DOI: 10.5604/20830157.1201319

JAK DEFINIUJEMY CYBERPRZESTĘPSTWO?

Monika Zbrojewska[1], Volodymyr Mosorov[2], Sebastian Biedron[2], Taras Panskyi[2]
[1] Uniwersytet Łódzki, Wydział Prawa i Administracji, [2] Politechnika Łódzka, Instytut Informatyki

Streszczenie. *W dzisiejszych czasach sieci komputerowe oraz oferowane przez nie usługi stały się najprężniej rozwijającą się dziedziną XXI wieku. Ich możliwości nie tylko pozwoliły na łatwiejszy kontakt użytkowników z całego świata, ale również wpłynęły na rozwój innych gałęzi nauki oraz technologii, ułatwiając codzienne życie. Wynalazek, który powstał do celów wojskowych w jednym z najbardziej mrocznych okresów ludzkiej cywilizacji , stał się największym odkryciem XX wieku łącząc miliony ludzi w jedną wielką społeczność. Obecnie każdy może skonstruować swoją własną sieć bądź dołączyć do największej z nich – Internetu za pośrednictwem lokalnego dostawcy internetowego. Niestety, Internet to nie tylko praktycznie nieograniczone źródło informacji, rozrywki, komunikacji oraz pracy. Obok swoich pozytywnych aspektów i udogodnień posiada też liczne zagrożenia, których nieświadomy użytkownik może stać się ofiarą. Niniejsze opracowanie ma na celu przybliżenie aspektów prawnokarnych i technicznych związanych z szeroko rozumianym zjawiskiem cyberprzestępczości.*

Słowa kluczowe: prawo karne, prawo w sieci, cyberprzestępstwo

HOW DO WE DEFINE CYBERCRIME?

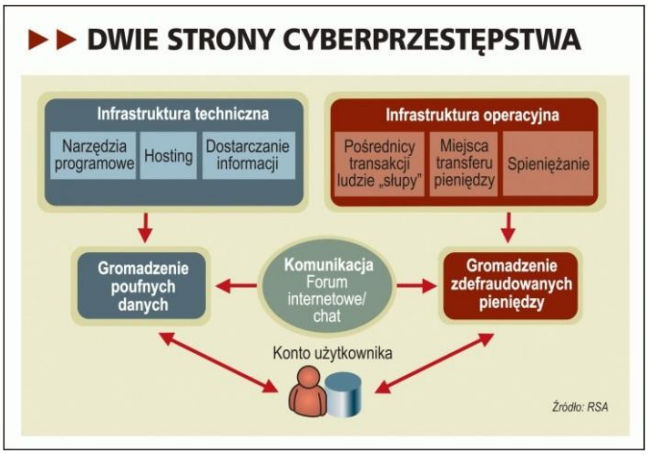
Abstract. *Nowadays, computer networks and the services they offer have become the fastest growing area of the XXI century. Their opportunities not only allowed for easier contact with users all over the world, but also influenced the development of other branches of science and technology. The invention, which was created in the purpose of war with the darkest periods of human civilization, has become the greatest discovery of the twentieth century, connecting millions of people in one big community. Today, everyone can build their own network or join the largest of them - the Internet via a local Internet provider. Internet virtually became unlimited resource of information, entertainment, communication and work. Apartment next to their positive aspects and features it has also many threats and unaware user can become a victim of them. This study aims to bring criminal and technical aspects related to the wider phenomenon of cybercrime.*

