Motto:

„*Daj mi wystarczająco dużo czasu, a dostanę się,*
gdzie tylko zechcesz nawet do Twojego prywatnego
notesu, który nosisz w marynarce ...
Oczywiście chodzi o notes elektroniczny!”

Michael L. Puldy
(szef zespołu Emergency Response Service)

Podziękowania

Dziękuję moim przyjaciołom, kolegom i rodzinie za wsparcie, którego udzielili mi podczas zbierania informacji i pisania tej książki. Dziękuję żonie za cierpliwość, a dzieciom — Weronice i Jakubowi — dziękuję za to, że kochają nadal ojca, którego prawie nie widywali przez lata pracy nad książką. Na moją wdzięczność za pomoc w tłumaczeniu tekstów zasłużyli sobie: Janusz Jaworski, Maria Chomont, Edward Zys, Halina Zyzańska oraz mój uczeń — Damian Till. Ogromnego wsparcia udzieliła mi wspaniała koleżanka z pracy Irena Karwala, która była pierwszą i nieocenioną recenzentką książki. Nie tylko udzielała mi wielkiego wsparcia redakcyjnego, ale także dodawała mi otuchy do dalszej pracy. Dziękuję więc za nieustanne zachęty i mądre rady.

Jestem dłużnikiem Was wszystkich!

D.D.

Wprowadzenie

U progu XXI wieku postęp cywilizacji i rozwój nowych technologii sprawiły, że zasypani wprost zostaliśmy kolejnymi wynalazkami. Wszystkie one miały ułatwić nam życie... Czy tak jest w istocie? I tak, i nie. Wystarczy przyjrzeć się jednemu z tych „cudów techniki i myśli dwudziestowiecznej", jakim niewątpliwie jest Internet. Przygotowany z myślą o potrzebach wojska upowszechnił się już na tyle, że liczba jego użytkowników przekracza najśmielsze oczekiwania projektodawców. Popularność wciąż rośnie. Niedługo już wszyscy — zaczynając od prezydenta czy premiera, a na uczniu szkoły podstawowej kończąc — dysponować będą swoją stroną WWW czy chociażby własnym e-mailem. Bowiem życie coraz intensywniej zaczyna się toczyć przeciążonymi kablami koncentrycznymi, skrętkami dwużyłowymi nieekranowymi czy światłowodami.

Jak to zwykle bywa, w tym wcale nie tak łatwym świecie cyberprzestrzeni możemy spotkać „nowicjuszy", którzy po uruchomieniu przeglądarki internetowej nie wiedzą, jak wykorzystać to narzędzie, i „specjalistów" doskonale orientujących się w prawidłach, rządzących wirtualną rzeczywistością. Właśnie oni bywają groźni. Bo naszym programom zagrażają nie tylko wirusy, ale przede wszystkim komputerowi przestępcy — hakerzy, czyli technoanarchiści cyberprzestrzeni. Ta książka jest właśnie o nich, o ich metodach pracy, a także o motywacji, która skłania do „łamania systemów". Opisuje w miarę szczegółowo przypadki z ostatnich lat w aspekcie technicznym, moralnym i prawnym. Ukazuje najwybitniejszych hakerów, którzy uważają, że granice należy przekraczać, a zapory — omijać. Słowem — „sięgać, gdzie wzrok nie sięga". Ale romantyczna maksyma w cyberprzestrzeni traci metafizyczny kontekst. „Niepokorni internauci" najczęściej włamują się do systemów z przyczyn trywialnych — dla frajdy lub dla satysfakcji, której w realnym świecie nie potrafią osiągnąć. Wielu z nich to życiowi nieudacznicy, nieśmiali bohaterowie wymyślanych historii, tych, co rzadko znajdują spełnienie. Są to rozgoryczeni marzyciele. Włamując się do kolejnych systemów i obalając piętrzące się bariery, potwierdzają więc własną wartość. W tym właśnie odnajdują siebie, swoją godność i tożsamość. Są biało-czarni dokładnie tak jak bohaterowie wersternów, które oglądali w dzieciństwie i nie mogli odtworzyć w młodości. Ale przepełnieni celuloidowymi ideałami wielbiciele iluzji nie zaprzestali walki z wyimaginowanymi Indianami, wciąż ich zabijają, by na zdobytych ziemiach założyć „Nowy Kraj", wolny i nieograniczony jak niegdyś Ameryka. Może dlatego bywają nazywani „cybernetycznymi kowbojami klawiatury"... Po ich stronie jest przecież siła, a co się z tym wiąże — możliwość ustanawiania nowych praw. Czerpią więc radość ze świadomości, że

