PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
SERIA: Edukacja Techniczna i Informatyczna 2009 z. IV

Tomasz Prauzner
Akademia im. Jana Długosza w Częstochowie

PRAWO A BEZPRAWIE W INTERNECIE

Wstęp

Burzliwy rozwój Internetu, którego jesteśmy świadkami w ostatnich latach, u wielu osób może wywołać wrażenie, iż sieć ta jest wynalazkiem bardzo nowoczesnym. Tymczasem historia Internetu sięga już ponad ćwierć wieku wstecz. Zaczyna się ona w 1969 roku, kiedy to w Uniwersytecie Kalifornijskim w Los Angeles (UCLA), a wkrótce potem w trzech, następnych uniwersytetach, zainstalowano w ramach eksperymentu finansowanego przez ARPA (Advanced Research Project Agency, zajmującą się koordynowaniem badań naukowych na potrzeby wojska) pierwsze węzły sieci ARPANET – bezpośredniego przodka dzisiejszego Internetu.

Internet jest największym systemem komputerowym na świecie. Stanowi olbrzymią sieć sieci, ogarniającą cały świat, bezustannie ewoluującą i przekształcającą się. Internet dostępny jest dla każdego, kto dysponuje modemem, linią telefoniczną, komputerem lub stałym połączeniem z tą siecią. Zawiera nieograniczone źródło danych, do którego dostęp jest umożliwiony w każdym miejscu i czasie[1]. Wielu użytkowników Internetu nie zdaje sobie sprawy z niebezpieczeństwa, jakie czyha na nich w sieci. W swojej pracy starałem się opisać najpopularniejsze przestępstwa komputerowe oraz ich zwalczanie.

Przestępczość komputerowa, jej podział i charakterystyka

Rosnąca od kilku lat liczba użytkowników sieci internetowej powoduje, że korzystają z niej różne osoby, które wykorzystują Internet do przestępstw[2]. Nie istnieje jednoznaczna definicja tego zjawiska. Większość ekspertów ma swoje własne określenie, a zastosowanie jednego nie jest wyczerpujące. Jest to dosyć trudne zagadnienie ze względu na różnice, jakie istnieją między tym a zwykłym przestępstwem. Przestępczość komputerowa jest znacznie trudniej-

sza do wykrycia niż pospolite przestępstwo, głównie ze względu na możliwość nieobecności przestępcy w miejscu przestępstwa, a co się z tym wiąże znikomym lub czasami brakiem jakichkolwiek śladów[3]. Istnieje wiele podziałów przestępczości komputerowej. Według angielskiego prawnika Petera Sommera przestępczość komputerową można podzielić następująco:

1. Niemożliwą do dokonania poza środowiskiem komputerowym, do których zalicza: manipulacje dokonywane za pomocą komputera na zbiorach danych i oprogramowaniu, nieuprawnione wejście do systemu komputerowego, czyli tzw. Hawking.
2. Ułatwianą przez komputery, obejmującą: oszustwa, fałszerstwa, kradzież informacji oraz podsłuch, rozpowszechnianie w ogólnie dostępnych sieciach komputerowych (np. Internet) wiadomości obraźliwych lub pornograficznych.
3. Popełnianą przy biernym udziale komputerów, oszustwa przez prowadzenie np. podwójnej księgowości lub wyrządzanie szkód w interesach prywatnych poprzez np. naruszanie osobistych praw autorskich.
4. Dokonywaną przez profesjonalnych przestępców z wykorzystaniem komputerów służących do wspomagania swojej działalności (nadzór interesów, zacieranie śladów, komunikacja, produkcja fałszywych dokumentów itp.)[3].

Według Międzynarodowej Organizacji Policji Kryminalnych „Interpol" przestępczość komputerową zdefiniować można jako przestępczość w zakresie technologii komputerowych i podzielić ją na:

1. Naruszanie praw dostępu do zasobów, a w szczególności:
   - hacking, czyli nieupoważnione wejście do systemu informatycznego,
   - przechwytywanie danych,
   - kradzież czasu,
   - modyfikację zasobów za pomocą bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego.
2. Oszustwa z użyciem komputera, a w szczególności:
   - oszustwa bankomatowe,
   - fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesorowych),
   - oszustwa na maszynach do gier,
   - oszustwa poprzez podanie fałszywych danych identyfikacyjnych.
3. Powielanie programów, w tym:
   - gier we wszelkich postaciach,
   - wszelkich innych programów komputerowych,
   - topografii układów scalonych.
4. Sabotaż zarówno sprzętu jak i oprogramowania[4].

