Dorota Sokołowska

PRZESTĘPSTWA INTERNETOWE – ZARYS PROBLEMATYKI

ETAPY ROZWOJU

Rozwój techniki komputerowej, a wraz z nią błyskawiczny rozwój sieci internetowej, daje szereg możliwości wykorzystania jej w różnych celach: profesjonalnym, rozrywkowym, informacyjnym, jako medium komunikacyjne. Cybernetyczny kosmos, jak wiele innych wynalazków technologicznych, jest niewątpliwie dowodem postępu technicznego ostatnich lat, niesie ze sobą wiele udogodnień dla codziennego funkcjonowania. Z drugiej strony, dostęp do szerokiego spektrum informacji zawartych w cyberprzestrzeni może nieść pewne zagrożenia. Przestępczość związana z systemem elektronicznego przetwarzania danych rozpoczęła się wraz z pojawieniem się techniki komputerowej około1940 roku. Komputeryzacja była wykorzystywana do sterowania rutynowymi czynnościami w gospodarce
i administracji na początku lat pięćdziesiątych. Jednakże dopiero w latach sześćdziesiątych ujawniono pierwsze, a siedemdziesiątych poważniejsze wypadki oszustw, sabotażu, a także szpiegostwa gospodarczego z wykorzystaniem komputerów. W latach sześćdziesiątych rozpoczęło się masowe przetwarzanie informacji danych osobowych przez tworzenie banków danych. Niemal równocześnie z pojawieniem się w latach siedemdziesiątych otwartych systemów sieciowych rozpowszechniły się ich nadużycia określane jako hacking. Upowszechnienie komputerów osobistych w latach osiemdziesiątych spowodowało masowe zjawisko sporządzania pirackich kopii programów, a rozwinięcie sieci bankomatów, natychmiast skutkowało nadużyciami za pomocą kart magnetycznych. Zorganizowane grupy przestępcze zaczęły wykorzystywać powszechność poczty elektronicznej, mailboxów, ISDN, a także ścisłe powiązania między systemami przetwarzania danych a telekomunikacją również do celów przestępnych zarówno kryminalnych, jak
i gospodarczych, a nawet do perfekcyjnego zacierania śladów przestępstwa.

METODY PRZESTĘPCZEGO DZIAŁANIA

OSZUSTWO

Internet stwarza wprost nieograniczone możliwości na dokonywanie oszustw. Powstały już nawet wyspecjalizowane grupy przestępcze, których jedynym polem działania jest Cyberprzestrzeń. Oszustwo w sieci jest integralnie połączone
z hackingiem komputerowym, jako elementem koniecznym do dokonania tego typu przestępstwa.

Podstawowym oszustwem jest posługiwanie się skradzionym wcześniej numerem karty kredytowej. Typowa struktura gangu komputerowego, składa się
z wielu wyodrębnionych grup, z których każda ma inne zadanie. Pierwszym etapem jest zawsze zdobycie koniecznych informacji. W tym celu dochodzi do włamań do systemów informatycznych organizacji, dokonujących jakichkolwiek transakcji
w cyberprzestrzeni. Spotyka się działania bardziej prymitywne - drobni przestępcy, często bardzo młodzi ludzie, zbierają numery kart w sklepach czy restauracjach. Dysponując numerem karty, dokonuje się zakupów w sklepach internetowych, wypożycza samochody, a nade wszystko okrada banki, kasy i ubezpieczycieli. Straty ponoszone przez te instytucje w wyniku cyberoszustwa są wielokrotnie większe niż na skutek napadów i wymuszeń. Kolejnym rodzajem oszustwa jest manipulacja programem. Polega na takim przygotowaniu programu i „wszczepieniu" go do systemu, aby system wykonywał określone czynności bez woli operatora. Typowym przykładem takiej działalności, jest włamanie się do systemu bankowego i podrzucenie programu „obcinającego" minimalne kwoty z rachunków bankowych
i przesyłanie ich na jedno konto. Ze względu na olbrzymia liczbę rachunków, straty liczone są w milionach dolarów.