Keywords: law, cybercrime, criminal law

1. Aspekty prawnokarne

Kluczowym rozdziałem regulującym odpowiedzialność prawnokarną z tytułu cyberprzestępczości jest przede wszystkim rozdział XXXIII k.k. Jego analiza wskazuje na to, że ustawodawca dokonuje sukcesywnej penalizacji zachowań niebezpiecznych i zasługujących na penalizację z punktu widzenia prawa karnego. Powodem tego postępowania naszego prawodawcy jest dynamiczny rozwój zjawiska cyberprzestępczości, który obejmuje coraz to nowe sposoby, jak i metody jego działania (rys. 1). Aktualnie w ramach wspomnianego rozdziału kodeksu karnego ustawodawca spenalizował takie zachowania jak: nielegalne uzyskanie dostępu do informacji lub systemu informatycznego i z nimi związane (art. 267 k.k.), czyny polegające na niszczeniu, uszkadzaniu, usuwaniu, zamienianiu istotnej informacji lub czynnościach zbliżonych (art. 268 k.k.), czyny polegające na niszczeniu, uszkadzaniu, usuwaniu zmienianiu lub utrudnianiu dostępu do danych informatycznych albo w istotnym stopniu zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (art. 268a k.k.), czyny polegające na tzw. sabotażu informatycznym (art. 269 k.k.) zwanymi też dywersją informatyczną, czyny polegające na zakłócaniu w istotnym stopniu pracy systemu komputerowego lub sieci teleinformatycznej (art. 269a k.k.) oraz czyny polegające na bezprawnym wytwarzaniu (lub czynnościach zbliżonych) urządzeń lub programów komputerowych przystosowanych do popełnienia określonych przestępstw, haseł komputerowych, kodów dostępu lub innych danych (art. 269b k.k.) [13]. Poza wymienionym rozdziałem ustawodawca odrębnie unormował przestępstwo oszustwa komputerowego (art. 287 k.k.), kradzież programu komputerowego (art. 278 § 2 k.k.) oraz paserstwo programu komputerowego (art. 293 k.k.). Rozwiązania przyjęte w rozdziale XXXIII k.k. są następstwem podpisania przez Polskę dnia 23 listopada 2001 r. Konwencji Rady Europy nr 185 o cyberprzestępczości oraz decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne [1, 2].

Pod pojęciem cyberprzestępczości należy rozumieć wszystkie rodzaje przestępstw, do których popełnienia użyto Internetu lub innych sieci komputerowych. Komputery przy tym i sieci komputerowe mogą służyć do popełnienia przestępstw na kilka sposobów.



Rys. 1. Dwie strony cyberprzestępstwa [6]

Po pierwsze komputer lub sieć mogą być narzędziem przestępstwa, czyli mogą być użyte do popełnienia przestępstwa (computer as tool), jak na przykład oszustwo i fałszerstwo komputerowe. Po drugie komputer lub sieć mogą być celem ataku, czyli mogą być „ofiarą" przestępstwa [8]. Można je nazwać przestępstwami przeciwko poufności, integralności i dostępności danych informatycznych i systemów (computer as target). Po trzecie komputer lub sieć mogą być użyte do zadań dodatkowych, które to zadania związane są z popełnieniem przestępstwa. Można także wyróżnić czyny, w których komputer służy jako narzędzie do przechowywania nielegalnych danych (computer as storage device), jak na przykład pornografia dziecięca oraz czyny związane z naruszeniem praw autorskich i praw pokrewnych. W literaturze przedmiotu wskazuje się, że przestępstwa związane z komputerami stanowią wyjątkowo transnarodową formę przestępczości, o dużym stopniu skomplikowania i różnorodności [15].

Właściwie wszystkie przestępstwa ujęte w rozdziale XXXIII k.k. mogą być popełnione przy użyciu komputera. Staną się one wówczas przestępstwami komputerowymi. W niektórych przypadkach użycie komputera stanowi okoliczność zaostrzającą odpowiedzialność karną, np. art. 268 § 2 i 3 k.k., natomiast w innych sytuacjach sprawca popełniając przestępstwo z wyko-

rzystaniem komputera będzie traktowany tak samo, jak sprawca działający w inny sposób, np. art. 265 k.k., art. 266 k.k.

Zasadniczym przedmiotem ochrony penalizacji przestępstw komputerowych jest tradycyjna wolność i prywatność jednostek, choć ujmowana z perspektywy komputerowej, ale nie tylko, bowiem ochronie podlega także dane zgromadzone w systemach, jak również same systemy i ich integralność, której naruszenie może mieć nierzadko bardzo poważne następstwa społeczne [7]. Jednocześnie, należy nadmienić, że prawnokarna regulacja cyberprzestępczości napotka na dwa zasadnicze problemy. Pierwszy związany jest z zasadą jurysdykcji. Przestępstwa komputerowe popełniane w Internecie bardzo często mają charakter transgraniczny, a czasami wręcz aterytorialny, w tym sensie, że często są popełniane w oderwaniu od terytorium danej jurysdykcji. Drugim problemem jest bardzo szybki rozwój nowych postaci cyberprzestępczości, za którym ustawodawcy z reguły nie nadążają.