zdobywają dostęp do mocno strzeżonych tajemnic, że są sprytniejsi od pseudospecjalistów, zatrudnionych na stanowiskach administratorów systemów w agencjach rządowych lub słynnych korporacjach. Cieszą się, że obnażają prymitywizm pozornie wyrafinowanej kultury. Ale czasem, gdy zwiedzie ich brawura, zostają przyłapani na „gorącym uczynku". Co się wtedy dzieje? Może się to wydać zaskakujące, ale nie zawsze spotykają ich restrykcje prawne. Nieraz zdarza się, że hakerzy zostają zaproszeni do grona superspeców komputerowych, zdobywają uznanie, duże pieniądze, trafiają do komputerowego panteonu i stają się elementami systemu, z którym tak intensywnie walczyli.

Jednak bardzo często „przekwalifikowany" haker traci szacunek i podziw współwyznawców. Bo wiele lat temu fakt posiadania tego tytułu był prawie tak samo ważny jak nagroda Nobla. Splendor nadali mu ludzie penetrujący Sieć, dla który świat zero-jedynkowych wartości nie miał tajemnic. Współcześnie jednak termin ten kojarzy się z przestępstwem, łamaniem prawa. Bo trzeba pamiętać, że wszelkie złe konotacje zawdzięcza mediom, szarym użytkownikom i wreszcie samym hakerom. Kiedyś był to bardzo szczelnie zamknięty, całkowicie elitarny świat, do którego dostęp był dany tylko nielicznym użytkownikom Uniksa. Rozwijając konsekwentnie swoje komputerowe umiejętności, właśnie oni „zbudowali" dzisiejszy Internet i wiele innych systemów komputerowych, do których teraz niemal każdy może wejść, skopiować i użyć exploity, w celu nieupoważnionego dostępu do systemu. Bo dzisiaj „Eden Hakerów" praktycznie jest otwarty dla każdego. Gościnnie zaprasza do przestąpienia jego progów.

Rodzi to niezliczone zagrożenia i ustawiczne naruszanie prawa stanowi drugą, ciemną stronę Internetu, o której mówi się niewiele i niezmiernie rzadko. Dlaczego? Bowiem wraz z nowymi możliwościami i perspektywami, jakie stwarza to nowe „medium informacyjne", nadeszły nowe, nieznane rodzaje przestępczości, funkcjonujące w cyberprzestrzeni. Najczęściej nie zdajemy sobie w ogóle sprawy z zagrożeń czyhających w Sieci, nie znamy skutecznych sposobów obrony przed nimi ani metod zwalczania ich. Nie wiemy nawet, czego się bać. „Cybernetyczni przestępcy" wykorzystują to bezlitośnie. Ich ofiarą może zostać każdy — od niewinnej nastolatki rozmawiającej na IRC-u po specjalistę w dziedzinie bezpieczeństwa w Internecie, od małej firmy, providera internetowego czy firmy telekomunikacyjnej po wielkie światowe koncerny, takie jak Microsoft czy Netscape, od niewielkich szkół po najwyższe i najważniejsze instytucje rządowe (Pentagon, NASA, NSA itd.). Nikt nie jest bezpieczny, każdy może stać się ofiarą sieciowego podziemia.