Innymi klasycznymi oszustwami tego typu są fałszerstwa listy płac. Po włamaniu się do systemu obsługującego taka listę, wstawia się „martwe dusze", osoby nieistniejące,

których pobory przelewane są na określone konto cyberprzestępcy. Jest to działanie skomplikowane i wymagające już dużej wiedzy informatycznej.
Odpowiedzialność karna za większość oszustw może wypływać z przepisów dotyczących klasycznego oszustwa. Jednak coraz częściej zauważa się konieczność specjalnego uregulowania tych kwestii.

HACKING - WŁAMANIE DO SYSTEMU KOMPUTEROWEGO
Jest to najbardziej swoiste ze wszystkich przestępstw, które można popełnić w Sieci. W większości cyberoszustw, cyberkradzieży, hacking jest elementem koniecznym do ich zaistnienia. Typowymi sposobami stosowanymi przez hackerów komputerowych są:

- „koń trojański"
- „back door"
- „exploit"
- IP spoofing
- „sniffing"

„**Koń trojański**" jest to program który pełni specjalne funkcje (przydatne dla hackera), udając inny program. Przykładem może być tutaj podmieniony program logujący, który poza tym że loguje użytkownika, zapisuje wprowadzone hasło do pliku, tak aby później hacker z łatwością mógł je odczytać. Stosowane są także „konie trojańskie", działające na zasadzie klient/serwer. Składają się one z programu dzięki któremu można niejako „wydawać polecenia", oraz „sługi" - zainstalowanego w obcym komputerze programu, wykonującego różnego rodzaju zadania.

„**Back door**" dosłownie „tylne drzwi". Jest to program (często koń trojański) instalowany głównie na serwerze, umożliwiający hackerowi dostanie się do niego z ominięciem zabezpieczeń. Jest to bardzo często stosowana technika, za której pomocą hacker może wielokrotnie powracać nawet na bardzo dobrze zabezpieczony serwer, nie włamując się ponownie od początku.

„**Exploit**" jest to program, który wykorzystuje różne dziury w systemach, mogący mieć wpływ na ich działanie, zawieszać je lub nawet przejąć nad nimi kontrolę. Najczęściej exploitem jest program dla Unixa lub Linuxa (czyli systemu operacyjnego nie tak rozpowszechnionego jak Windows). Jednocześnie jest to często źródło z którego każdy administrator lub hacker może się zapoznać z jego działaniem i wykorzystać go do własnych celów. Dla Windows także istnieje wiele różnych exploitów, lecz ustępują tym z innych systemów.

IP spoofing jest to bardzo skuteczna i często stosowana technika umożliwiająca podszycie się pod inny komputer. Jest kilka jego odmian - można stosować odpowiednie oprogramowanie na własnym komputerze, lecz także można odpowiednio podrzucić program do obcego komputera, dzięki któremu zamiast do tego komputera, informacje przekazywane będą do własnego. Do spoofingu należy także wysyłanie poprzez otwarty port ICQ (program do komunikacji w Sieci) dowolnych informacji, podając jako nadawcę cudzy numer identyfikacyjny.

„**Sniffing**" dosłownie „wąchacz". Jest to niezwykle efektywna technika służąca do podsłuchiwania pakietów pomiędzy komputerami. Dzięki niej można np. przechwycić wysyłane i niezwykle istotne dane, np. hasła, kody dostępu itp. Sniffer umieszczony w odpowiednim miejscu w Sieci, staje się bardzo niebezpiecznym narzędziem w rękach hackera.

Hacking sam w sobie, można zdefiniować jako łamanie zabezpieczeń dla samej przyjemności i satysfakcji pokonania barier technicznych. Nie zmienia to jednak faktu, że integralność systemu jest zachwiana i mamy do czynienia z naruszeniem prawa. Nie jest bowiem możliwe wyraźne oddzielenie hackingu nie powodującego żadnych negatywnych skutków, od hackingu w efekcie którego powstaną szkody. Najbardziej dobitnym