Spotykając się po raz pierwszy z pojęciem „przestępstwa komputerowego" możemy zauważyć, że istnieje wiele definicji tego zjawiska, jakim powinniśmy określać czyny polegające na naruszeniu dóbr prawnych chronionych przez prawo za pomocą urządzeń informatycznych. W różnych publikacjach oraz artykułach możemy spotkać się z określeniem „przestępstwo komputerowe", „cyberprzestępstwo", „przestępstwa IT" czy „przestępstwa z wykorzystaniem komputera" Przyczyną braku ścisłości w nazewnictwie i klasyfikacji opisywanego problemu jest przede wszystkim rozległość samego zakresu wszystkich technologii umożliwiających manipulowanie i przesyłanie informacji, różnorodności przestępstw informatycznych oraz często niskiego stanu wiedzy technicznej osób zajmujących się opisywaną problematyką od strony prawnej. Jako pierwszą definicję przestępczości informatycznej przyjęto tą zaproponowaną w 1973 r. przez Rainera von Zur-Mühlena. Określa ona za przestępcze działanie te czyny, w którym komputer stanowi albo narzędzie, albo przedmiot zamachu" (all jenes deliktische Handeln, bei dem der Computer Werkzeug oder Ziel der Tat ist) [16] . Kolejnym bardzo znaczącym i popularnym pojęciem, zarazem będącym synonimem przestępstwa komputerowego, jest „cyberprzestępstwo". Samo słowo cyberprzestrzeń zostało użyte przez Williama Gibsona podczas konwencji science-fiction w 1981 roku na którym autor prezentował swoją książkę. Pojęcie to określało wirtualną rzeczywistość, w której W. Gibson umieścił swoich bohaterów. Znaczenie tego słowa uległo od tego czasu drobnej zmianie. W dzisiejszych czasach rozumiemy je jako przestrzeń otwartego komunikowania się za pośrednictwem połączonych urządzeń końcowych i serwerów pełniących określone funkcje. Taka definicja została zaproponowana przez Pierre Delvy w tekście „Drugi Potop" napisanym na zlecenie Komisji Kultury Rady Europy w 1996 r. [9].

Tak jak w przypadku świata rzeczywistego w świecie cyberprzestrzeni pojawiło się cyberprzestępstwo. Jest to dosyć nowe zjawisko, które rozwija się w zastraszającym tempie w krajach wysokorozwiniętych i silnie zinformatyzowanych. Zagrożenie to stanowi bardzo poważny problem ze względu na:

- transgraniczność – przestępstwo można dokonać z dowolnego miejsca na Ziemi często na ofierze oddalonej o setki kilometrów znajdującej się w innym państwie czy na innym kontynencie. Taki stan rzeczy utrudnia określenie systemu prawnego, na podstawie którego miałoby nastąpić ściganie takiego przestępstwa oraz podmiotów odpowiedzialnych za zapobieganie oraz bezpieczeństwo [11].
- ogólnodostępność – wystarczy posiadać podstawową wiedzę oraz urządzenie końcowe takie jak np. komputer podłączone do Internetu, aby dokonać przestępstwa. W wielu przypadkach złamanie prawa następuje jednak nieświadomie, gdy osoba ściąga dany utwór czy film za pomocą programów PvP (peer to peer), które jednocześnie udostępniają innym użytkownikom to co zostało pobrane (kwestia nieświadomego rozpowszechniania).
- anonimowość – zachowanie anonimowości w świecie wirtualnym jest dużo łatwiejsze do osiągnięcia. Wykrycie przestępcy w sieci nie jest niemożliwe, jednak wymaga bardzo dużo nakładu pracy, żmudnych poszukiwań [3] oraz współpracy kilku instytucji często wywodzących się z innych krajów. Dosyć dużym utrudnieniem jest również łatwy dostęp do Internetu. Obecnie wiele centrów handlowych, restauracji, cafeterii oferuje bezprzewodowy darmowy dostęp dla swoich klientów nie oczekując od nich jakiejkolwiek autentykacji czy innych danych na podstawie których można byłoby stwierdzić tożsamość danej osoby.
- niematerialny charakter – dane w sieci mają charakter niematerialny znajdują się w „cyberprzestrzeni" do której jedyny możliwy dostęp jest przez urządzenia do tego przeznaczone jak np. komputer. Jeżeli nie posiadają odpowiednich zabezpieczeń można je bez ograniczeń kopiować i przechowywać w Internecie lub na nośnikach fizycznych.
- brak scentralizowanego ośrodka kontroli – pomimo, że przestępstwa mają przeważnie postać transgraniczną, tak każde państwo posiada swój własny ośrodek kontroli nad Internetem oraz dział zajmujący się przestępczością komputerową. Od ich międzynarodowej współpracy zależy czy dani przestępcy komputerowi zostaną wykryci. Często na tym etapie na przeszkodzie staje zróżnicowanie w zaawansowaniu technologicznym ośrodków, biurokracja poziom wykfalifikowanej kadry oraz nierzadko bariera językowa.

