Hakerzy.
Technoanarchiści cyberprzestrzeni

Autor: Dariusz Doroziński
ISBN: 83-7197-463-9
Format: B5, stron: 368

Jest to książka o „ciemnej stronie Internetu". Hakerów nazywa się w Stanach Zjednoczonych „cybernetycznymi kowbojami klawiatury". Czy są romantycznymi wojownikami bezprzymiotnikowej wolności, czy przestępcami? Niniejsza pozycja jest próbą odpowiedzi na to pytanie. Istotną zaletą książki jest wyjaśnienie terminologii używanej w branży specjalistów od bezpieczeństwa sieci. Można się z niej także dowiedzieć m.in.:

- jak wielkie straty ponoszą światowe koncerny z powodu działalności hakerów,
- jak zminimalizować ryzyko włamania do swego komputera,
- czy realne jest wykorzystanie Internetu przez politycznych terrorystów,
- jak ustrzec się oszustów posługujących się Internetem, by „łowić" ofiary,
- dowiedzieć się, co oznaczają takie pojęcia jak: warez, koń trojański i mail bombing oraz jakie zagrożenie dla użytkowników może spowodować cracking, phreaking i carding.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 1.
Niejasności terminologiczne

Słowo *haker* jest jednym z tych słów, które wciąż jeszcze pobudza wyobraźnię i wywołuje ten sam dreszczyk emocji wśród ludzi na co dzień stykających się z komputerem, jak i robiących to okazjonalnie.

Termin ten zwykle kojarzy się dość jednoznacznie. Najczęściej *haker* postrzegany bywa jako przestępca, niebezpieczny maniak komputerowy, którego dla dobra ludzkości należałoby zamknąć w więzieniu. Takie pojmowanie słowa — może i nie do końca pozbawione uzasadnienia — jest moim zdaniem niewspółmierne do rzeczywistości. Błędne rozumienie motywacji *hakerów*, które zmuszają ich do takiego, a nie innego działania, owocuje wciąż nowymi opisami i rodzi rozmaite mity, krążące w komputerowym światku. Sądzę, że przyczyn takiego stanu rzeczy doszukiwać się można w sztucznym nagłośnieniu problemu, za które odpowiedzialność ponosi wielu dziennikarzy i reporterów poszukujących sensacji. Jednak „prawda o hakerach" zdecydowanie różni się od obiegowych teorii.

Kim zatem są hakerzy i czym się zajmują? Gdyby zapytać ich samych, co oznacza ten termin, prawdopodobnie odpowiedzieliby, że chodzi o cieślę lub stolarza, który w swojej pracy korzysta z siekiery. Może się to wydać zaskakujące, ale właśnie takie jest pierwotne znaczenie tego słowa. Prócz tego — nieco siermiężnego określenia — pojawiają się jednak inne. W środowisku „świadomych użytkowników Sieci" funkcjonuje równocześnie kilka obiegowych definicji tego słowa. Co ciekawe — żadne z nich nie określa osobnika penetrującego komputery i sieci komputerowe w celach destrukcyjnych czy dezorganizacyjnych. Taką działalność przypisuje się innym użytkownikom Sieci. Wśród niech najczęściej wymieniani są crakerzy (choć czasem niesłusznie) i to właśnie oni — zdaniem niektórych — są źródłem złego rozumienia właściwych intencji działalności hakerów. Tak więc crakerzy nie są lubiani przez resztę komputerowej społeczności. Nie ma w tym nic dziwnego, gdyż są poniekąd główną przyczyną negatywnych opinii krążących wokół komputerowych specjalistów.

Mimo że słowo to zostało już wcielone do języka polskiego i określona została jego ortografia, w leksykonach na próżno poszukiwalibyśmy wyjaśnienia, które rozwiałoby wszelkie wątpliwości. Słownik współczesnego języka polskiego definiuje słowo haker jako: osobę włamującą się do programów komputerowych. Jak widać określenie to nie jest precyzyjne i więcej wiadomości dostarczyć nam może notka zamieszczona w *Wielkim słowniku angielsko-polskim* sygnowanym przez Jana Stanisławskiego:

hack:

1. po/siekać, po/rąbać, po/ciąć, po/krajać; to hack one's chin- zaciąć/nać się (przy goleniu);
2. kop-nąć/ać (przeciwnika) w goleń;
3. pokiereszować (pacjenta); pokrajać nieudolnie (pieczeń);
4. obciosać/ywać;
5. kaszleć suchym (urywanym) kaszlem;

hack (*er*) — cieśla lub stolarz, który w swojej pracy korzysta z siekiery.

Dodatkowe informacje znaleźć możemy w słownikach zachodnich, ale i tu nie spotkamy się z jednoznacznym określeniem. Na przykład według *The Little Oxford Dictionary haker* to „entuzjastyczny użytkownik komputera". Jak można przypuszczać w tym określeniu odzwierciedlenie znajduje narosła wokół hakerów legenda z początku lat osiemdziesiątych. Jednak słownik *Longmana* uważa już hakera za „kogoś, kto jest w stanie używać lub modyfikować informacje zgromadzone w obcych komputerach". Bezpowrotnie znika więc dawny entuzjazm. Natomiast w sygnowanym przez samych hakerów *Jargon Dictionary* słowo to posiada aż osiem znaczeń. Siedem kolejnych określeń przedstawia hakera jako „kogoś, kto uwielbia badać każdy szczegół systemu komputerowego", „obsesyjnego programistę", „eksperta od dowolnego programu". Jak widzimy następujące po sobie definicje wzajemnie się wykluczają i stają się przyczyną zamętu terminologicznego.

Słowo *haker* jest zatem bardzo pojemne semantycznie. Najczęściej jednak jego synonimem bywa pirat komputerowy, który zajmuje się poszukiwaniem rozmaitych sposobów dostępu do zabezpieczonych programów, systemów komputerowych lub baz danych. Mimo że biorąc pod uwagę historię tego wyrazu, należałoby wiązać z nim kogoś, kto świetnie zna system i potrafi „zmusić" komputer do rzeczy niemożliwych, kogoś, kto potrafi ominąć wszelkie zabezpieczenia, by dostać się do programu, słowem „haker" określają siebie prawie wszyscy ludzie, lubiący „buszować" w Sieci. Nawet ci, którzy zdolni są jedynie do uruchamiania cudzych programów, do łamania zabezpieczeń i niszczenia danych. Znawcy tematu próbują ich odróżnić od hakerów, używając określenia *cracker* — „łamacz". A różnica między nimi jest zasadnicza i najprościej można ją określić, uciekając się do obrazowego zestawienia działalności Robin Hooda i zbrodni Kuby Rozpruwacza. Jak widać rozpiętość jest dość duża, gdyż *cracker* to programista włamujący się do programów lub systemów komputerowych w celu ich uszkodzenia po to tylko, by poczuć dreszcz emocji lub osiągnąć pewien zysk materialnych.

Aby zatem pojąć właściwie istotę działań hakera, trzeba przedrzeć się przez obiegowe stereotypy, rozpowszechniane masowo przez media. Bo haker nie jest złowrogim osobnikiem, który czyha tylko na odpowiedni moment, by włamać się do systemu, zniszczyć jego zabezpieczenia i wykorzystać zdobyte dane w celach przestępczych. Wręcz przeciwnie. Słowo „haker" pierwotnie określało kogoś, kogo interesuje przede wszystkim potencjał komputera (zarówno od strony sprzętowej, jak i programistycznej), kogoś, kto z pasją wyszukuje różne luki w zabezpieczeniach systemów operacyjnych po to, by wkraść się do określonych systemów i przejąć nad nimi kontrolę (np. za pomocą napisanego do tego celu programiku tzw. *exploita*). Reasumując — słowem tym nazywamy kogoś, kto przekraczając istniejące granice, zwiększa możliwości, kogoś, kto programuje dla samej przyjemności poznania. Bowiem termin *hak* oznacza inteligentny, z polotem napisany program. Tak więc w odróżnieniu od tego, co można usłyszeć, hakerzy nie są maniakalnymi przestępcami, lecz bardzo często genialnymi programistami.

Hakerem jest zatem osoba, która w przeciwieństwie do większości użytkowników komputerów chcących poznać wybrany zakres programu niezbędnie potrzebny do pracy, zajmuje się przeszukiwaniem i rozpracowywaniem szczegółów systemów programistycznych oraz sprawdzaniem ich możliwości. Termin ten może także oznaczać przynależność do międzynarodowej społeczności definiowanej jako „sieć" lub „cyberprzestrzeń".

W każdym przypadku jednak wiąże się z nim dogłębna, intelektualna eksploracja potencjału systemu komputerowego. Ale nie tylko, gdyż działalność hakera ma też wymiar — by tak rzec — metafizyczny. Zasadza się bowiem na przekonaniu, że w komputerach odnaleźć można piękno, a każdy program może dać wyraz myślom i intencjom programisty, że elektronika i telekomunikacja są nadal w większości terenami niezbadanymi, które stawiają wyzwania poszukiwaczom przygód. Są więc ludzie, dla których hakerstwo jest jak wdychanie powietrza, jak spontaniczność, która sprawia, że życie otwiera nieograniczone możliwości rozwoju jednostki.

Podsumowując zatem rozważania, można pokusić się o próbę stworzenia kilku nowych definicji, które ze względu na rodzaj wykonywanych działań pozwolą nam określić specyfikę bywalców cyberprzestrzeni. Pierwszą i najbardziej godną uwagi grupę tworzą *hakerzy.* Ich charakterystyczne cechy współtworzy miłość do komputerów i cyberprzestrzeni, umiejętność łamania różnego rodzaju zabezpieczeń i zamiłowanie do programowania, podporządkowanie „cybernetycznej podróży" zamiarom poznawczym, a nie destrukcyjnym, świetna znajomość systemów operacyjnych komputera i podstawowych języków programowania, opracowywanie programów kontrolujących integralność innych programów, dążenie do ulepszenia tego, co już istnieje, czyli swoista tendencja do poprawiania świata.

Drugą, równie liczną, ale nieporównywalnie bardziej niebezpieczną grupę stanowią *crackerzy.* Bardzo rzadko łamiąc zabezpieczenia, piszą oni własne programy. Zwykle posługują się cudzymi narzędziami. Nie używają ich do zwiększenia bezpieczeństwa, ale do jego burzenia. Znają luki, różne tricki, umożliwiające im przejęcie kontroli nad systemem. Często ich największą przyjemnością jest możliwość szkodzenia innym. Przyczyniają się więc do tego, że programiści zwiększają ilość zabezpieczeń programów przed nielegalnym kopiowaniem.