przykładem takiego działania, jest sprawa grupki młodych niemieckich hackerów, którzy włamali się do kilku amerykańskich systemów komputerowych, a następnie sprzedali wiedzę uzyskaną podczas cybernetycznej podróży byłej radzieckiej służbie wywiadowczej KGB. Sami „klasyczni hackerzy" twierdzą, że ich celem nie jest nigdy spowodowanie szkody, lecz tylko zabawa. Dlatego wprowadzają osobną kategorię „crackerów", którzy dokonują włamań aby uzyskiwać z tego powodu korzyści. Właściwie to dopiero działalność owych „crackerów" spowodowała, że zaczęto bardzo poważnie podchodzić do bezpieczeństwa w Sieci.
Dyskusja nad tym czy hacking powinien być spenalizowany, czy też nie, trwa nadal. Przeciwnicy penalizacji hackingu utrzymują, że ograniczanie dostępu do skomputeryzowanej informacji za pomocą zakazów karnych powoduje niebezpieczeństwo nadmiernej kryminalizacji. Natomiast zwolennicy takiej regulacji podnoszą przede wszystkim prawo użytkownika systemu do wyłącznego, niezakłóconego i zapewniającego poufność zarządzania systemem informatycznym. Ponadto nawet „nieszkodliwe" włamanie do systemu, powoduje wysokie koszty usunięcia skutków działania hackera, choćby koszty odblokowania zawieszonych programów i utrata w związku z tym danych. Nie ulega wątpliwości, że nie można pozostawić działania hackerów poza regulacjami prawnymi. Obecnie w Internecie istnieją oficjalne (!) strony organizacji hackerskich. Każdy może uzyskać tam pierwszy stopień wtajemniczenia, dowiadując się w jaki sposób włamać się np. do banku i uzyskać pieniądze. Jakkolwiek nie będzie rozwiązany sam problem hackingu, to takie działanie, z całą pewnością można traktować jako podżeganie do popełnienia przestępstwa, a nawet pomocnictwo w jego dokonaniu. Z punktu widzenia prawa karnego, zupełnie irrelewantne są sformułowania, często obecne przy wchodzeniu na takie strony. Oto napis widniejący przed wejściem na stronę hackera:
„Autor strony nie odpowiada za ewentualne szkody wynikające z niewłaściwego użycia zamieszczonych programów oraz opisów. Wszelkie materiały zamieszczone zostały wyłącznie w celach edukacyjnych, a ich zadaniem jest naświetlić tematykę związaną z hackerstwem i ochroną przed nim, ale nie mają służyć jako gotowe instrukcje do włamań, ataków itp."
Od samych hackerów możemy się też dowiedzieć, jak sami siebie definiują: Hacker to osoba zafascynowana jakimś obiektem do takiego stopnia ze pragnie znać jego każdy szczegół, oraz zasadę działania. Hacker komputerowy - to osoba zafascynowana komputerami i wszystkim co z nimi jest związane. Pragnie znać bardzo szczegółową zasadę ich działania, często po to, aby doprowadzać je do granic ich możliwości, a czasami po to aby sprawić żeby robiły rzeczy, do których nie są specjalnie przystosowane. Hackerzy bardzo uwielbiają manipulować i eksperymentować, przez co pogłębiają swoją wiedzę na dany temat, stając się jeszcze lepszymi specjalistami w danej dziedzinie.
Obok hackerów i „crackerów", w Sieci można też spotkać Phreakerów. Są to hackerzy systemów telekomunikacyjnych, znający zasadę działania aparatów telefonicznych, central, oraz doskonale orientujący się w działaniu systemów telekomunikacyjnych. Wyszukują oni luki w działaniu tych systemów po to, aby wykorzystać je do swoich celów, (np. do darmowego dzwonienia). Posługują się przy tym przede wszystkim lukami, w źle zabezpieczonym systemie przekazywania wiadomości głosowych. W momencie podłączenia się przez hackera z „automatyczną sekretarką", stwarza się możliwość wykorzystania otwartej linii telefonicznej.