Przestępstwa elektroniczne – analiza pojęć, rodzaje i charakterystyka

Szczególne znaczenie przestępstw elektronicznych wynika przede wszystkim z faktu, że miejsce gdzie są one dokonywane, nie zawsze jest „miejscem" w potocznym tego słowa znaczeniu. W życiu codziennym, można spotykać na każdym kroku słowo komputer, program albo Internet. W stosunku do tych pojęć, często istniejące regulacje prawne nie wystarczają do ich opisania. Wykorzystywanie Internetu do popełniania przestępstw jest niebezpieczne, ze względu na wysoką liczbę potencjalnych ofiar oraz trudności w wykrywaniu ich sprawców. Cyberprzestrzeń pozbawiona jest wszelkich fizycznych atrybutów czyjejś obecności, takich jak: odciski palców, głos, wizerunek. Dlatego niezwykle istotne jest, aby stworzyć takie prawo, które można by stosować do tego „nowego świata"[5].

Metody przestępczego działania:

Koń trojański (trojan) – program, który nadużywa zaufania użytkownika wykonując bez jego wiedzy dodatkowe, szkodliwe czynności. Konie trojańskie często podszywają się pod pożyteczne programy, jak np. zapory sieciowe, wygaszacze ekranu lub też udają standardowe usługi systemowe, jak np. logowanie.

Bomba logiczna (ang. *logic bomb*) – fragment kodu programu komputerowego umieszczony w nim bez wiedzy użytkownika i wykonujący pewne instrukcje po spełnieniu określonych warunków. Najczęściej spotykanym typem bomb logicznych są bomby czasowe (ang. *time bomb*), realizujące się o określonym czasie.

Wirus komputerowy to najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy, w przeciwieństwie do robaka komputerowego, do swojej działalności wymaga *nosiciela* w postaci programu komputerowego, poczty elektronicznej itp.

Robak komputerowy to powielający się program komputerowy, podobny do wirusa komputerowego. Robaki komputerowe w swoich kopiach mogą posiadać funkcje znane z trojanów: zamykanie, restart, wylogowanie się z systemu.

Backdoor (z ang. *tylne drzwi*) – luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania. Backdoor w systemie może być pozostawiony przez crackera, który włamał się przez inną lukę w oprogramowaniu[7].

Symulacja i modelowanie jest to użycie komputera jako narzędzia planowania bądź kontroli przestępczości. Przykładem może być symulacja procesu określenia możliwości powodzenia planowanego przestępstwa[6].

Zwalczanie przestępstw komputerowych

Zapobieganie przestępstwom komputerowym może przybierać różne formy. Cały czas prowadzone są akcje informacyjne, wykrywcze oraz podejmowane są działania w celu utworzenia spójnego systemu informacji prawnych. Zwalczanie przestępczości komputerowej zostało opisane w dwóch zaleceniach Komitetu Ministrów Rady Europy. W pierwszym zaleceniu przedstawiono zapisy, jakie powinny się znaleźć w przepisach prawa karnego, aby skutecznie zwalczać tego typu przestępstwa. Drugie zalecenie określa, jakie przepisy powinien zawierać Kodeks Postępowania Karnego, jakie powinny powstać struktury organów ścigania, by możliwe było zwalczanie przestępczości komputerowej. Wynika z tego, iż procedury stosowane w zwalczaniu przestępstw komputerowych muszą być proste i szybkie[8].

Polska wraz z innymi krajami Europy Środkowej i Wschodniej przyłączyły się do inicjatywy eEuropa+ w maju 2000 roku, która polega na podniesieniu konkurencyjności wspólnej gospodarki i zajęciu czołowej pozycji w tej dziedzinie. Środkiem do tego ma być rozbudowa infrastruktury informatycznej. W inicjatywie eEuropa+ zapisano szereg postanowień, jakie musi spełnić każdy kraj uznający tę inicjatywę. Postanowienia te określają: pobudzanie współpracy między sektorem publicznym i prywatnym w dziedzinie niezawodności infrastruktur informacyjnych, w tym, rozwoju systemów wczesnego ostrzegania, szkolenie personelu policyjnego i sądowego oraz specjalistów przemysłowych w zakresie zagadnień dotyczących zarówno przestępstw popełnianych z wykorzystaniem wysokiej technologii, jak i w zakresie bezpieczeństwa[3].