Podróżując po cybernetycznej przestrzeni wcześniej czy później spotkamy również *phreakerów*, czyli domorosłych specjalistów zajmujących się łamaniem zabezpieczeń telefonicznych i uzyskiwaniem gratisowych połączeń. To subkulturowe zjawisko miało swego czasu w USA duży zasięg, co zaowocowało wieloma publikacjami, które ukazały się na długo przed upowszechnieniem się komputerów osobistych. Działania *phreakerów* cieszyły się na początku poparciem opinii publicznej niechętnej wielkim koncernom w nie mniejszym stopniu niż nasi abonenci praktykom Telekomunikacji Polskiej S.A.

Po wielu latach spędzonych w „podziemiu", phreakerzy odnoszą w Polsce spektakularne sukcesy. Czasem udaje im się więc uzyskać poprzez Internet dowolnie odległe połączenie, a nawet wysłać faks na drugi koniec świata po kosztach rozmowy miejscowej. Natomiast w przypadku, gdy phreaker posiada umiejętności elektroniczne, bez trudu zbudować może małego *Tone Dialera* i bezpłatnie dzwonić, gdzie tylko zechce.

Kolejną grupę tworzą *piraci komputerowi*, którzy rozpowszechniają programy łamane przez crackerów. W gronie tym najczęściej pojawiają się zwykli paserzy, gromadzący programy „rozprute" przez innych i odsprzedający je za relatywnie niskie (w stosunku do cen oryginalnych produktów) sumy, co przy nieznacznych kosztach własnych (nie biorąc pod uwagę ryzyka) bywa źródłem sporych dochodów. Skala rozpowszechnienia tego procederu jest w dalszym ciągu bardzo duża. Tak więc z punktu widzenia prawa wszyscy piraci komputerowi są przestępcami, a ich motywacja nie ma żadnego znaczenia. Bez względu na to, czy robią to dla zysku, czy też wiedzie ich chęć oddania bezinteresownej przysługi, czekają ich takie same konsekwencje.

Innym rodzajem przestępczej działalności, z którym możemy się zetknąć w Sieci jest *carding* — egzotyczna rozrywka polegająca na specyficznej zabawie z kartami kredytowymi. Istnieją tu dwie możliwości. Pierwszą jest zdobycie prawdziwych numerów karty, a drugą — wygenerowanie ich. W następstwie obydwu można zamawiać i kupować rozmaite produkty, posługując się czyjąś kartą.

Potomkowie „rewolucji elektonicznej"

Hakowanie może być rozrywkowym i edukacyjnym zajęciem. Sprowadza się bowiem do nieupoważnionego wejścia do systemu komputerowego i penetrowania jego zawartości, co jest efektem myślenia dedukcyjnego. Hakerzy, których poznałem zbierając informacje o „sieciowym undergroundzie", wyjaśniali mi kolejno zasady hakowania. Głównym celem jest tu przede wszystkim pogłębienie wiedzy o oprogramowaniu komputerów, o Sieci, a co się z tym wiąże — zwiększanie swoich umiejętności. Dla prawdziwego hakera sam proces „włamywania" jest dużo bardziej podniecający i satysfakcjonujący niż zdobyte konta czy pliki odkryte w zabezpieczonych, odległych systemach.

Wydaje się nawet, że hakerów można nazwać bezpośrednimi „potomkami" telefonicznych phreakerów sprzed dwudziestu lat, czyli z czasów, gdy młodziutka wówczas, siedemnastoletnia Susan Headley z garstką innych zapaleńców rozpoczęła swoje „podróże telefoniczne" do Kalifornii.

Jako cel obrała wtedy lokalną firmę telefoniczną, wykradła potrzebne informacje i udostępniała je w Sieci. Możliwe, że to właśnie posunięcie zainicjowało rozwój „sieciowego podziemia".

Warto wspomnieć, że w końcu lat 60. zaczęły powstawać eksperymentalne sieci (np. *ARPANET — Advanced Research Projects Agency Network*). Fakt ten stał się przyczyną ruchu, którego nieco później nie dało się już zahamować. Zainteresowania hakerów wykroczyły bowiem daleko poza ich prywatne komputery. Nie musiało upłynąć dużo czasu, by zajęli miejsca przy uniwersyteckich terminalach, a wówczas stali się uprzywilejowanymi jednostkami. Byli przecież w centrum „rewolucji elektronicznej", mieli dostęp do uczelnianych zasobów i mogli wykorzystywać terminale do pracy.

Tak właśnie zaczynała się historia wielu z nich, a między innymi — słynnego dzisiaj Billa Gatesa. Najbogatszy współcześnie człowiek Ameryki w latach młodzieńczych był prymusem i w ten sposób wspominają go nauczyciele i koledzy z lat szkolnych. Wychowany na powieściach popularno-naukowych Edgara Rice'a Burronghsa i Isaaca Asimova, wybitny intelekt Gatesa nie zawsze jednak ułatwiał mu kontakty z kolegami z klasy. Nie dziwi zatem fakt, iż komputery — a przede wszystkim zwiększające się nieustannie możliwości — urzekły młodocianego adepta sztuki informatycznej, który w swym zwykłym, codziennym życiu nie zawsze mógł się spełnić. Miał bowiem trudności ze znalezieniem wśród rówieśników kogoś, kto byłby w stanie dotrzymać mu kroku w wyczynach matematyczno-logicznych. Spotkanie z „magicznym pudełkiem" stało się dla Billa najważniejszym wydarzeniem w życiu. Zaczął więc pisać błyskotliwe programy komputerowe. Bardzo szybko zauważył, że to właśnie monitor komputera stanowi swoiste lustro dla jego talentu.

Było to jednak niedostępne i bardzo duże lustro, gdyż pod koniec lat sześćdziesiątych komputery miały tak olbrzymie rozmiary, że często nie mieściły się w jednym pokoju. Na rynku konkurowało ze sobą dwóch producentów: IBM i DEC (*Digital Equipment Corporation*). Jesienią 1968 roku Bill Gates i jego najbliższy przyjaciel Kent Evens rozpoczęli naukę w liceum Lakeside, którego dyrekcja przydzielała swoim uczniom godziny, w czasie których mogli oni połączyć się z mikrokomputerem PDP-10. W efekcie tych udogodnień młody Gates miał zapewniony stały dostęp do sprzętu informatycznego i bardzo szybko odkrył w sobie niepohamowaną pasję do programowania. Po lekcjach razem z kolegą spędzał długie godziny w sali z terminalami. Tam spotkał Paula Allena, kolegę z trzeciej klasy licealnej. Między trójką chłopców nawiązała się przyjaźń. Młodego Gatesa pociągało tworzenie programów mających wartość praktyczną i pogrążył się prawie bez reszty w programowaniu gry Monopoly. Paula natomiast bardziej interesowały subtelności asemblera (języka programowania). Poczynania chłopców sprawiły, iż budżet roczny szkoły nie wytrzymał lekkomyślnych eksperymentów z grą Monopoly. Dostęp do terminali zaczął być kontrolowany. W związku z tym Bill wraz z kolegami zaoferowali swoje usługi CCC (*Computer Center Corporation*). Była to firma, która zajmowała się czymś, co moglibyśmy określić jako sprzedaż „czasu komputerowego" rozmaitym przedsiębiorstwom. W zamian za nieograniczony dostęp do komputera PDP-10 chłopcy mieli wykryć i wyeliminować wszystkie usterki systemu operacyjnego tego komputera. Umowa została zawarta. Licealiści spędzali wszystkie wolne

wieczory w sali pełnej terminali i analizowali kod systemu komputerowego. Podczas poznawania tajników minikomputera PDP-10 młodzi geniusze zapełniali wiele dziesiątków stron dziennika CCC opisami powodów zawieszania się komputera. Poddali przy tym komputer najwymyślniejszym „torturom". Fakt ten zaprowadził ich na zakazane obszary. Bowiem w systemie operacyjnym PDP-10, aby uzyskać dostęp do własnych informacji, użytkownik musi podać swoje własne nazwisko i własne tajne hasło, a Bill nabrał przekonania, że te zabezpieczenia można obejść. Traktował je jako wyzwanie intelektualne i zaczął bardzo dokładnie analizować każdy aspekt problemu, aby znaleźć wreszcie sposób na „oszukanie" komputera. Do świadomości Gatesa dotarł fakt, że nagle zdobył on dostęp do informacji dotychczas zastrzeżonych.

Młodzi programiści posunęli się aż do modyfikacji systemu operacyjnego PDP-10, podejmowanych w celu przyśpieszenia jego działania. W czasie prób ze zmodyfikowanym systemem spowodowali poważne „zawieszenie" komputera. Właśnie wtedy inżynierowie CCC odkryli, że struktura haseł systemu została złamana. Fakt ten wywołał ogromne zamieszanie.

Działalność w CCC uświadomiła Gatesowi bardzo istotną rzecz. Dowiedział się, że PDP-10 z University of Washington jest podłączony do narodowej sieci komputerów zarządzanej przez CDC (*Control Data Corporation*), zwanej również Cybernet. Bill postanowił natychmiast wkraść się do owej sieci. Musiał w tym celu dokładnie przeanalizować oprogramowanie używane przez Control Data.

Zdobył zaufanie starszych kolegów z uniwersytetu. Wymyślił całą strategię obejścia zabezpieczeń. Próba zakończyła się powodzeniem. Udało mu się wejść do sieci, a nawet — umieścić na głównym komputerze sieci własny program, który był przesyłany do wszystkich innych komputerów CDC. Doprowadziło to do kolejnego „zawieszenia". Administratorzy sieci Cybernet namierzyli młodego hakera. Bill zaprzestał więc swej działalności. Wraz z kolegami zaczął pisać komercyjne programy księgowe, programy zarządzające szkołami czy analizujące ruch samochodowy. Zarobił w ten sposób pierwsze duże pieniądze.

Historia Gatesa uświadamia, że hakowanie nie jest nowym i zdumiewającym zjawiskiem. Rozpoczęło się właśnie z początkiem 1960 roku, kiedy to na dość szeroką skalę w uniwersyteckich miejscowościach zaczęły się pojawiać komputery. Równolegle z rozwojem sieci uniwersyteckich, na „nieoficjalnych" obszarach sieci komputerowych zaczęły ukazywać się pierwsze elektroniczne tablice ogłoszeniowe — BBS-y (*Bulletin Board System*). Za ich pomocą już we wczesnych latach 80. osoby, które kontaktowały się ze sobą przez telefon, mogły magazynować i odzyskiwać software. Pod koniec tej dekady powstał nawet pierwszy piracki BBS, który pozwalał „ściągnąć" przez modem konkurencyjny software bez uiszczania jakichkolwiek opłat. Można tam było również znaleźć rozmaite rady i wskazówki, dotyczące odbezpieczania programów i nielegalnego kopiowania.