SABOTAŻ KOMPUTEROWY
Pojęcie „sabotażu komputerowego" obejmuje swym znaczeniem takie zjawiska jak:
- Ø wirusy komputerowe
- Ø programy-robaki
- Ø bomby logiczne

Wirusy komputerowe to programy, które po dostaniu się do komputera, błyskawicznie rozchodzą się do innych programów i po pewnym czasie powodują olbrzymie szkody, często nieodwracalne. Dostają się one do komputerów na wszelakie sposoby - przez dysk, dyskietkę, bezpośrednio z Internetu, czy też przez E-mail. Jednak zawsze ukryte są

w jakimś programie, gdyż same będąc programem, muszą zostać otwarte, aby mogły działać. Sam fakt, iż np. dostało się wirusa nie stanowi zagrożenia, dopóki samemu nie wprowadzi się go do własnego systemu. Dlatego też cyberprzestępcy coraz lepiej maskują swoją „broń". Wirusy posiadają zdolność oddziaływania na dowolny element systemu komputerowego w szczególności:

¨ wyświetlania nietypowych obrazów na ekranie (rysunków, znaków albo napisów),
¨ 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 i zakłócanie danych w połączeniach modemowych, inicjowanie „fałszywych" połączeń telefonicznych, zmiana położenia lub kierunku działania myszki),
¨ spowalniania pracy systemu komputerowego (np. modyfikowanie przerwań sprzętowych),
¨ powodowania fizycznych uszkodzeń podzespołów systemu komputerowego.

Z każdym rokiem wzrasta liczba i rodzaj wirusów komputerowych. Wirusy można podzielić na:

a) zdolne do rozmnażania się (samo kopiowania)
b) zdolne do przechwytywania programu gospodarza podczas pracy i obejmowania kontroli nad systemem.

Wirus komputerowy stał się bardzo niebezpieczna bronią w rękach osoby, chcącej sparaliżować system komputerowy, a co za tym idzie - określoną dziedzinę życia. Wraz z coraz większym rozwojem komputeryzacji, rozpowszechnianie wirusów komputerowych, będzie stawało się coraz groźniejszym przestępstwem.
Już dziś, większość służb specjalnych na całym świecie, obawia się pojawienia się cyberterrorysty, który zamiast bomb, porywania samolotu - po prostu wprowadzi do systemu niepozorny program, który w przeciągu kilkunastu minut będzie w stanie unieruchomić całe państwo. Pierwsze doświadczenia z przestępstwami sabotażu komputerowego polegającego na rozpowszechnieniu wirusa na olbrzymią skalę mamy już za sobą.
26 marca 1999 roku w wielu skrzynkach pocztowych na całym świecie pojawił się wirus nazwany Melissa. Jego twórca skonstruował go w niezwykle przebiegły sposób. Pojawiał się on jako załącznik do poczty elektronicznej, która przychodziła od znajomych z którymi na co dzień prowadzona była korespondencja. Natychmiast po wejściu do komputera, dołączał się ten wirus do pierwszych 50 adresów z listy adresowej. Spowodował to lawinowy i nieprawdopodobnie szybki rozwój i rozprzestrzenianie się wirusa. Otwarcie wiadomości zainfekowanej wirusem Melissa powodowało, że wirus „zarażał" programy w najbardziej popularnym edytorze tekstów - Word. W ciągu 5 dni wirus zaatakował w samych tylko Stanach Zjednoczonych ponad milion komputerów osobistych.
1 kwietnia 1999 roku, członkowie specjalnego oddziału ds. przestępczości technologicznej z New Jersey i agenci specjalni FBI, aresztowali podejrzanego o stworzenie wirusa 31 letniego Davida Smitha. Ten przyznał się do zarzucanego mu czynu. 9 grudnia 1999 roku Stanowy Sąd Najwyższy, a następnie Sąd Dystryktowy orzekł najwyższą możliwą karę dla tego typu przestępstwa - 10 lat pozbawienia wolności za przestępstwo stanowe i 5 lat pozbawienia wolności za przestępstwo federalne, ponadto Smith będzie musiał zapłacić 400 tysięcy dolarów grzywny. Straty na jakie oszacowano skutki Melissy, wyniosły ponad 80 milionów dolarów. Prokurator Robert Cleary stwierdził, że wreszcie pokazano, iż wirusy komputerowe to nie jest „gra" lecz poważne przestępstwo.
Po raz pierwszy prawo karne, tak surowo zostało wykorzystane w przestępczości internetowej.