Podsumowując należy pamiętać, że w naszym systemie prawnym nie ma jasno sformułowanej definicji cyberprzestępczości. Z tego powodu powinno się w takiej sytuacji posiłkować organizacjami, które stworzyły już swoje standardy i określił co powinno się zaliczyć do przestępczości komputerowej. Do takich organizacji zaliczamy Interpol, UE, Radę Europy czy ONZ. Wszystkie one stworzyły definicje, nieznacznie się od siebie różniące.

Według Rady Europy jako cyberprzestępstwo uznajemy fałszerstwo komputerowe, oszustwo komputerowe, naruszenie praw autorskich i praw pokrewnych oraz przestępstwa związane z treściami dotyczącymi pedofilii.

Interpol ukazuje cyberprzestępczość na dwóch płaszczyznach. Jedną definiuje jako rodzaj przestępstw, które mogą wystąpić tylko w Internecie. Druga natomiast jako przestępstwa wykorzystujące technikę elektroniczną.

Definicja opracowana przez Unię Europejską, która została ujętą w komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 r. pt. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" jako cyberprzestępstwo uznaje działanie które wymierzone jest przeciwko poufności, integralności danych, sabotaż komputerowy, szpiegostwo komputerowe a także nielegalny podsłuch. Do tych działań zalicza się tzw. przestępstwa „contentowe" i „klasyczne" oraz te związane z naruszeniem praw autorskich.

Organizacja Narodów Zjednoczonych na X kongresie w Sprawie Zapobieżenia Przestępczości i Traktowania Przestępców opracowała definicję cyberprzestępczości, którą należy rozpatrywać w sensie wąskim, jak i szerokim. W wąskim sensie rozumiane jest jako nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych. W sensie szerokim definiujemy nielegalne działania popełnione za pomocą lub dotyczące urządzeń teleinformatycznych do których zaliczamy między innymi nielegalne posiadanie i rozpowszechnianie informacji wykorzystując fizyczne nośniki lub Internet. Należy zawsze pamiętać, że wymienione definicje nie są definicjami w pełni określające cyberprzestępstwo. Każdego roku powstają nowe technologie, które umożliwiają rozwój nowych narzędzi oraz metod za pomocą których można dopuścić się działań bezprawnych.

2. Aspekty techniczne

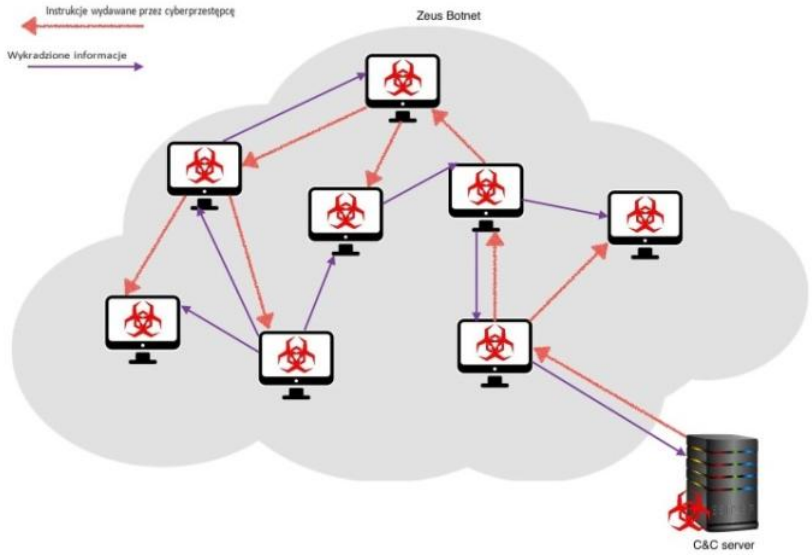
Analizując zjawisko cyberprzestępczości nie można pominą aspektów technicznych tego zjawiska. Zrozumienie podstaw działania sieci oraz technik i narzędzi wykorzystywanych do popełnienia przestępstw w cyberprzestrzeni jest kluczowe z punktu widzenia możliwości opracowania skutecznych metod przeciwdziałania i walki z tym co raz bardziej nasilonym zjawiskiem. Postaramy się przedstawić skróconą wersję problemu na przykładzie funkcjonowania wirusa, sieci botnet, ataku man-in-the-middle oraz ostatnimi czasy bardzo popularnego ataku phisingowego.