Z historią BBS-ów wiążą się losy niejakiego Bernarda Klatta, który stworzył jedną z pierwszych narodowych sieci wykorzystujących łącza telefoniczne. Człowiek ten, fanatycznie zaangażowany w wolność słowa, nalegał, by jego sieć była wolną prze-

strzenią dla użytkowników. Starał się realizować ów postulat i — jak na ironię — połączenie telefoniczne zniszczyło sieć BBS. Towarzyszył temu splot zaskakujących zdarzeń. Zainicjował je pozornie niewinny podarunek, jaki Klatt otrzymał na początku 1982 roku. Był to nowy modem, który został wysłany pocztą w prezencie od filadelfijskiej telekomunikacji. Zdaniem ofiarodawcy dar ten miał przyśpieszyć prędkość BBS-u. Wdzięczny Bernard Klatt przyjął go, nie podejrzewając nawet, jak perfidny podstęp kryje się w tym geście. Cóż się bowiem okazało? Modem był skradziony. Kiedy zatem nieświadomy niczego Bernard Klatt w kwietniu tego samego roku spędzał wakacje w Kanadzie, policjanci z biura śledczego Hrabstwa Santa Clara oraz agenci bezpieczeństwa z telekomunikacji wtargnęli do jego mieszkania z nakazem przeszukania wydanym przez sąd. Wszystkie dyski BBS-u zostały skonfiskowane. Na tym się skończyło. Wprawdzie Klattowi nie zagrażały żadne represje karne, ponieważ nie wiedział on, że otrzymany modem był skradzioną własnością, ale losy jego BBS-u były już przesądzone.

Mimo wielu niepowodzeń — historia Klatta nie jest jedyną niezrealizowaną opowieścią — ruch hakerski rozwijał się nadal. Zmieniało się wiele i to bardzo szybko — domowe komputery osobiste stały się szeroko dostępne, a wraz z nimi modemy przestały być luksusem nielicznych. Sieć natomiast przestała być domeną elity informatycznej.

Równolegle z tym rozwijała się ciekawość świata, pobudzana dodatkowo przez możliwości komputera i Sieci pojmowanej jako nowe medium, które zdecydowanie ułatwiało kontakty między ludźmi i niwelowało istniejące w rzeczywistości różnice. Jako że piękne ideały nie zawsze znajdują spełnienie, z tych niezaspokojonych pragnień narodził się współczesny typ buntowniczego marzyciela, kogoś, kto marzy o poznaniu zawartości wszystkich — nawet cudzych, rządowych lub korporacyjnych — twardych dysków, a jednocześnie ceni dyskrecję i chroni swój dysk przed ingerencją innych. Jednak „nieproszeni goście", którzy buszują w Internecie i zwiedzają dobrze zabezpieczone systemy — hakerzy, bardzo różnią się między sobą umiejętnościami związanymi z obsługą komputerowych programów, podstawową wiedzą o tym, jak są zorganizowane dane systemy. Tym, co łączy ich wszystkich jest przede wszystkim determinacja, czujność, optymizm oraz zdolność do analizowania i syntezowania, czyli — dedukcyjnego myślenia. Są bowiem ludźmi zafascynowanymi programowaniem i poznawaniem możliwości systemów. Najlepsi, najsłynniejsi współcześni włamywacze komputerowi posługują się szeroką gamą języków programowania, potrafią pracować w różnych systemach operacyjnych. Te umiejętności bywają nagradzane i po szaleństwach „młodości górnej i chmurnej", często przyjmują oni posady w renomowanych firmach, gdzie pracują jako doświadczeni i cenieni w branży programiści lub administratorzy systemów. Są i tacy, którzy nigdy nie rezygnują. Właśnie ich coraz częściej nazywa się cyberpunkami. Słowo to zaczerpnięte z kultowej książki Williama Gibsona *Neuromaucer*, wskazywać ma na trudności związane z jednoznacznym określeniem ludzi, zajmujących się hakowaniem.

Jeden z byłych hakerów — Bill Landreth — wyróżnia co najmniej pięć kategorii różnicujących grupę hakerów. Jego zdaniem można tu wyodrębnić:

- *nowicjuszy (The Novis)*, których pociągają np. gry komputerowe czy zawartość zbiorów i danych, ale ich działania w odniesieniu do systemów są nie do przewidzenia;
- *analityków lub badaczy (The Student)* zainteresowanych poznaniem różnego rodzaju komputerów bez czynienia jakichkolwiek szkód;
- *turystów (The Tourist)* traktujących systemy komputerowe jak łamigłówki, do których nie powracają po ich rozwikłaniu;
- *wandali (The Crasher)* dążących umyślnie do wyrządzenia użytkownikom komputerów jak największych szkód; ich głównym zajęciem jest tworzenie coraz to wymyślniejszych wirusów, których celem jest destrukcja systemu, kasowanie danych, ataki typu „Denial of Service" (dosłownie — *odmowa usług*), zakłócenie pracy serwerów, przetwarzanie stron WWW;
- *złodziei (The Thief)* działających na ogół na rzecz firm konkurencyjnych.

Do tego podziału warto dodać jeszcze trzy inne kategorie:

- *zdobywców (Score Keepers)*, którzy włamują się dla sprawdzenia własnych umiejętności;
- *szpiegów (Spys)*, którzy włamują się w ściśle określonym celu, np. po to, aby wykraść informację, uszkodzić lub zdestabilizować system;
- *cyberterrorystów (Cyberterrorists)*, którzy wykorzystują własne umiejętności tylko po to, by destabilizować, uszkadzać systemy lub wykradać dane. Tymi działaniami terroryzują firmy, żądając od nich wysokich okupów. Kradną też dane z przedsiębiorstw i administracji państwowej. Szpiegostwo gospodarcze może poważnie zagrozić przedsiębiorstwu, jeśli na przykład konkurencja wykradnie plan nowej kampanii marketingowej albo dane dotyczące nowych technologii. Łupem są coraz częściej zbiory danych osobowych (rządowe lub bazy danych klientów) z profilami, czyli informacjami określające preferencje związane z zakupami, stanem finansowym oraz numerami kart kredytowych. „Terroryści" mogą zniszczyć system lub dane, albo żądać okupu za pozostawienie ich w stanie nienaruszonym z takimi sytuacjami spotykamy się coraz częściej, wiele firm decyduje się zapłacić okup, bo to wychodzi taniej niż przestój spowodowany destrukcją systemu komputerowego. Firmy te nikogo o tym nie informują, nie chcą przyznać się, że uległy szantażowi.

Działalność prawdziwych hakerów ma nie tylko złe strony. Liczne udane próby pokonania barier zmusiły projektantów do poszukiwania nowych rozwiązań, do konstruowania lepszych szyfrów. Stanowiły wyzwanie dla marzeń kreujących wizję świata jako wielkiej, elektronicznej wspólnoty i spowodowały rozwój międzynarodowych, ogólnodostępnych sieci i nowych urządzeń zabezpieczających. Można by zadać sobie pytanie o to, co skłania kogokolwiek do spędzenia ośmiu, dziesięciu czy dwunastu godzin samotności ze wzrokiem wbitym w ekran monitora? Odpowiedzią jest chyba zagadkowość komputerowych programów i fascynacja połączona z intelektualnym wyzwaniem. To może być wystarczającą motywacją dla młodego adepta sztuki hakerskiej. Dodać można do tego dreszczyk emocji, towarzyszących

przy pokonywaniu zabezpieczeń oraz nadzieję na ekscytującą podróż w nieznane. Można to porównać do nałogu, swoistego uzależnienia od komputera. Bo jest coś hipnotycznego w tym dwuwymiarowym ekranie monitora, który pozwala na nieograniczoną niczym wędrówkę po świecie cyberprzestrzeni. Poza ciekawością istnieje jednak wiele innych powodów.

Często jest to urok, jaki niesie ze sobą możliwość dostępu do ciekawych, zastrzeżonych informacji, może to być także traktowane jako dobra metoda na zrobienie kariery, szpiegostwo, kradzież, wandalizm. Przyczyną są również powody polityczne, zemsta lub po prostu megalomania. Rozwojowi nowych międzynarodowych sieci informacyjnych często towarzyszą nowe, dotychczas nieznane problemy socjalne. Dla kogoś, kto działalności elektronicznych włamywaczy przygląda się z zachowaniem odpowiedniego dystansu, haker może się kojarzyć z rozpowszechnionym przez media stereotypem, który każe wiązać tę postać z portretem nieprzystosowanego socjalnie osobnika, który stawia towarzystwo komputera przed kontaktami ludzkimi i budzi powszechną nieufność ze względu na nieobliczalne straty, jakie jest w stanie wywołać swą działalnością. *Suma sumarum* — nawet wśród profesjonalistów hakowanie nie cieszy się uznaniem.

Obiegowe sądy nie zawsze mijają się z prawdą. Wspólną cechą włamywaczy — zdaniem wielu specjalistów — jest bowiem osamotnienie i brak akceptacji społecznej. Wedle opinii amerykańskiego socjologa, Sherry Turkle, hakerzy są zwykle fanami science fiction, którzy zdecydowanie unikają złożonych problemów społecznych.

Często mają oni uzasadnione powody do obaw i są pełni kompleksów. Nie potrafią sobie poradzić ze skomplikowanymi stosunkami międzyludzkimi. Nieśmiałemu i pełnemu oporów człowiekowi towarzystwo zastępuje więc ekran monitora. A w świecie elektronów i bitów pozycję zdobywa się znacznie łatwiej. Obowiązuje tu ściśle określony porządek — o miejscu w hierarchii międzynarodowej społeczności hakerów decyduje ilość i klasa włamań oraz jakość zdobytych informacji. Życie jest prostsze i pozwala się sprowadzić do konkretnych wymiarów.

Wydawca słynnego poradnika *The Haker's Handbook*, Steve Gold, sugeruje jednak, że osobowość hakera jest bardziej złożona. Bo jest nim zwykle człowiek inteligentny, który po prostu poszukuje wyzwania. Szkoła (czy nawet praca) nie daje mu możliwości zaspokojenia ambicji, więc kieruje się w stronę komputera. Często okazuje się jednak, że zabawa rozpoczęta z ciekawości, przekształca się w coś bardziej niebezpiecznego. Wiele ofiar tej perfidnej gry z komputerem nie zdaje sobie nawet sprawy z tego, że popełnione zostało przestępstwo i nie przeczuwa konsekwencji, jakie może za sobą pociągnąć. Bowiem komputer, jak twierdzi Steve Gold, ogranicza w znacznym stopniu świadomość i wszelkie doznania sprowadza do analizy efektów wizualnych, które ukazują się na ekranie. Jako że włamanie do systemu obronnego państwa czy banku danych w szpitalu i naruszenie zawartych w nich informacji nie różni się technicznie od ingerencji w swe własne zbiory, dla hakera nie ma więc posmaku przestępstwa. Jest zatem ubocznym skutkiem podejmowanych działań.