Programy - robaki - pojawiają się w sieciach komputerowych, wykorzystując łączność między komputerami i użytkownikami jako nośnik transmisji. Paraliżują one kolejne

warstwy systemu w celu przejęcia uprawnień administratora węzła sieciowego. Są podobne do wirusa, ale wytwarzają swoje dokładne kopie w całości bez potrzeby istnienia programu nosiciela. Po raz pierwszy pojawiły się w 1988 roku, kiedy amerykański student zablokował ponad 6 tysięcy komputerów, w ciągu kilku dni.

Bomby logiczne- to program komputerowy realizowany w odpowiednim czasie lub okresowo w systemie komputerowym, który określa warunki lub stany komputera ułatwiające dokonanie czynów niedozwolonych. Może ona polegać na wprowadzeniu do systemu operacyjnego komputera tajnych instrukcji (konia trojańskiego), które będą realizowane w późniejszym czasie jako tzw. bomby czasowe.

Sabotaż komputerowy, stanowi coraz większy problem, gdyż coraz większa część społeczeństwa jest uzależniona od sprawnie działającego systemu komputerowego. Na całym świecie powstały i powstają instytucje, mające przewidywać i błyskawicznie reagować na przypadki cyberterroryzmu. Według prognoz jednej z takich instytucji ze Stanów Zjednoczonych możliwe akcje cyberterrorystyczne to np.:

Ø Cyberterrorysta rozmieści kilka skomputeryzowanych bomb w mieście, wszystkie transmitują określony kod, który dociera do każdej z nich. Jeśli transmisja zostanie przerwana, bomby zostaną symultanicznie zdetonowane
Ø Cyberterrorysta będzie jednocześnie zręcznym hackerem dokona włamania do systemu finansowego państwa. Grożąc jego całkowitym paraliżem, będzie wysuwał żądania
Ø Cyberterrorysta zaatakuje system kontroli powietrznej i doprowadzi do zderzenia dwóch samolotów pasażerskich, grożąc następnymi
Ø Cyberterrorysta dokona zmian w komputerowych recepturach na podstawie których produkowane będą lekarstwa (wystarczy choćby zmiana proporcji)
Ø Cyberterrorysta zmieni zasadniczo ciśnienie w gazociągach, powodując eksplozję.
Sieć komputerowa jest wprost wymarzonym polem działania dla terrorystów.

PRZESTĘPSTWA POPEŁNIANE W INTERNECIE

Szczególną grupę przestępstw stanowią czyny, dla których Sieć nie jest immanentnym medium, podmiotem „na którym" dokonuje się naruszenie prawa, jest tylko narzędziem służącym rozpowszechnianiu. Należy tu wymienić:

Ø rozpowszechnianie treści rasistowskich
Ø rozpowszechnianie pornografii
Ø handel narkotykami i lekarstwami

Rozpowszechnianie treści rasistowskich – już w latach osiemdziesiątych sieci komputerowe były wykorzystywane przez grupy neonazistowskie takie jak: Ku-Klux-Klan, Ruch Oporu Białych Aryjczyków do głoszenia swoich poglądów. Organizacje także publikowały w Internecie nazwiska żydowskich „wrogów", z zachętą do stosowania przemocy. W Niemczech zarówno prawicowi jak i lewicowi ekstremiści jako jedni z pierwszych zaczęli używać poczty elektronicznej, aby usprawnić komunikację. Prawicowcy założyli sieć 10 mailbox-ów, zwanych „Thule-Network", w której rozpowszechniali propagandowe materiały. Bardzo szybko zaczęły powstawać gry komputerowe udostępniane publiczności, których celem była dezintegracja mniejszości narodowych i cudzoziemców. Na przykład w grze pt. „Meneger w obozie koncentracyjnym" młodzież musiała decydować czy człowiek narodowości tureckiej pierwszy miał być wysłany do pracy w kopalni, czy też natychmiast zagazowany. „Thule – Network" zostało zlikwidowane dopiero pod koniec 1994 roku przez agencję z Badenii-Wirttenbergii.