Każdy użytkownik sieci komputerowej słyszał lub miał kontakt z pojęciem wirusa komputerowego. Jednak niewiele osób wie czym tak naprawdę jest wirus i jak powstaje. Pierwszym wirusem w historii był opracowany przez Boba Thomasa wirus o nazwie „Creeper". Kod ten był niegroźny i raczej miał formę żartu niż groźnego zagrożenia dla poufności danych. Jego zadanie polegało na wyświetlaniu na zainfekowanym komputerze komunikatu „I am Creeper, chatch me if you can". Czyli wirus komputerowy to obcy fragment kodu dołączony do programu, który dokonuje zaplanowanych przez jego twórcę, niepożądanych działań w środowisku systemu ofiary, uszkadzając dane, aplikacje, zmieniając sposób funkcjonowania sprzętu itp. Uruchomienie tego kodu inicjowane jest przeważnie przez nieświadomego użytkownika wraz z innym programem. Wirus, infekuje dodając swój kod do pozostałych programów znajdujących się na pamięci masowej np. dysku twardym. Konsekwencje dla ofiary takiego zainfekowania zależą jedynie od twórcy i jego intencji, które mogą być zwykłym żartem jak w przypadku wyżej opisanego „Creepera", miejscem replikacji lub w najgorszym wypadku uszkodzeniem plików czy kradzieżą poufnych danych. Jednym z najgroźniejszych narzędzi w rękach cyberprzestępców jest koń trojański. Nazwa została zaczerpnięta z greckiej mitologii i tak jak pozorny podarunek, a w rzeczywistości kryjówka greckich żołnierzy, którzy opanowali Troję, współczesne konie trojańskie to programy komputerowe zawierające w sobie fragment kodu, które wydają się użyteczne dla ofiary. W istocie stanowią zagrożenie bezpieczeństwa i powodują wiele zniszczeń. Coraz częściej zaszywają się one w systemie operacyjnym i przejmują nad nim kontrolę. Zwykle poczynaniami konia trojańskiego kieruje człowiek – gdy komputer jest podłączony do Internetu, jesteśmy narażeni na utratę danych, kradzież haseł, inwigilację a nawet sformatowanie dysku twardego. Konie trojańskie najczęściej nie replikują się tak jak zwykłe wirusy. Kolejnym narzędziem z tej rodziny cyberataków jest robak. Jego bardzo ważna cechą odróżniającą go od reszty jest samo-replikacja oraz fakt, że nie potrzebuje on programu, ani pliku-nosiciela. Jego budowa pozwala mu na automatyczne, samodzielne kopiowanie się z jednego komputera na inny, często przejmując kontrolę nad funkcjami urządzenia ofiary, umożliwiającymi przesyłanie plików lub informacji. Należy pamiętać, że taką umiejętność robaki nabywają po przejęciu jednego z zasobów komputera ofiary jakim jest program pocztowy. Robak może rozsyłać kopie siebie do wszystkich osób znajdujących się w książce adresowej i w ten oto sposób może zainfekować inne komputery.

Botnet (rys. 2) to rodzaj sieci złożonej z komputerów, która została zainfekowana złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem. Sieć taka zostaje powołana do wykonania odpowiedniego celu, zadania, które wyznaczył jego twórca.

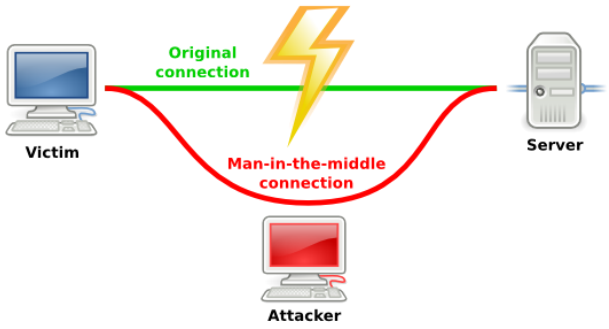
Każdy zainfekowany komputer określany jest jako „zombie" – osoba niepożądana w pełni przejmuje kontrolę nad nieświadomą ofiarą. Może przeglądać jego dane znajdujące się na dyskach twardych czy innych pamięciach masowych oraz dokonywać ataków na inne cele z komputera ofiary. Urządzenia, które tworzą botnet mogą zostać wykorzystane do tzw. ataku DDoS (Distributed Denial of Service). W tym przypadku komputery zombie będące częścią danej sieci botnet przeprowadzają skoordynowany atak uniemożliwiając funkcjonowanie danego serwisu np. portalu internetowego poprzez zajęcie wszystkich wolnych zasobów ofiary. Najbardziej znanym narzędziem do tworzenia sieci botnet jest Zeus. Jest on jednym z pierwszych jakie powstały i na pewno jednym z najbardziej dochodowych. Jego istnienie zostało ujawnione w roku 2007. Głównym celem Zeusa było monitorowanie komputerów ofiar i tak zwany atak „Keystroke logging" czyli sczytywanie wszystkich przyciśniętych klawiszy klawiatury oraz wysyłanie ich do właściciela danego botnetu.