W tym duchu utrzymaną definicję prezentuje Guy Steele, autor *The Hakers Dictionary*. Utrzymuje on, że *haker* to osoba, której przyjemność sprawia poznawanie szczegółowej wiedzy na temat systemów i rozszerzanie tej umiejętności (w przeciwieństwie do większości użytkowników komputerów, którzy wolą uczyć się niezbędnego minimum) lub osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny.

Natomiast prawnicy bardzo często w odniesieniu do hakerstwa używają określenia „zamiar przestępczy", które koncentruje uwagę na stanie umysłowym człowieka planującego wykroczenie przeciw prawu i pozwala ustalić, jakie miał on intencje. Jeśli zatem podejrzany przypadkowo spenetrował system komputerowy używając do tego celu metod dostępnych każdemu obywatelowi, nie może być mowy o istnieniu jakichkolwiek zamiarów przestępczych. Gdy jednak podejrzany wiedział, że narusza bezpieczeństwo i świadomie korzystał w tym celu z wyszukanych metod, mamy do czynienia z zamiarem przestępczym. Na tej podstawie można by nawet wyznaczyć granicę między hakowaniem (pierwszy rodzaj) a crackowaniem (drugi rodzaj).

Donosząc o popełnieniu przestępstwa prokuratorzy najczęściej opierają się na fakcie zaistnienia zamiaru przestępczego. Wydaje się jednak, że jest to miara zbyt surowa, ponieważ problem hakerów i crackerów jest dużo bardziej złożony.

Najpierw należy bowiem poznać motywację i sposób życia tych jednostek oraz narzędzia, którymi się posługują. Są to przede wszystkim języki programowania stanowiące zestawy instrukcji i bibliotek. Jeśli zostaną one odpowiednio ułożone i skompilowane, stają się funkcjonalnym programem komputerowym. Składniki tych języków niemal zawsze są takie same. Stąd też każdy programista używa podobnych narzędzi. Oto dwa z nich :

1. *biblioteki* — gotowe funkcje wykonujące często powtarzane czynności i spotykane w wielu programach (na przykład procedury odczytujące zawartość katalogów);
2. *kompilatory* — programy przetwarzające tekst programu do postaci wykonywalnej, czyli dającej się uruchomić na danej platformie.

Narzędzia te oraz podręczniki opisujące sposób korzystania z nich to wszystko, czym dysponuje haker. Reszta zależy już od niego. Często się zdarza, że opracowując programy, tworząc je w celach poznawczych, wprowadza element, którego nie ma zarówno w samym języku, jak i w bibliotekach: wyobraźnię.

Wielu z tych, którzy należą do tzw. elity hakerskiej, często balansuje czasem na granicy dwóch światów. Nie chodzi tu jednak o granicę między rzeczywistością materialną a wirtualną, lecz o wartości bardziej fundamentalne — dobro i zło. Możemy znaleźć mnóstwo ilustracji tego zjawiska, za przykład jednak niech posłużą dzieje niejakiego Randala Schwartza, który był niezwykle utalentowanym programistą, autorem lub współautorem wielu książek o Perlu, m.in. *Learning Pearl*, która została opublikowana przez O'Reilly&Associates. Schwartz zajmował wówczas stanowisko konsultanta na Uniwersytecie Bufallo, w firmach Silicon Graphics (SGI),

Motorola Corporation oraz Air Net. Mimo że nadal jest ceniony za wkład, jaki wniósł w badanie języków skryptowych, a jego prace okazały się pomocne i wykorzystano je w Internecie, nie można się oprzeć podejrzeniu, że balansował on na cienkiej linii dzielącej hakera od crackera.

Kiedy jesienią 1993 roku, Schwartz pracował jako administrator systemu firmy Intel w Oregonie, miał prawo wykonywać niektóre procedury związane z zapewnieniem bezpieczeństwa. Rozszerzone preferencje, pobudziły jednak jego pasje odkrywcze. I poznawał system — by tak rzec — bez ograniczeń. 28 października 1993 roku inny administrator systemu zauważył, że na jego komputerze uruchomione zostały procesy w dużym stopniu wykorzystujące zasoby. Stwierdził, że funkcjonujący program to *crack*, czyli popularne narzędzie do łamania haseł Uniksa. Dalsze badanie pozwoliło stwierdzić, że procesy są wprawione w ruch przez Schwartza lub kogoś innego, kto jednak posługuje się jego nazwą użytkownika i hasłem. Administrator porozumiał się z przełożonym, który potwierdził, że Schwartz nie miał pozwolenia na łamanie haseł w firmie. Nie dalej jak l listopada 1993 roku administrator złożył oświadczenie do protokołu, które wystarczyło, by u Schwartza przeprowadzić rewizję. Nieco później Schwartz został aresztowany i oskarżony zgodnie z tamtejszym prawem o przestępstwach komputerowych.

Sprawa ta nie jest jednoznaczna. Mamy bowiem znanego i utalentowanego programistę odpowiedzialnego za utrzymanie bezpieczeństwa wewnętrznego dużej firmy, który wykonuje działania mające na celu przetestowanie możliwości systemu. Sumiennie i z polotem wykonuje on swoje obowiązki, co kończy się... aresztowaniem. Tak to przynajmniej wygląda. Ale tylko z pozoru, bowiem Schwartz nie był upoważniony do łamania haseł, a ponadto istnieją dowody na to, że przekroczył znacznie więcej zasad. Zainstalował na przykład skrypt powłoki, który pozwalał mu na logowanie się do sieci Intela z zewnątrz. Powstała niewielka luka w zaporze sieciowej (*firewall*), co zostało zauważone przez innego administratora. Wykrył on program, zamroził konto Schwartza i porozumiał się z nim. Sprawę załatwiono polubownie — Schwartz przyznał, że nie był to najlepszy pomysł i zobowiązał się do przestrzegania reguł obowiązujących w firmie. Po jakimś czasie ten sam administrator odkrył, że Schwartz ponownie zainstalował program tyle że pod inną nazwą.

Najprawdopodobniej Schwartz wielokrotnie przekraczał obowiązujące granice, jednak z jego zeznań wynika, że nigdy nie przedstawiono mu regulaminu Intela, a przynajmniej nie dano mu żadnego dokumentu, w którym jasno byłoby napisane, że takie czynności są zabronione. Tak czy inaczej, jest oczywiste, że Schwartz nadużył swojego stanowiska.

Z historii tej należałoby wyciągnąć pewne wnioski. Większość administratorów odpowiedzialnych za bezpieczeństwo korzysta z takich narzędzi jak *crack*, gdyż stanowi to rutynową metodę znajdowania słabych haseł, czyli takich, które nietrudno złamać. W tamtym czasie jednak narzędzia tego typu były stosunkowo rzadkie, więc ogólnie ich nie pochwalano. Przypadek Schwartza poruszył wielu programistów i ekspertów bezpieczeństwa w Stanach Zjednoczonych. Jeffrey Kegler (w artykule *Intel kontra Randal Schwartz: co to oznacza?*) uznał całą sprawę za złowieszczą prognozę:

«Randal powinien był zdawać sobie sprawę z tego, co robi. Stał się pierwszym profesjonalnym informatykiem, który obrócił się ku bezprawiu. Wcześniejsi przestępcy komputerowi to samouki i nastolatki. Nawet Kevin Mitnick ze swoją złożoną osobowością nigdy nie zasłynął inaczej niż przestępstwem. Przed Randalem jeszcze nikt związany z „białą magią" nie przestąpił progu „czarnej magii"».

(Materiały zaczerpnięto z artykułu Keglera, który w całości znajduje się na stronie: *http://www.lightlink.com/spacenka/fors/court/court.html*).

Można by więc zapytać, dlaczego zrobił to Randal Schwartz. Ale odpowiedź nie jest tak prosta, jak mogłoby się wydawać z pozoru. Bo w istocie ten utalentowany programista nie popełnił żadnego przestępstwa. Odkrył jedynie, że prawo obowiązujące w świecie rzeczywistym nie dosięga Sieci. Tam granice wyznacza wiedza i zdolności programistyczne.

Krótka historia hakerstwa

W kwestiach związanych z hakerstwem coraz częściej pojawiają się różnorodne metafory i przedziwne porównania. Są one nieodzowne przy próbie opisu tej tajemniczej — jakby na to nie patrzeć — działalności. Posługując się zatem określeniem Keglera, spróbujmy prześledzić proces przechodzenia od białej magii Internetu do tej czarnej, która z wolna zaczyna wyznaczać coraz ciemniejsze rejony hakowania. Oto sporządzone naprędce kalendarium porządkujące najważniejsze wydarzenia w historii hakerstwa lat osiemdziesiątych.

1983

W jednej z pierwszych policyjnych akcji wymierzonych przeciw hakerom FBI aresztowana została sześcioosobowa grupa nastolatków, znana jako „414" (nazwa pochodzi od telefonicznego numeru kierunkowego). Grupę oskarżono o około sześćdziesiąt włamań (w tym do sieci scalającej komputery Laboratorium Los Alamos).

1984

Eric Corley, używający pseudonimu Emmanuel Goldstein założył w Nowym Jorku kwartalnik *2600: The Haker Quaterl*, który błyskawicznie zyskał renomę sztandarowego pisma środowiskowego.

1985

„Podziemni" dziennikarze *Taran King* i *Knight Lighting* otworzyli elektroniczny magazyn *Phrack* zawierający różnorodne informacje dotyczące hakowania.

1987

Siedemnastoletni Herbert Zinn, znany władzom jako „Shadow Hawk", przyznał się oficjalnie do włamania do komputerów AT&T w New Jersey. Władze federalne wydały oświadczenie, z którego wynikało, że nastolatek omal nie dotarł do wewnętrznej centrali firmy i systemu zarządzania połączeniami. A dokonał tego posługując się domowym komputerem ulokowanym na przedmieściach Chicago... Zinn był pierwszym skazanym na podstawie ustawy „Computer Fraud and Abuse Act" z 1986 roku, która zabraniała między innymi korzystania z cudzych haseł.

1988

Robert Morris, dwudziestodwuletni student z Cornell University uruchomił w Internecie „robaka", czyli program, który żerował na nieścisłościach w oprogramowaniu i wykorzystywał luki w zabezpieczeniach Uniksa. Obecnie nazwalibyśmy go już „wirusem", gdyż zaprojektowany został w ten sposób, że penetrował inne systemy i „rozmnażał" się w nich błyskawicznie. „Robak" Morrisa był pierwowzorem późniejszej „Melissy" i „I love You". Jego obecność stwierdzono na ponad sześciu tysiącach dysków twardych, co w 1988 roku stanowiło mniej więcej 1/10 wszystkich komputerów podłączonych do Sieci. Straty oceniono na piętnaście do stu milionów dolarów. Morris został ujęty, skazany warunkowo na trzy lata, czterysta godzin pracy społecznej i dziesięć tysięcy dolarów grzywny.