Rozpowszechnianie pornografii – jest to jedno z najbardziej nagminnych zjawisk w dzisiejszym Internecie. Ze względu na ogólną dostępność, Internet stanowi swoisty poligon doświadczalny dla wszelkich pomysłów i sposobów zarabiania pieniędzy. Jednym z najlepszych sposobów jest założenie popularnej strony, którą będzie odwiedzało wielu gości. Pozwoli to na umieszczenie dużej ilości reklam, banerów, odnośników. Jedną z największych widowni mają strony z zawartością stron pornograficznych. Problem pornografii jest problemem zawsze wywołującym gwałtowne dyskusje. Nie wdając się w nie, należy zauważyć, że w Internecie nie ma, jak na razie, możliwości kontroli dostępu do stron pornograficznych. Nawet jeżeli przyjmiemy, że osoba dorosła ma

prawo oglądać co zechce (pod warunkiem, że nie jest pokazywane przestępstwo), to obecnie nie da się zagwarantować zamknięcia dostępu przed dziećmi. Nie ma bowiem sensownego systemu weryfikacji wieku.

Pornografia w Internecie istnieje w wielu postaciach: listy, dyskusje, zdjęcia, przekazy „na żywo" poprzez kamery podłączone do komputera. O ile problem „zwykłej pornografii" jest trudny do rozwiązania, to z całą pewnością na błyskawiczną reakcję zasługuje problem pornografii z wykorzystaniem dzieci. Jedną z najnowszych form rozpowszechniania pornografii w Internecie, jest produkcja i dystrybucja zdjęć, w których nieletni zostali wygenerowani komputerowo. Są tylko tworem grafiki komputerowej.

Pedofile znaleźli w Sieci warunki dokonywania i propagowania przestępstw seksualnych z udziałem dzieci oraz szybki sposób dotarcia do potencjalnych ofiar na całym świecie. Wykorzystują oni każdy sposób, by zbliżyć się do swej ofiary – np. podają się za nastolatków w grupach dyskusyjnych, przebywają w „chat-roomach" dla młodzieży. Nawiązują kontakt, który potem przeradza się w zależność fizyczną, często niszcząc psychikę dziecka.

Handel narkotykami i lekarstwami – obecni handlarze narkotyków coraz częściej używają Internetu, jako miejsca przeprowadzania swoich transakcji. Wykorzystują do tego formułę sieci jako „sklepu". W Internecie możemy spotkać trzy rodzaje „aptek":

a) Odpowiednik tradycyjnych aptek, w których wymagane jest przedstawienie ważnej recepty od lekarza (w postaci faksu, lub w formie zeskanowanego e-mailu) przed dostarczeniem wymaganego lekarstwa. Choć już tutaj pojawia się problem, gdyż niektóre leki mogą być całkowicie legalne w jednym kraju, a w innym mogą nie być dopuszczone do używania.

b) Apteki, w których można za pośrednictwem Sieci uzyskać „diagnozę" będącą podstawą uzyskania recepty i dostarczenia następnie leku, całkowicie bez fizycznego kontaktu z lekarzem. Takie apteki zazwyczaj używają sieciowego kwestionariusza lekowego, w którym „pacjent" opisuje swój stan zdrowia, obecnie używane leki i historię choroby. Na tej podstawie lekarz wydaje „diagnozę". Wielokrotnie może stanowić próbę uniknięcia ewentualnej odpowiedzialności karnej, poprzez powoływanie się na wprowadzenie w błąd przez klienta, który będąc całkowicie zdrowy chciał uzyskać określone lekarstwa.

c) Trzecią kategorię stanowią apteki, gdzie bez jakichkolwiek formalności można zakupić wszelkie lekarstwa. W tych przypadkach oferujący takie usługi, jest często zupełnie nieznany, a ponadto wykorzystuje wszelkie możliwe sposoby aby ukryć prawdziwe miejsce działania i utrudnić jego wykrycie. Tym sposobem handlarze narkotyków znajdują miejsce działania, które jest doskonała okazją do rozszerzenia terytorium ich działania.