Według najnowszych statystyk FBI w ubiegłym roku w Stanach Zjednoczonych każdego dnia zgłaszanych było około 30-40. spraw dotyczących naruszenia prawa w Internecie. Ich liczba rośnie z roku na rok w zatrważającym tempie. I chociaż kilka lat temu liczba zgłoszonych przestępstw wynosiła w ciągu całego roku niewiele ponad 600, prognozy na następne lata mówią już o 140-200. przypadkach włamań dziennie (ze wszystkich zgłaszanych wniosków tylko 31% uznawanych jest za uzasadnione lub istotne i wobec nich podejmowane są działania operacyjne). Dane te to jedynie wierzchołek góry lodowej, bowiem statystyki wskazują, że tylko 10% włamań do sieci korporacyjnych, kradzieży informacji i defraudacji jest w ogóle zgłaszanych. Najczęściej nie są one ujawniane w obawie przed zniszczeniem dobrej

opinii firmy, a co się z tym wiąże — utratą klientów lub są bagatelizowane w przekonaniu, że ich sprawcy i tak nie zostaną ujęci. Co tydzień liczba popełnianych przestępstw wzrasta o 4,5% . Jednocześnie tylko 2-3% spraw o naruszenie prawa obowiązującego użytkowników Internetu kończy się wyrokiem skazującym. Dzieje się tak głównie z powodu „luk" w przepisach i niedostosowania istniejącego prawa do „cybernetycznej" rzeczywistości. I coraz to inni „włamywacze" zdobywają kolejne systemy, bowiem wciąż pozostają bezkarni. Straty spowodowane przez cybernetyczne podziemie sięgają miliardów dolarów. Firma Ernst&Young podaje, że w przybliżeniu wynoszą one około pięciu miliardów dolarów rocznie, zaś średnia wartość przestępstw popełnianych za pośrednictwem Sieci wynosi 90000 USD. (Według SEARCH straty te są znacznie większe i dochodzą do czterdziestu miliardów dolarów). Same tylko firmy telekomunikacyjne i operatorzy sieci komórkowych w wyniku kradzieży i udostępnieniu w Internecie numerów kredytowych kart telefonicznych ponieśli straty rzędu pięćdziesięciu milionów dolarów. Mogą im pozazdrościć producenci oprogramowania, których straty spowodowane nielegalnym kopiowaniem i dystrybucją ich produktów w Internecie szacowane są przez Software Publishers Association na blisko 2 miliardy dolarów. Według SPA od początku istnienia Internetu firmy te straciły już ponad 7,4 miliarda dolarów. Liczby te są przerażające, a trzeba mieć na uwadze, że wciąż się zwiększają.

Ale straty wyrządzone przez crackerów mogą być jeszcze dotkliwsze. Jakiś czas temu kilku z nich w geście protestu przeciwko łamaniu praw człowieka w Chinach unieruchomiło chińskiego satelitę komunikacyjnego. Inna grupa — również w geście protestu, który tym razem wymierzony był przeciwko próbom jądrowym dokonanym przez Indie — włamała się do systemu komputerowego Bhabha Atomic Research Center w Bombaju i zdezorganizowała funkcjonowanie poczty elektronicznej, wykorzystywanej w komunikacji pomiędzy naukowcami Centrum. A są to tylko pojedyncze przypadki naruszenia systemów informatycznych instytucji i organizacji rządowych. W 1995 roku zanotowano 250 000 włamań do serwerów Departamentu Obrony Stanów Zjednoczonych i 120 000 do serwerów NASA (wiele z nich zakończonych pomyślnie). Nie wiadomo dlaczego, szczególną estymą hakerzy darzą komputery Pentagonu, które jak pokazuje rzeczywistość, nie są stuprocentowo odporne na ataki z zewnątrz. Skoro więc internetowe podziemie jest w stanie dostać się na tak strategiczne serwery, to już tylko jeden krok pozostał do powstania cybernetycznych terrorystów, którzy mogliby szantażować całe rządy i światowe organizacje. Wiele wskazuje na to, że nie jest to tylko teoria. Dlaczego tak się dzieje?