Departament Obrony USA odłączył komputery Milnetu od Arpanetu (późniejszego Internetu) po tym, jak stwierdzono włamanie do co najmniej jednego z komputerów obrony. Pierwszym odnotowanym wydarzeniem był tu spektakularny atak słynnej grupy hakerskiej „Legion of Doom". Pod koniec 1988 roku opanowali oni BBS (*bulletin boards*), wykradli dokumenty techniczne od firm telefonicznych i rozprowadzali za pośrednictwem BBS-ów.

1989

Clifford Stoll, administrator systemu komputerowego Berkley University, przeprowadził prywatne dochodzenie w sprawie systematycznych włamań do uniwersyteckiego komputera. Stwierdził, że pochodzą one z tych samych źródeł, co ataki na rządowe komputery podłączone do Sieci. Doprowadził nawet do ujęcia trójki zachodnioniemieckich cyberszpiegów, którzy sprzedawali informacje Związkowi Radzieckiemu. Niejaki Stoll wykorzystał te informacje i nieco później napisał bestseller *The Cuckoo's Egg*. Mimo to żaden ze szpiegów — jakby na przekór skazującym wyrokom — nigdy nie trafił za kraty.

W tym samym roku jednak został skazany Kevin Mitnick. Podstawą do wyznaczenia kary była kradzież oprogramowania DEC-a i kodów rozmów długodystansowych z MCI. Jest to fakt godny odnotowania, gdyż Mitnick był pierwszym skazanym na podstawie nowej ustawy zabraniającej dostępu do międzystanowej sieci komputerowej w celach przestępczych. Wprawdzie po roku zwolniono go warunkowo, ale otrzymał prawny zakaz korzystania z komputerów i kontaktowania się z innymi hakerami.

1990

Policja ujęła czterech członków grupy „Legion of Doom". Przedstawiono im zarzut kradzieży technicznej specyfikacji sieci 911 firmy BellSouth. W aktach sądowych zostało odnotowane, że informacja ta mogła posłużyć dla zakłócenia czy nawet — zablokowania sieci numerów 911 w całych Stanach Zjednoczonych. BellSouth stwierdził, że hakerzy wykradli również numery kont, adresy i hasła dostępu do sieci komputerowej. Firma wydała trzy miliony dolarów na walkę z nimi. Ze sławetnej czwórki trzech osobników zostało oskarżonych i skazanych na kary od czternastu do dwudziestu jeden miesięcy więzienia. Musieli oni wpłacić również zadośćuczynienie w wysokości dwustu trzydziestu trzech tysięcy dolarów.

Właśnie wtedy amerykańska Secret Service rozpoczęła operację „Sundevil", wymierzoną przeciwko cybernetycznej przestępczości. Agenci zarekwirowali sprzęt komputerowy aż w czternastu miastach. Na nic się to zdało, bo już w marcu tego samego roku niejaki Steve Jackson — właściwe pośrednio, ale skutecznie — ośmieszył Secret Service. W jaki sposób? Po prostu w ramach operacji „Sundevil" przetrząśnięty został dom pewnego mieszkańca Austin (Steve'a Jacksona), który pisał gry komputerowe. Cóż się okazało? Pełni zapału i dobrej woli agenci zatrzymali jego komputer, gdyż uważali, że zawierał on „podręcznik przestępczości komputerowej", który okazał się zwykłą książką. Jackson nie został oskarżony, gdyż nie udało się sformułować zarzutów przeciwko niemu.

1991

Aresztowany został w tym roku Justin Petersen z Dallas. Zarzutem, który mu przedstawiono było... posiadanie kradzionego samochodu. Przy okazji policja odkryła jednak pliki sugerujące, że dokonane zostało włamanie do komputerów TRW, czyli jednej z wiodących amerykańskich firm specjalizujących się między innymi w wojskowych systemach informatycznych. Zamiast więzienia FBI zaproponowało Petesenowi współpracę i przez jakiś czas pomagał on w przeprowadzaniu dochodzeń śledczych (między innymi przeciw Mitnickowi). Dwa lata później nagle zniknął i został uznany za zbiegłego. Nieco później jednak zaistniał ponownie. Tym razem — w sprawie prowadzonej przeciwko Poulsenowi.

Ale to nie wszystko, co wydarzyło się w roku 1991. W tym samym czasie bowiem grupa holenderskich nastolatków uzyskała dostęp do komputerów Departamentu Obrony. Miało to miejsce w czasie „wojny w Zatoce", a dyski twarde komputerów, których oprogramowanie zostało spenetrowne przez hakerów zawierały szczegóły operacji wojskowych, informacje o ilości sił przerzuconych w rejon konfliktu, a także dane osobowe jednostek wojskowych i zapowiedzi nowych rodzajów broni.

1992

Rok ten zainicjowało aresztowanie pięciu członków „Masters of Deception", grupy nastolatków z Brooklynu i Queens. Zarzucono im włamanie między innymi do systemów AT&T, Bank of America, TRW i Narodowej Agencji Bezpieczeństwa.

Podczas dochodzenia po raz pierwszy w śledztwie prowadzonym przeciw hakerom posłużono się podsłuchem. Mark „Phiber Optik" Abene został skazany na rok, a pozostała czwórka — na sześć miesięcy.

W grudniu 1992 roku Kevin Poulsen, który już wcześniej niszczył dane zawarte w sieciach komputerowych, został posądzony o kradzież rozkazów dotyczących ćwiczeń Air Force One. W akcie oskarżenia była mowa o kradzieży tajemnic państwowych, które podlegały sekcji federalnych przestępstw szpiegowskich i Poulsenowi groziła kara 10 lat więzienia.

1993

Sprawa się przeciągnęła i dopiero w następnym roku Kevin Poulsen został oskarżony o komputerowe oszustwo w konkursach promocyjnych, organizowanych przez trzy stacje radiowe w Los Angeles. Stawką były dwa Porsche i dwadzieścia tysięcy dolarów w gotówce. Rzecz nie do pogardzenia, więc Poulsen skorzystał z nadarzającej się okazji lepszego życia. Mimo, że był poszukiwany pod zarzutem włamań do sieci telekomunikacyjnych i komputerowych, działał dalej wraz z Ronaldem Austinem i Justinem Petersenem, który wcześniej współpracował z FBI w sprawie Mitnicka. Trójka hakerów zdołała przejąć więc kontrolę nad telefonami do stacji, upewniając się, że tylko ich połączenia będą przyjęte. Ale nie długo sprzyjała im Fortuna.

1994

W tym właśnie roku dwójka hakerów, znanych jako Data Stream i Kuji, włamała się do komputerów Bazy Sił Powietrznych w Griffith, NASA, Koreańskiego Instytutu Badań Atomowych i setek innych systemów. Poszukiwaniem sprawców zajęli się specjaliści ze Scotland Yardu i niedługo trzeba było czekać na efekty. Data Stream okazał się szesnastoletnim angielskim chłopcem. W momencie aresztowania opuściła go dawna pewność i nonszalancja; kulił się, płakał, gdy stanęli przed nim policjanci. Kuji nigdy jednak nie został odnaleziony.

Ale wydarzyło się coś jeszcze — anonimowy haker rozpoczął atak skierowany na sieć komputerów Tsutomu Shimomury, eksperta od zabezpieczeń w San Diego Supercomputer Center. Jego twarde dyski zawierały zaawansowane oprogramowanie zabezpieczające. Shimomura dołączył więc do poszukiwań Kevina Mitnicka, który był domniemanym sprawcą włamania.

1995

Aresztowany i osadzony w więzieniu został Kevin Mitnick. Trzeba tu podkreślić, że do jego ujęcia przyczynił się znacznie wspomniany już Tsutomu Shimomura. W efekcie hakera oskarżono o szereg włamań, kradzież około dwudziestu tysięcy numerów kart kredytowych i nielegalne kopiowanie oprogramowania. Mitnick

pozostał w areszcie do marca 1999 roku, czyli do czasu, gdy przyznał się do popełnienia siedmiu przestępstw. Wtedy został już prawomocnie skazany na dziesięć miesięcy pozbawienia wolności. Wyszedł z więzienia w styczniu 2000 roku.

Kolejnym bohaterem roku stał się również Wladimir Levin, trzydziestoletni Rosjanin, którego aresztowano w Wielkiej Brytanii. Przedstawiono mu zarzut nielegalnego transferu około czterech milionów dolarów z nowojorskiego Citibanku na swoje konta ulokowane na całym świecie. Po ekstradycji do Stanów Zjednoczonych Levin został skazany na trzy lata więzienia i dwieście czterdzieści tysięcy dolarów odszkodowania na rzecz Citibanku.

Na tym jednak nie koniec — w Sieci pojawił się Satan. Był to program opracowany w ten sposób, by znajdował i demaskował luki w zabezpieczeniach komputerów z systemem Uniksa, które zostały połączone do Internetu. Jego autorem okazał się między innymi Dan Farmer. Ten znany ekspert w dziedzinie bezpieczeństwa twierdził, że wprowadzenie Satana do Sieci było jak najbardziej pozytywnym działaniem, gdyż miało na celu ujawnienie luk w oprogramowaniu komputerów, które administratorzy mogli poznać i wyelimowanować na długo wcześniej nim hakerzy postanowią wykorzystać je do własnych celów.

1996

Haker znany jako Johnny [Xchaotic] dokonał perfidnego ataku na około czterdziestu polityków, biznesmenów i innych osób, subskrybując ich w mnóstwie internetowych list dyskusyjnych. Nieszczęsne ofiary otrzymywały potem około dwudziestu tysięcy wiadomości, które trafiły do ich skrzynek e-mailowych.

1998

John Hamre z amerykańskiego Departamentu Obrony oświadczył, że Pentagon stał się ofiarą najbardziej zorganizowanego i systematycznego ataku hakerskiego, jaki kiedykolwiek miał miejsce. Atak miał na celu uzyskanie dostępu i zmianę danych dotyczących płac i innych akt osobowych. Wkrótce potem FBI aresztowało dwóch nastolatków z niewielkiej miejscowości Cloverdale w Kalifornii. Ich przywódca o pseudonimie „Analyzer" został ujęty niespełna miesiąc później.

Zdarzyło się jednak w tym roku coś, co warto podkreślić ku przestrodze młodocianym włamywaczom, władze federalne USA po raz pierwszy oskarżyły nieletniego przestępcę. Powodem było zablokowanie systemu komunikacyjnego lotniska w Worcester (Massachussets) dokonane poprzez sieć Bell Atlantic. Atak hakera spowodował sześciogodzinną przerwę w łączności pomiędzy samolotami a wieżą kontrolną. Na szczęście ofiar nie było. Chłopca skazano więc warunkowo. Musiał odpracować dwieście pięćdziesiąt godzin prac społecznych i wpłacić pięć tysięcy dolarów grzywny. Jego nazwiska nie ujawniono.