Umożliwiało to napastnikowi wykradanie z komputerów mieszkańców USA oraz Wielkiej Brytanii poufnych danych – głównie informacji niezbędnych do zalogowania się do kont bankowych. Analiza problemu opisana przez Secure Works informuje, że na samym początku rozwojem Zeusa zajmowała się jeden człowiek, który współpracował z grupą przestępczą o nazwie UpLevel, a sam program był tylko oprogramowaniem typu spyware wyspecjalizowanym w wykradaniu danych. W roku 2010 do sieci trafiła informacja że właściciel zaprzestał swojej działalności a kod źródłowy wirusa przekazał innemu twórcy złośliwego oprogramowania, który był właścicielem botnetu o nazwie „SpyEye". Rok później doszło do wycieku kodu źródłowego narzędzia. Przez co każdy mógł go sobie pobrać i dowolnie modyfikować oraz uruchomić swoją własną sieć Zombie. Od tamtej pory powstało wiele modyfikacji tego złośliwego oprogramowania między innymi ZeuS P2P, który jest pozbawiony największej wady podstawowej wersji czyli scentralizowanego serwera zarządzającego.



Rys. 2. Działanie sieci Botnet [10]

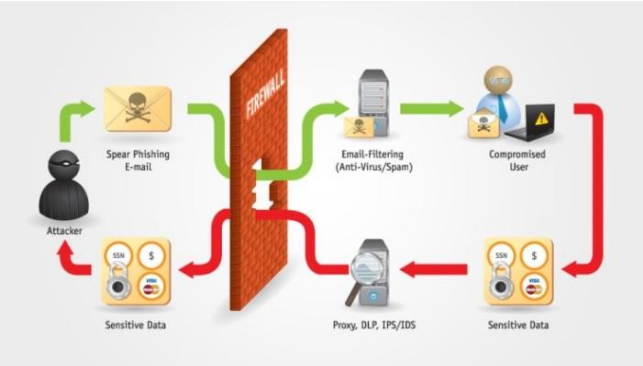
W ataku **man-in-the-middle** [4] mamy do czynienia z przechwytywaniem przez cyberprzestępcę wiadomości pomiędzy dwiema stronami, które uważają, że komunikują się bezpośrednio ze sobą. Osoba nieuprawniona nie tylko ma możliwość podsłuchania takiej rozmowy, ale również modyfikacji każdej z wiadomości (rys. 3).



Rys. 3. Schemat ataku man-in-the-middle [5]

