finlandii, a od ubiegłego roku także w Polsce. Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom programu komputerowego przystosowanego do popełnienia przestępstwa określonego w art. 268a, art. 269 § 2 albo art. 269a jest zagrożone w Polsce karą pozbawienia wolności do lat 3. Interpretując semantycznie ww. przepis czynem karalnym nie jest przechowywanie takich programów na nośnikach danych we własnym celu czy używanie ich w celu sprawdzenia systemu zabezpieczenia własnego komputera. Sprawę podobnie traktuje Konwencja o cyberprzestępczości. W art. 6 pt. 2 mówi, że „niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcia do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2 - 5 niniejszej Konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego”.

W razie skazania za przestępstwo wytwarzania, udostępniania, pozyskiwania lub zbywania sąd orzeka obligatoryjnie przepadek określonych w nim przedmiotów, a może orzec ich

[8] I. Wetemeier, Zwalczanie przestępczości internetowej jako międzynarodowe wyzwanie, Rozmowy Gdańskie 2002

przepadek, jeżeli nie stanowiły własności sprawcy. Takie rozwiązanie wydaje się być w pełni racjonalne do popełnionych czynów.