Natomiast 22 kwietnia 1998 roku Miedzynarodowa Grupa Hakerów podała do wiadomości, że włamała się do komputera Agencji Aeronautyki i Przestrzeni Kosmicznej (NASA). Następne włamanie do NASA zrealizowała grupa hakerska MOD, do której między innymi należą Amerykanie, Brytyjczycy, Rosjanie. Przedstawiciel tej grupy przesłał do servisu AntiOnline informację o udanym ataku na jeden z systemów NASA. Celem był jeden z systemów Agencji znajdujący się w Jet Propulsion Laboratory (JPL) w Pasadenie (Kalifornia).Wykorzystując złożony system haseł oraz routing bazujący na sieci różnych komputerów rozsianych po całym świecie, hakerzy z MOD przesłali na adres AntiOnline dowody świadczące o tym, że udało się im uzyskać dostęp do oprogramowania uniksowego służącego do wykrywania ataków na systemy NASA.

1999

Ofiarą komputerowych wandali padł szereg stron amerykańskiego senatu, Białego Domu i armii. Hakerzy pozostawili na nich wiadomości, które szybko usunięto. Jedna z nich, umieszczona na stronie Amerykańskiej Agencji Informacyjnej brzmiała: *I love You, Crystal — Zyklon*, co świadczy o swoistym poczuciu humoru.

Wtedy również norweska grupa „Masters of Reverse Engineering" (MoRE) przełamała klucz zabezpieczający przed kopiowaniem nagrań DVD. Program dekodujący, zwany DeCSS, został rozprowadzony w Sieci. Rozpoczęło to trwającą do dziś lawinę pozwów sądowych skierowanych przeciwko właścicielom stron oferujących DeCSS.

Dokonano również kradzieży 300 000 numerów kart kredytowych należących do giganta sieciowego, a jednocześnie właściciela jednego z najpopularniejszych internetowych sklepów muzycznych — firmy eUniverse. Sprawcą okazał się dziewiętnastolatek z Rosji — „Maxus" oferujący sprzedaż numerów wykradzionych kart na swojej stronie.

2000

W ciągu trzech dni hakerzy zablokowali wiodące portale internetowe (między innymi — *Yahoo!*, *Amazon.com*, *Buy.com* oraz *CNN.com)*, bombardując je taką ilością zgłoszeń, której nie były w stanie przyjąć ich serwery. Co ciekawe — mimo że wiadomo, iż „rozkazy" wysyłane były z uniwersyteckiej czytelni Stanforda, sprawcy do dziś pozostali nieznani.

2001

Dzień 11 września wstrząsnął milionami ludzi na kuli ziemskiej. Wobec światowego terroryzmu nie pozostają obojętni również hakerzy. Zaatakowali oni muzułmańskie strony internetowe, w tym oficjalną stronę rządzących w Afganistanie talibów. Zamiast ich tekstów pojawił się tam w czwartek 13 września list gończy FBI za Osamą bin Ladenem.

Kim Schmitz, Ex-haker zaoferował na swojej stronie internetowej nagrodę w wysokości 10 mld USD, za informacje, które przyczynią się do ujęcia postaci numer jeden światowego terroryzmu.

W tym samym roku nastoletni hakerzy włamali się do laboratoriów prowadzących badania nad bronią nuklearną. Jak podaje BBC — pięciu nastolatków w wieku 15 – 17 lat z terytorium Stanów Zjednoczonych wykradło hasła tysięcy użytkowników serwerów dwudziestu sześciu różnych dostawców usług internetowych i — podszywając się pod niczego nieświadomych klientów tychże operatorów — włamało się do laboratoriów Sandia i Oak Ridge w USA. Obydwa laboratoria zajmują się dostarczaniem składników do produkcji broni nuklearnej, a Oak Ridge ponadto wytwarza pluton i inne materiały radioaktywne dla celów militarnych.

Biorąc więc pod uwagę, że przedstawione informacje stanowią skrócony i niepełny przegląd hakerskiej działalności ostatnich lat, nie sposób nie zauważyć, że efekty ich działań z każdym dniem stają się bardziej imponujące i... przerażające, gdyż w coraz większym stopniu naruszają granice prawa i koncentrują się na obiektach najbardziej niedostępnych — sieciach rządowych różnych mocarstw. Warto zatem przyjrzeć się bliżej ludziom, którzy być może nie długo przechwycą dane dotyczące losów świata.

Haker, czyli nowy rodzaj buntownika

Po zaznajomieniu się z kalendarium zestawiającym hakerskie osiągnięcia, nie można nie zauważyć ich zwiększającej się z dnia na dzień skali. W pewien sposób odzwierciedla to naszą rzeczywistość. Fakt nadejścia ery komputerów osobistych wiele zmienił w kulturze Zachodu. I były to zmiany niezwykle dramatyczne. Nagle — właściwie z dnia na dzień — wszystko, co w naszym życiu istotne zostało ściśle związane z wirtualną rzeczywistością zerojedynkowych przekazów. Komputery są już wszędzie. Technologia informatyczna uzależniać zaczęła od siebie prawie każdy rodzaj kontaktu. Zaczynając od wielkich inwestycji gigantycznych korporacji, a na zwykłych listach przesyłanych pocztą elektroniczną kończąc, wszystko krąży wokół niewielkiego, ale jakże znaczącego peceta. Spotkanie „twarzą w twarz" już nie jest warunkiem koniecznym do zaistnienia społecznej interakcji. W tym sensie komputeryzacja stanowi podłoże „rewolucji informatycznej", która — niezauważenie być może, ale za to skutecznie — dokonała się na naszych oczach. Doświadczamy bowiem swoistej syzygii, znanej z pism McLuhana prorokującego nadejście świata globalnej wioski.

Nie da się ukryć, że pionierami na „nowym lądzie wirtualnej przestrzeni" są hakerzy. Stanowią oni „nasienie" cyberprzestrzeni. Są nie tylko najpotężniejszą cyberkulturę on-line, ale również jedną z najbardziej intrygujących społeczności. Są inteligentni, żądni przygód i nieposkromieni wobec wyzwań, które sami sobie stawiają. Dla nich kontakt z komputerem nie jest łamigłówką nie do rozwiązania. Ale, co zaskakujące — wszystko, co robią ci ludzie ma swoje bardzo konkretne podstawy. Chcą sławy i chwały, pragną znaleźć się w elicie i właśnie dlatego zdobywają kolejne „poziomy

sprawności i wtajemniczenia". A wszystko to dlatego, że w hakerskim świecie obowiązuje inna waluta. Najważniejsza jest tu ekonomia informacji. Elita postrzega bowiem wiedzę i intelektualną sprawność jako klucz do zdobycia bogactwa, potęgi i sławy. Używa inteligencji, by zyskać uznanie w oczach innych kolegów z grupy lub zdobyć siłę poza nią. Nie jest ważne, czy informacja zamknięta jest w skłębionych zwojach mózgowych hakera, czy znajduje się na dysku twardym jego komputera. Tu albo tam — jest środkiem, dzięki któremu społeczność ta wzmacnia się, jednoczy i utrwala.

Nie może zatem dziwić fakt, że jakość hakera jest mierzona ilością jego wiedzy. Może ona dość łatwo przerodzić się w potęgę. Odkąd sprawność intelektu jest postrzegana jako klucz do elity, jej praktyczny wykładnik, jakim jest informacja, stał się wysoko ceniony. Jest towarem. I hakerzy wykorzystują wszelkie zdobyte informacje, czytają nawet zawirusowane pliki, gdyż wiedzą, jak sobie z nimi poradzić. Dobrze znają i rozumieją wartość informacji i robią wszystko, aby ją posiadać, czy to przetrząsając „śmieci", czy włamując się do dobrze strzeżonych rządowych baz danych. Korzystają ze wszystkiego, co może przynieść im informacja, czyli najlepszy, najbardziej drogocenny towar cyberprzestrzeni. Tylko w ten sposób mogą podnieść swój status. Hakerzy bowiem wiedzą, że informacja jest równoznaczna z posiadaniem dużych pieniędzy. Bo można nią handlować jak każdym innym towarem. Dlatego hakują. Haking jest bowiem nowym rodzajem buntu. Buntu wymierzonego w kontrowersyjną hierarchię wartości dwudziestego wieku.

Trzeba więc zapytać: czym jest haking? Z mnóstwa odpowiedzi, które mogą się tu pojawić, najistotniejsza wydaje się definicja przytoczona przez autora Zina hakerskiego L.O.A. Jego zdaniem haking to czyn polegający na penetrowaniu systemów komputerowych, gromadzeniu wiedzy o systemach i o tym, w jaki sposób działają. Bezsprzecznie jest to proceder nielegalny, ponieważ jego skutkiem bardzo często staje się niszczenie zabezpieczeń danych komputerowych.

Właśnie ten fakt wzbudza negatywne emocje ludzi postronnych. Hakerzy są bowiem potępiani przez społeczeństwo. Ludzie powszechnie postrzegają ich jak zwykłych kryminalistów. Z tego powodu właśnie hakerzy za wszelką cenę starają się utrzymać własną anonimowość. Rzadko rozmawiają o swoich odkryciach z ludźmi spoza elity. Boją się, aby nie zostali postawieni w stan oskarżenia. A przecież — jak uważają sami zainteresowani — często są karani jedynie za inteligencję. Rządy krajów rozwiniętych poświęcają bardzo wiele czasu i środków, aby aresztować niepokornych włamywaczy, podczas gdy tak naprawdę wielu groźnych przestępców jest na wolności. Mordercy, gwałciciele, terroryści, porywacze powinni być ukarani za to, co zrobili. Czy jednak powinno karać się hakerów za chęć rozwijania własnej osobowości i intelektu? Niestety tak, gdyż wiedza może przybrać rozmaite formy spełnienia i w przypadku, gdy staje się zagrożeniem dla wielu nieświadomych tego ludzi, musi być poskromiona. Trzeba zatem pamiętać o istnieniu różnorodności w hakerskim półświatku. Można wymienić tyle odmian hakerstawa, ile rodzajów ludzi jesteśmy w stanie rozpoznać na ulicy. Bo każdy haker wykorzystuje swą wiedzę zgodnie z psychologicznymi uwarunkowaniami jego osobowości. Wielu z nich nie próbuje nikomu grozić, nie chce uszkadzać komputerów. Ale są i tacy, którzy nazywając siebie hakerami, dążą jedynie do destrukcji terminali w Sieci. Właśnie oni naruszają prawo.

Przez chwilę jednak zapomnijmy o tym negatywnym aspekcie i przyjrzyjmy się słynnej w hakerskim świecie próbie autoidentyfikacji:

Słynne słowa mentora!

Dziś złapali następnego.

Piszą o tym we wszystkich gazetach.

„Młodociany aresztowany w aferze komputerowej,

Haker aresztowany podczas włamania do banku"

...Przeklęte dzieciaki. One wszystkie są takie same...