Podsumowanie

Internet postrzegany jest coraz częściej jako zjawisko społeczne i kulturowe. Liczba użytkowników Sieci równa jest sześciu największym metropoliom świata i wciąż dynamicznie wzrasta. Pojawienie się Internetu otworzyło nowe, olbrzymie możliwości dla nauki, biznesu i kultury. Zaczęły się rozwijać nowe elektroniczne dziedziny w handlu, bankowości, edukacji. Internet stał się efektywnym narzędziem pracy dla lekarza, biznesmena, naukowca, dziennikarza i wielu innych grup zawodowych. To jedna, powszechnie znana strona Internetu. Przestępczość to jego druga, ciemna strona, o której mówi się niewiele i rzadko. Wraz z nowymi możliwościami i perspektywami, jakie stwarza Internet, nadeszły nowe, nieznane rodzaje przestępczości. Dlatego najczęściej nie zdajemy sobie w ogóle sprawy z zagrożeń czyhających w Sieci, nie wiemy, jak się przed nimi bronić ani jak je zwalczać. Cybernetyczni przestępcy wykorzystują to bezlitośnie. Ich ofiarą może zostać każdy.[9] Z Internetu należy

korzystać rozważnie i mądrze, a wtedy, przy zachowaniu podstawowych zasad bezpieczeństwa, przyniesie on wiele korzyści. Te zasady to:

1. Zainstaluj program antywirusowy i regularnie uaktualniaj bazę sygnatur wirusów.
2. Zainstaluj firewall i utrzymuj go szczelnym, instalują wszystkie „łaty" do niego.
3. Sprawdź skanerem pobranym np. z http://www.grc.com/, jak bardzo podatny na atak włamywaczy jest Twój komputer.
4. Sprawdź, czy nie masz zainstalowanego spyware'u, np. aplikacją Ad-aware pobraną z witryny www.lavasoftusa.com
5. Nie instaluj programów niepewnego pochodzenia.
6. Czytaj uważnie komunikaty przeglądarki, a nie akceptuj wszystkiego w ciemno[10].

Przestępczość internetowa jest rozpowszechniona na wielką skalę, jeżeli będziemy stosować powyższe zasady bezpieczeństwa, instnieje duże prawdopodobieństwo, że ochronimy nasz komputer przed „nieproszonymi gośćmi" jakimi są hakerzy.

Literatura

[1] „Internet Co to jest?" (http://www.lo.olecko.pl/dowww/ictj.htm)
[2] Zespół Prewencji Kryminalnej Nieletnich i Patologii „Prewencja – Przestępczość Internetowa" KPP Strzelin, http://www.strzelin.policja.gov.pl
[3] Funk Ch., Przestępstwo w sieci – Hacking, http://www.dzien-e-mail.org
[4] Kliś M., Przestępczość w Internecie. Zagadnienia podstawowe, http://www.vagla.pl
[5] Kliś M., Martiszek T., Przestępstwa elektroniczne, http://www.vagla.pl
[6] Płaza A., Przestępstwa komputerowe, http://www.vagla.pl, Rzeszów 2000.
[7] Definicje pojęć zaczerpnięte ze strony: www.wikipedia.org
[8] „Piractwo komputerowe i kopiowanie okazyjne", http://www.microsoft.com
[9] Szewczyk B., Przestępczość, Wyższa Szkoła Informatyki i Zarządzania, witryna internetowa, http://stud.wsi.edu.pl/~dratewka/crime/przestepczosc.htm, 2009.
[10] Bezpieczeństwo w sieci – Internet (http://prace.sciaga.pl/20467.html)

Tomasz Prauzner

LAW AND LAWLESSNESS IN THE INTERNET

Summary

The main aim of my thesis is to show the problem of crimes in Internet. The Internet serves people some fun, science but it is the place of many different and dangerous crimes. The Hakers are used a many computers programs for example: “the horse of troy” and “the bomb of logistic”whitch can use to break into the computers. In the world exist many ways to prevent this crimes but it’s neither sufficiently good to save it.