Atak ten w literaturze naukowej możemy spotkać pod różnymi nazwami „Man in The Middle" (MiTM), „Man in The Middle Attack" (MiTMA) oraz jako „atak przechwycenia sesji". Ten sposób nielegalnego pozyskiwania informacji stanowi poważne zagrożenie dla bezpieczeństwa usług online, ponieważ dają on atakującemu możliwość przechwytywania poufnych danych i ich manipulacji w czasie rzeczywistym podczas przebiegającej transakcji, przebiegu rozmów czy przesyłania plików. Najczęściej spotykanym atakiem MiTM jest atak umożliwiony poprzez złośliwe oprogramowanie jak wirus czy koń trojański. Złośliwy program daje atakującemu dostęp do przeglądarki internetowej ofiary lub pozwala na modyfikację lokalnych plików cache DNS. Domain Name Serwer, w skrócie DNS jest jedną z ważniejszych usług oferowanych nam podczas surfowania w Internecie. Każda strona internetowa, od prywatnych stron zaczynając na stronach bankowych kończąc posiada swój własny adres IP, będący identyfikatorem\lokalizacją danej usługi. Ma on postać cztero-oktetową np. 212.77.100.101 w tym przypadku jest to adres portalu „Wirtualna Polska". Po wpisaniu jego w miejsce paska adresu internetowego w przeglądarce otworzy nam się strona WP. Już samo spamiętanie kilku adresów staję się dla przeciętnej osoby problemem, nie mówiąc już o setkach tysięcy innych. Z pomocą przychodzi usługa DNS, której zadaniem jest zamiana adresów łatwych do zapamiętania jak np. www.wp.pl na adresy zrozumiałe dla urządzeń informatycznych, w tym przypadku 212.77.100.101. Użytkownik nie musi pamiętać ciągu liczb, a jedynie skróty słowne pod jakimi kryje się dana strona. Osoba niepożądana może wykorzystać tą usługę do swoich własnych celów poprzez modyfikację lokalnego pliku cache DNS znajdującego się na komputerze ofiary. Plik ten zawiera ostatnie używany adresy. Cyberprzestępca modyfikuje ten plik dodając własne wpisy lub podmienia go. Nieświadomy użytkownik wpisując adres www.wp.pl zostaje przekierowany do witryny kontrolowanej przez atakującego, która wygląda dokładnie tak samo jak oczekiwany portal. Ofiara logując się do dowolnej usługi jak np. poczta WP zostaje przekierowana do oryginalnej strony, jednak na komputerze cyberprzestępcy pozostawia informacje o loginie i haśle jakich użyła do autentykacji. Oszust otrzymuje poufne dane, a ofiara nie jest świadoma, że właśnie udostępniła swoje prywatne hasła. Ostatnimi czasy bardzo popularny stał się atak wykorzystujący ruter Wifi jako urządzenie umożliwiające nielegalne przechwycenie komunikacji użytkownika lub użytkowników. Cel ten można osiągnąć za pomocą odpowiednio przygotowanego „złośliwego rutera" , który udawałby legalne urządzenie lub poprzez wykorzystanie luki w legalnym ruterze spowodowanym brakiem umiejętności w konfiguracji przez jego właściciela jak np. pozostawienie domyślnych haseł. Pierwsza opcja polega na stworzeniu urządzenia – hotspota WiFi, które udawałoby ruter jakieś instytucji jak np. ruter w kawiarni, w urzędzie. Następnym krokiem jest wykorzystanie nieuwagi użytkownika. Ofiara loguje się do takiego urządzenia, a następnie stara się dotrzeć do krytycznie ważnych miejsc, takich jak witryny banków internetowych lub e-sklepów pozostawiając nieświadomie na urządzeniu cyberprzestępcy wszystkie informacje potrzebne do autentykacji na odwiedzonym portalu. Druga opcja polega na przejęciu kontroli przez cyberprzestępcę legalnie działającego urządzenia pod nieuwagę jego właściciela. Znalezione luki w bezpieczeństwie napastnik stara się wykorzystać do podsłuchiwania komunikacji oraz gromadzenia ogromnych ilości poufnych danych. Od tej chwili metoda pozyskiwania jest taka sama jak w przypadku opisanej opcji pierwszej z tą różnicą, że cyberprzestępca nie tworzy fałszywego rutera, a korzysta z legalnie istniejącego na którym złamał zabezpieczenia otrzymując prawa administracyjne.

Phishing [14] inaczej „password harvesting fishing" jest to metoda oszustwa polegająca na kontakcie napastnika z ofiarą w celu kradzieży informacji osobistych bądź haseł dostępowych do kont (rys. 4). Cyberprzestępca dokonuje tego podając się za przedstawiciela legalnego, zaufanego portalu lub firmy np. pracownika banku w którym odbiorca ma konto. Sprawca kontaktuje się za pomocą internetowego środka komunikacji jak np. mail. Strony na których najczęściej dochodzi do ataku phisherów to PayPal, eBay, MSN, Yahoo, BestBuy i America Online, czyli jak widzimy większość z nich związana jest z finansami. Phisher wysyła zazwyczaj spam do wielkiej liczby potencjalnych ofiar, kierując je na stronę w Internecie, która udaje rzeczywisty portal internetowy. Tak samo jak przy ataku man-in-the-middle cyberprzestępca przechwytuje login i hasło niedoświadczonego użytkownika. Najbardziej popularnym sposobem jest wykorzystanie maila z informacją o rzekomym zdezaktywowaniu konta i o konieczności ponownego jego reaktywowania, z podaniem wszelkich poufnych informacji. Inną metodą jest tworzenie fałszywych stron pod adresami bardzo przypominającymi oryginalny, a więc często łatwym do przeoczenia dla nieuważnej osoby np. www.nbank.pl zamiast www.mbank.pl.