Ale czy ty, tak, właśnie TY, czy kiedykolwiek spojrzałeś w oczy hakera?

Nie jakiegoś ulicznego handlarza pirackich CD-ROM-ów,

tylko hakera? Czy kiedykolwiek zastanawiałeś się, jaki on jest naprawdę, dlaczego robi to wszystko?

Dla rozgłosu — bzdura, dla sławy — nonsens!!! Więc dlaczego? Nie wiesz...

A może po prostu nie chcesz wiedzieć? Może boisz się stanąć z nim twarzą w twarz?

Za późno...

Jestem hakerem, witaj w moim świecie...

Mój świat zaczyna się w szkole...

Jestem mądrzejszy niż większość innych dzieciaków...

Te wszystkie bzdury, których tu uczą, po prostu mnie nudzą...

Przeklęty wiek... Oni wszyscy są tacy sami...

Jestem w podstawówce, liceum lub technikum...

Słucham po raz pięćdziesiąty jak nauczyciel tłumaczy teorię względności...

Rozumiem to.

„Nie, panie profesorze, Nie mogę pokazać pracy domowej.
Mam to wszystko w głowie...

„Przeklęty dzieciak. Pewnie od kogoś przepisał... One wszystkie są takie same..."

Dziś odkryłem coś ważnego. Znalazłem komputer.

Moment, to całkiem fajne. Robi dokładnie to, czego od niego chcę.
Jeśli się pomyli, to dlatego, że ja zrobiłem błąd. Nie dlatego, że mnie nie lubi...

I nie mówi, że jestem do niczego... I nie uważa, że jestem przemądrzałym cwaniakiem...

I nie powtarza ciągle, że powinienem się cieszyć i nie dotykać komputera...

„Przeklęty dzieciak. Ciągle tylko gra... One są wszystkie takie same...”

Wreszcie to się stało... otwarte drzwi na świat... modem... potrzebuję tego jak narkoman heroiny, elektroniczne impulsy przepływają przez komputer... tworzymy jedność... już zawsze będziemy jednością... dzień po dniu szukam, analizuję, przetwarzam... w końcu odkryję czyjeś niedbalstwo, niedopatrzenie... dziurę w systemie... znalazłem furtkę

„ To właśnie to... właśnie tego szukałem...”

Znam tu wszystkich... nawet jeśli nigdy nie spotkamy się „in real”, nigdy nie porozmawiamy, może nawet nigdy więcej o sobie nie usłyszymy...

Znam Was wszystkich

„Przeklęty dzieciak. Znów blokuje telefon... One wszystkie są takie same...”

Nie mylisz się jeśli uważasz, że jesteśmy tacy sami... Byliśmy karmieni papką dla niemowląt, kiedy mieliśmy ochotę na soczysty stek... ta odrobina wolności, jaka docierała pod klosz, którym nas otoczyliście, nie mogła nauczyć nas życia... Sieć to zmieniła, to tu jest nasz dom, nasze życie... Byliśmy zdominowani przez sadystów lub ignorowani przez ważniaków... Nikogo nie obchodziło, co czuliśmy... Tylko kilkoro z was, dorosłych starało się to zmienić... Próbowali nauczyć nas czegoś, próbowali nas zrozumieć... Byli jednak jak krople wody na pustyni... Nie mogli zmienić świata... My możemy...

Mamy własny świat... UNDERNET... świat elektronów, przełączników, połączeń. Korzystamy z waszych usług nie płacąc za nie, bo tak jest zabawniej, tak jest po prostu ciekawiej...

A wy nazywacie nas kryminalistami... To przecież wasze wychowanie przynosi efekt... Nie wiedzieliście, że przemoc rodzi bunt? My szukamy, cały czas szukamy... A wy nazywacie nas kryminalistami. My szukamy, żeby zrozumieć... A wy nazywacie nas kryminalistami. Żyjemy ponad waszymi podziałami, nie ważny jest dla nas kolor skóry, narodowość. Nie ma wśród nas fanatyków religijnych i nacjonalistów... A wy nazywacie nas kryminalistami... To wy zbudowaliście bombę atomową, to wy wywołujecie wojny, mordujecie, oszukujecie i usiłujecie nam wmówić, że to dla naszego dobra...

TO WY jesteście kryminalistami.

Tak jestem kryminalistą.

Moją zbrodnią jest myślenie.

Moją zbrodnią jest to, że oceniam ludzi za to, co robią i myślą, a nie za to, co usiłują pozorować. Moją zbrodnią jest to, że przejrzałem waszą grę, coś czego nigdy mi nie wybaczycie...

Jestem hakerem, i to jest mój manifest...

Możesz mnie powstrzymać, ale nie jesteś w stanie powstrzymać nas wszystkich....

Nie pokonacie nas, bo widzicie... my wszyscy jesteśmy tacy sami...

Przywołany tu manifest powstał w roku 1994 i został napisany z okazji zjazdu hakerów „DefCon II", który miał miejsce w Las Vegas w drugim tygodniu lipca tegoż roku. Znamienny wydaje się społeczny oddźwięk przesłania, bowiem niecały tydzień później na pierwszej stronie „New York Timesa" — ukazało się ogromne zdjęcie niejakiego Kevina Mitnicka z podpisem:

Najbardziej poszukiwany cybernetyczny przestępca wymyka się pościgowi FBI

Problem odpowiedniej motywacji

Skąd wynika zatem ten jakże łatwo zauważalny kontrast między pędem do wiedzy a sankcjami karnymi i powszechną negacją wypływającą ze strony społeczeństwa, które jakże często prześladują hakerów? Aby odpowiedzieć na to pytanie, trzeba przede wszystkim zaznajomić się z motywami hakerskich poczynań, bowiem to one właśnie są w stanie określić kolejne włamanie do systemu jako zachłanne zdobywanie wiedzy czy też czyn noszący znamiona przestępcze.

Mimo że teoretycznym spekulacjom wcześniej czy później grozi mielizna suchych wywodów, które tracą spoistość i sens w momencie, gdy za bardzo oddalą się od problematycznych kwestii, spróbujmy na moment o tym zapomnieć i zastanowić się nad problemem hakerów w perspektywie antropologicznej teorii Maxa Webera, który zakładał, że rdzennie społeczne uwarstwienie było oparte na trzech czynnikach: bogactwie, potędze i prestiżu. Pojawienie się jednego z tych czynników bynajmniej nie warunkuje następnych, ale również ich nie wyklucza. To wystarczy, by pobudzić wyobraźnię. Tak więc trójdzielny system Webera jest bardzo użyteczny w objaśnieniu społecznego stanu rzeczy. Bo dla hakerów informacja, bywa środkiem torującym drogę do osiągnięcia kolejnych celów — bogactwa, siły i prestiżu.

Hakerzy, którzy należą do elity rzadko się do tego zniżają. Satysfakcjonuje ich sama możliwość. Są to — moglibyśmy powiedzieć — współcześni Don Kichoci. Potencjalne możliwości nadają im rangę, pragmatyzm natomiast zniszczyłby zdecydowanie poezję ich poczynań. Ale stanowią oni niewielką grupę. Znacznie częściej spotkać bowiem możemy „hakerów praktykujących", dla których włamywanie się do systemów oznacza jedynie korzyści materialne.

Tak przedstawia się problem cardingu, czyli użytkowania i bezkarnego posługiwania się skradzionymi kartami kredytowymi. Mimo, że wielu z nich nie przysporzy on zaszczytów, jest łatwym sposobem na zdobycie gotówki i dlatego wciąż cieszy się zainteresowaniem włamywaczy komputerowych z nizin hakerskiego undergrundu.

O prestiż jednak trzeba się postarać i zyskują go zwykle ci, którzy zdobywają największą ilość informacji. Ten stan posiadania daje siłę i zapewnia szacunek współbraci. Stanowi więc motywację. Wiedzieć, wiedzieć jak najwięcej, aby zaistnieć — o paradoksie! — w wirtualnej przestrzeni. A jednak to robią. Wiedzą coraz więcej, włamują się do coraz bardziej niedostępnych systemów. Zdobywają. Zdobywają świat wirtualny. Nieistniejący świat w rzeczywistości świat zerojedynkowych wartości. Są więc chyba ostatnimi marzycielami naszych czasów.

Ale przy całej poezji i wzniosłości hakerskiej wyobraźni pojawiają się już całkiem konkretne konsekwencje tych poczynań. Rozmarzone technodzieciaki potencjalnie mogą całą ludzką technologię, całą cywilizację złapać za gardło, zniszczyć rzeczywisty świat za pomocą kilku kliknięć czy też paru stuknięć w klawisze. Tacy właśnie są. Wzniośli i niebezpieczni. Może więc warto ich poznać bliżej, zastanowić się, kim są i skąd pochodzą, a przede wszystkim spróbować odpowiedzieć na pytanie — dlaczego to robią?

Kim są hakerzy?

W książce Winna Schwartau *Information Warfare*, której tekst odnaleźć można w Internecie, przedstawione są dwa typy hakera. Jeden zaprezentowany został z pozycji samych zainteresowanych, drugi zaś — z punktu widzenia psychologii. Schwartau opierając się na rozlicznych kontaktach ze społecznością hakerską stwierdził, że wiele określających ich cech powtarza się i można je sprowadzić do poziomu ogólników. A więc — zwykle są to mężczyźni w wieku między 12 – 28 lat, często bardzo inteligentni, którzy nie znajdują dla siebie miejsca w realnym świecie. Bardzo często odróżniają się oni ubiorem, co wizualnie znamionować ma ich alienację. Nierzadko też pochodzą z rozbitych rodzin.

Nie jest rzeczą łatwą uzyskanie od hakerów jakiejś informacji na ich temat, gdyż anonimowość jest niepisanym prawem tej grupy. Wielu z nich ukrywa więc skrupulatnie swoją działalność i zainteresowania. Jedyne, czego się nie wstydzą to inteligencja. Haker często nawet jest zmuszony do demonstrowania swojej technicznej sprawności. W ten sposób może manipulować technologią i ludźmi.