Aby odpowiedzieć na to pytanie, trzeba się przyjrzeć „sieciowym przestępcom". Internet jest z całą pewnością domeną młodego pokolenia, przed którym komputer nie ma tajemnic. Właśnie oni — młodociani poszukiwacze mocnych wrażeń — stanowią trzon „cybernetycznego podziemia". Zdaniem wielu psychologów i socjologów jest wśród nich zakompleksiona młodzież, szukająca potwierdzenia swojej wartości, ale często zdarza się, że są to osoby o ponadprzeciętnym IQ, które w pracy z komputerem szukają ucieczki od szkolnej nudy. Dla innych motywem działania jest zabawa, choć są i tacy, którzy walczą o idee (np. idea freeware — Richard Stallmana), protestują przeciwko funkcjonowaniu różnych organizacji, a nawet rządów. Podobno funkcjonuje w tym świecie zależność, która prowadzi do wniosku, że im haker starszy, tym niebezpieczniejsze są pobudki jego działania. Wielu z nich szybko bowiem rezygnuje z satysfakcji, jaką daje znajomość zasad działania systemu i stara się na-

byte umiejętności wykorzystać w praktyce. To prowadzi do nieuniknionego końca wielkich złudzeń — na swój sposób wzniośli hakerzy stają się pospolitymi przestępcami, którzy są nastawieni na czerpanie zysku ze swojej działalności. Niekiedy zostają cybernetycznymi szpiegami gospodarczymi, wykradającymi na zlecenie dane i informacje z serwerów wskazanych firm. Dużą grupę stanowią tu osoby zwolnione lub niezadowolone z warunków pracy w swojej macierzystej placówce, twórcy oprogramowania, administratorzy, osoby mające dostęp do informacji i zabezpieczeń w swoich firmach. Motywem wielu działań jest seks i pornografia. Ale to domena pseudohakerów. Z czasem większość z nich i tak robi karierę. Sprawdzają się doskonale jako specjaliści od bezpieczeństwa danych w poważnych firmach, bankach, instytucjach, które zatrudniają ich świadomie i celowo.

Jak widać — rozpiętość przestępstw popełnianych za pośrednictwem Internetu jest nie tylko znaczna, ale również niezwykle zróżnicowana. Łatwo zauważyć, że wiele z nich zostało przeniesionych do Sieci z życia codziennego. Są to zatem:

- piramidy finansowe;
- wyłudzenia (czyli wszelkie działania zaczynające się magiczną formułą „wyślij pieniądze, a otrzymasz to czy owo”);
- puste obietnice wielkich zysków zdobytych bez odpowiedniego nakładu pracy i inwestycji;
- szeroka oferta materiałów niezbędnych dla prowadzenia domowego biznesu;
- fałszywe obietnice otrzymania karty kredytowej;
- obietnice darmowych z pozoru „prezentów”;
- reklamy tanich książek, zazwyczaj poradników, które nigdy nie docierają do adresata;
- usługi, które nigdy nie zostają wykonane;
- loterie;
- ruletki;
- zaproszenia do udziału w konkursach, w których nigdy nie ma zwycięzcy (ani głównej nagrody).

Przestępstwa te — określane terminem *scaming* — są popełniane najczęściej, lecz ich szkodliwość ogranicza się na ogół do utraty niewielkiej sumy pieniędzy, strat natury moralnej i zdenerwowania. Jednak zdarzają się przestępstwa znacznie groźniejsze. Z pewnością wiele osób słyszało o hakerach czy choćby wirusach komputerowych, ale nie wszyscy wiedzą, co to jest warez, koń trojański, mailing bomb albo czym może grozić cracking, phreaking czy też carding .

National Computer Crime Squad — specjalna komórka FBI, której celem jest wykrywanie i zapobieganie wszelkiego rodzaju cybernetycznym przestępstwom — ustaliła osiem rodzajów przestępstw popełnianych w Internecie. Są to:

- włamania do sieci komputerowych bądź serwerów;

- szpiegostwo gospodarcze z wykorzystaniem Internetu;
- piractwo komputerowe (warez);
- e-mail bombings;
- kradzież i wykorzystywanie cudzych haseł;
- Spoofing;
- oszustwa z wykorzystaniem kart kredytowych (carding);
- phreaking.

Opisowi niektórych z nich poświęcona jest ta książka.