Rys. 4. Działanie Phisingu [12]

Najgroźniejszą odmianą phishingu jest pharming. Jest to nowa metoda, która dla normalnego użytkownika, jak i jego zabezpieczeń, jest bardzo trudna do wykrycia. Napastnik za pomocą szkodliwego oprogramowania, jak np. trojany, zmienia lokalne pliki ofiary, tak samo jak w przypadku metody man-in-the-middle opisanej wyżej lub jego celem staje się serwer zewnętrzny DNS, który oferuje usługę tłumaczenia adresów. W tym ostatnim przypadku jedyną nadzieją jest doświadczenie w zapewnieniu bezpieczeństwa i szybka reakcja administratora sieci do której dany użytkownik jest podłączony [13].

Mając na uwadze przedstawione aspekty tak zarówno prawnokarne, jak i przede wszystkich techniczne nie może budzić wątpliwości jakie poważne zagrożenie niesie za sobą cyberprzestępczość i konieczność właściwej reakcji w szczególności poprzez unormowania w dziedzinie prawa karnego.

Bibliografia

[1] Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne.
[2] Dz. Urz. UE L z 2005 r., 69/67. Zobacz szerzej: F. Radoniewicz, Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym, Ius Novum 1/2009.
[3] Falliere N., Chien E.: Zeus: King of the Bots, Symantec.
[4] Fisher D.: Co to jest atak Man-in-the-Middle?, Kaspersky lab.
[5] Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!, Pe Hat.
[6] Janoś T.: Cyber-crime znaczy biznes, Computerworld.
[7] Kodeks karny. Część szczególna. Komentarz do artykułów 222–316, pod red. A. Wąska, R. Zawłockiego, Warszawa 2010, t. II, 576–579.
[8] Littlejohn Shinder D., Tittel E.: Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci, Gliwice 2004.
[9] Nowak M.: Cybernetyczne przestępstwa – definicje i przepisy prawne. Cyberkłopoty i pułapki sieci, 4/2010 (113).
[10] O'Connell J.: Gameover for P2P Zeus? OxCERT.
[11] Oleksiewicz I.: Ochrona praw jednostki a problem cyberterroryzmu. HSS 1/2014, 113–129.
[12] Phishing Infographic, http://www.deviantart.com/art/Phishing-Infographic-212547990.
[13] Radoniewicz F.: Odpowiedzialność za przestępstwo hackingu. Pr. w Dział. 13/2013, 29.
[14] Shi J., Saleem S: Phishing. CSc 566 Computer Security – Research Reports, 2012.
[15] Sieber U.: Mastering Complexity in the Global Cyberspace: the Harmonization of Computer – Related Criminal Law. Les chemins de l´harmonisation pénale, pod red. M. Delmas – Marty, M. Pieth, U. Seiber, Paris 2008, 127–128.
[16] Siwicki M.: Podział i definicja cyberprzestępstw. Prok. i Pr. 7–8/2012, 242.
[17] Wróbel W.: Kodeks karny Komentarz, red. A. Zoll, t. II, 2008, 1305.

Prof. Monika Zbrojewska

Monika Zbrojewska (born: August 5, 1972 – died: Oct. 30, 2015) Polish lawyer, Doctor of Law, Professor of University of Lodz, lawyer, in 2014–2015 Undersecretary of State in the Ministry of Justice. Author of numerous publications and books.

Prof. Eng. Volodymyr Mosorov
e-mail: w.mosorow@kis.p.lodz.pl

Volodymyr Mosorov received his Ph.D. in 1998 from the State University of Lviv, Ukraine. V. Mosorov was awarded the title of Doctor of Science from AGH University of Science and Technology Krakow Poland in 2009. He is now an associate professor at the Institute of Applied Computer Science of Lodz University of Technology, Poland. His research interests include data mining and clustering. He has 3been involved in these areas for more than 15 years. Member of the The Polish Information Processing Society. He has published more than 80 technical articles.

M.Sc. Eng. Sebastian Biedron
e-mail: sbiedron@kis.p.lodz.pl

A graduate of the Department of Science and Mathematics at Lodz University. From 2012 year is a court expert at the District Court in Warsaw. From 2013, Ph.D. student at the Institute of Applied Computer Science of Lodz University of Technology. Supervisor of the Ph.D. thesis is prof. Volodymyr Mosorov.

M.Sc. Eng. Taras Panskyi
e-mail: tpanski@kis.p.lodz.pl

Graduate of the Electrotechnics Department at the Lviv National Polytechnic University, Ukraine. From 2013, Ph.D. student at the Institute of Applied Computer Science of Lodz University of Technology, Poland. His research interests include data clustering, reliability and availability indexes of embedded systems, educational migration.

otrzymano/received: 14.02.2016 *przyjęto do druku/accepted: 18.02.2016*