Niezaprzeczalnym faktem jest, że hakerzy dysponują nieprzeciętnym potencjałem intelektualnym. Bardzo wielu z nich dodatkowo zdobywa wiedzę na uniwersytetach, ale zdarzają się równie często samouki. Niektórzy z nich twierdzą bowiem, że uczelnia nie może im wiele zaoferować. Więcej nawet. Wyobcowanie hakerów przyjmuje czasem skrajne formy i wielu z nich dochodzi do wniosku, że również

pospolite, codzienne życie rodzinne nie jest warte ich uwagi. Rzadko rozmawiają na ten temat. Często natomiast tracą kontrolę nad własnym życiem. Są zagubieni i nie bardzo bezpieczni. Znajdują więc schronienie w miejscu, nad którym mogą przejąć całkowitą kontrolę. Nie bez powodu zatem hakerzy bywają postrzegani jako grupa nie mająca poparcia i zrozumienia w społeczeństwie. Niezapisaną regułą hakerskiego półświatka jest więc to, że najlepsi z nich pozostają w ukryciu. Ujawnienie istnienia często wiąże się zatem z popełnieniem błędu, który zezwala na identyfikację. To są już poważne wpadki. I dla wielu niedoścignionym wzorem może być Kevin Mitnick, +ORC (prawdopodobnie pięćdziesięcioparoletni profesor matematyki, ekspert ds. kryptografii i zabezpieczeń, laureat nagrody Nobla) lub Cyberdaemon. Spekulacje trwają i nazwiska te stały się niejako symbolem wszechhakerów. Mianem „polskich Mitnicków" obdarza się najzdolniejszych włamywaczy, czyli dwie znane i szanowane osoby: Powera i Lcamtufa. Są oni autorami pierwszego polskiego hakzina — czyli magazynu — oraz najobszerniejszego w kraju FAQ, który obecnie stał się czymś, co można by nazwać „hak-biblią".

W przeciwieństwie do amerykańskich idoli, polscy bohaterowie — nawet, gdy są zmęczeni — żyją na wolności.

Stopnie wtajemniczenia

Specyfika hakereskiego półświatka nie jest ograniczona do jednej tylko „kultury softwarowej". Jest bowiem wielu ludzi, którzy wykorzystują metody i charakterystyczne dla hakerów style zachowań w innych zupełnie dziedzinach, takich jak elektronika czy muzyka. Rozpoznają ich „softwareowi hakerzy" i nazywają swymi sprzymierzeńcami. Są jednak tacy, którzy twierdzą, że hakerstwo tak naprawdę nie jest zależne od konkretnego medium, gdyż o byciu hakerem stanowi przede wszystkim typowy sposób pracy, umiejętności i określony sposób zachowania.

Hakerska elita jest niezwykłą grupą ludzi. Charakteryzuje ich przede wszystkim wiara we wzajemną pomoc i możliwość wymiany doświadczeń. Bo hakerzy włamują się do systemów nie po to, by je zniszczyć, lecz poznać, wzmocnić, ochronić przed kolejnym atakiem. Stąd wynika również konieczność emocjonalnego zaangażowania w pracę. Zatem jeśli młody człowiek chce zostać hakerem musi zdawać sobie sprawę z kilku podstawowych rzeczy. Po pierwsze — bycie hakerem może dawać złudzenie dobrej zabawy, ale to tylko ulotne wrażenie, za którym stoi naprawdę ciężka praca, wysiłek i samozaparcie. Nagrodą natomiast nie jest sława i majątek, lecz... satysfakcja, czyli towar bardzo nisko ceniony we współczesnym świecie. Niezbędny jest więc odpowiedni dystans i odrobina pewności siebie, która pozwala myśleć o tym, że rozwiązanie wielu komputerowych problemów mieści się w obrębie możliwości hakera.

Zaskakująca jest natomiast przedziwna solidarność tego półświatka, która zakłada istnienie wirtualnego rynku informacji. Hakerzy muszą bowiem dzielić się zdobytą wiedzą. Wynika to z faktu, że grupa ta dąży bezkompromisowo do ciągłego rozwoju i złamanie jakieś bariery, która stanowiła dla nich ograniczenie, musi natych-

miast zostać ujawnione, aby nie wstrzymywało współtowarzyszy w drodze do wytyczonego celu. Tak też się dzieje, a nagrodą dla włamywaczy-zdobywców jest — jak łatwo się domyślić — powszechny szacunek i uznanie. Bywa jednak tak, że życie hakera nie rozpieszcza i może się zdarzyć, że w zamian za udostępnienie informacji zażąda on wynagrodzenia mniej wirtualnego, czyli gotówki. Te przypadki zdarzają się równie często, co bezinteresowne udostępnianie znanych sposobów na przekroczenie systemu. Są powszechnie akceptowane.

Jak widać hakerski półświatek okazał się na tyle skonsolidowaną grupą, że wytworzył określone typy zachowań. Może mówienie o etyce, byłoby przesadą, jednak nie sposób nie zauważyć, że funkcjonują tu bardzo spójne zasady. Bo prawdziwy haker potrafi podporządkować się jedynie takim regułom, które sam wytworzył i dopasował do możliwości wirtualnej przestrzeni. Toteż odrzuca wszelkie konwencje i rozmaite rodzaje władzy, które pochodzą — by tak rzec — z zewnątrz. I nie ma w tym żadnych przejawów działania anarchistycznego czy nihilizmu. Po prostu haker nie dowierza realnie sprawowanym rządom. Zauważa niespójność w twardych regułach opisujących rzeczywistość i zero-jedynkową logiką cyberprzestrzeni. Inteligencja nie pozwala mu na mieszanie tych jakże różnych porządków.

Powszechnie wiadomo, że komputerowi włamywacze z natury sprzeciwiają się narzucaniu jakiejkolwiek formy władzy, bowiem każdy, kto ma wpływ na zachowanie hakera, staje się równocześnie największym zagrożeniem, gdyż może wydawać polecenia i jest w stanie — wbrew woli penetrującego informatycznego geniusza — powstrzymać go przed rozwiązywaniem istotnych problemów programów komputerowych.

Nie ma tu żadnych okoliczności łagodzących. Nawet fascynacja czyimiś umiejętnościami nie jest w stanie skłonić hakera do podporządkowania się i przyjęcia dominacji innej osoby. Pierwsze przykazanie sieciowego włamywacza powinno zatem brzmieć: rozglądaj się wokół i stale kontroluj, czy nie ma na ciebie wpływu ktoś o autokratycznym nastawieniu.

Nie chodzi tu bynajmniej o fakt zwalczania wszelkich form władzy. Istnieją przecież określone reguły życia społecznego, których nie sposób podważyć. A do nich należą dwie niezbywalne zasady — dzieci muszą być wychowywane, a przestępcy — izolowani. Nawet najbardziej zafascynowany ideą wolności haker nie może nie zgodzić się na zaakceptowanie pewnych form władzy.

Bardzo ważna jest tak zwana samoświadomość hakera. Bowiem bierne kopiowanie jakiejś postawy ze zwykłego zjadacza chleba nie uczyni hakera, tak jak mówienie o sporcie nie zmieni nikogo w mistrza olimpijskiego. Żeby zostać hakerem potrzeba nieprzeciętnej inteligencji, ćwiczeń, poświęcenia i wielu godzin ciężkiej pracy. Niezbędny jest również szacunek dla kompetencji innych „bywalców" Sieci.

Te wszystkie czynniki tworzą niezmienny zestaw cech, którymi dysponować powinien haker. Ale liczą się przede wszystkim jego umiejętności. Są one zmienne, tak jak zmienna jest technika opracowywania kolejnych programów. Kiedyś na przykład do podstawowych umiejętności hakera zaliczało się programowanie w języku maszynowym, a do niedawna nie należała do nich nawet znajomość HTML-a. Jednak by

znaleźć się w elicie trzeba jeszcze znać zasady programowania, opanować podstawy Uniksa i umieć nim zarządzać, a dodatkowo — posługiwać się sprawnie HTML-em (teraz już obowiązkowo) i World Wide Web.

Programowanie jest fundamentalną miarą kwalifikacji hakera. Jeśli nie zna on żadnego języka programowania, nie ma co liczyć na to, że kiedykolwiek znajdzie się w elicie i zdobędzie zaufanie innych. Musi ponadto mieć świadomość tego, iż niemożliwe jest osiągnięcie poziomu umiejętności hakera, a nawet zwykłego programisty, jeśli będzie znał zaledwie jeden język programowania. Dlaczego? To proste — języki programowania kształtują wyobraźnię i sprawiają, że człowiek zapomina o dawnych schematach i zaczyna „myśleć algorytmicznie". Po jakimś czasie haker osiąga więc poziom, na którym nauka nowego języka odbywa się mechanicznie. Skupia się bowiem na porównaniu zdobytych wcześniej wiadomości i wyselekcjonowaniu różnic. Trzeba więc ciągle rozszerzać swą wiedzę.

Podstawowym wymogiem jest znajomość języka *C*, który stanowi — by tak się wyrazić — rdzenny język uniksowy. Ważne są także inne języki, na przykład — *Perl* i *Lisp*. Pierwszy z nich jest bardzo praktycznym językiem, ułatwiającym tworzenie aktywnych stron WWW i pomagającym w administrowaniu systemu. Poznanie języka o uroczej nazwie Lisp nadaje już hakerowi odpowiednie znaczenie. Bo w wirtualnej przestrzeni — inaczej niż w życiu — jedynym miernikiem wartości człowieka jest jego wiedza. A każdy z tych języków uczy istotnych rzeczy. Można to porównać ze zgłębianiem tajników ortografii — najlepszą metodą na zwiększenie własnych umiejętności jest czytanie tekstów (kodów) pisanych przez mistrzów. Kiedyś znalezienie dobrego wzorca stanowiło nie lada problem, gdyż niewiele było programów dostępnych w kodzie źródłowym, który można by wykorzystać do nauki. Jednak obecnie sytuacja zmieniła się diametralnie i wszystko zależy od tego, czy adept sztuki hakerskiej wykaże zapał i odrobinę dobrej woli.

Podstawowy „warsztat" hakera wciąż stanowi Unix. Jest on najważniejszy, bo chociaż istnieją inne systemy operacyjne, to jednak są one dostępne tylko w kodzie binarnym, co uniemożliwia odczytanie kodu i wprowadzenie jakichkolwiek zmian. Nie należy zatem uczyć się hakowania w systemie *DOS*, *Windows* czy *MacOS*. Warto dodać, że Unix jest systemem operacyjnym Internetu, więc nie można penetrować Sieci, nie znając go dokładnie. Właśnie dlatego cała społeczność hakerów jest skoncentrowana wokół Uniksa.

Aby podsumować powyższe rozważania, warto przytoczyć artykuł niejakiego Erica S. Raymonda, który pisząc o hakerstwie lokuje ten problem w sferze nazywanej przez antropologów „kulturą darów". Bo żeby zdobyć określony status i reputację (nie poprzez dominację nad innymi ludźmi, nie za doskonały wygląd, ani nie dlatego, że posiada się coś, co chcą mieć inni) trzeba dać coś innym. I to za darmo. Rozdaje się bowiem czas spędzony na poznawaniu systemu, kreatywność, efekty skrupulatnie zdobywanych stopni wtajemniczeń.

Hakerski półświatek sformułował więc podstawowe zasady, których trzeba przestrzegać, by znaleźć i utrzymać swe miejsce we wspólnocie. Oto one:

- trzeba umieć pisać programy i dobrowolnie udostępniać ich kody źródłowe;
- trzeba wytrwale testować różne programy i pomagać w usuwaniu błędów;
- trzeba publikować w Sieci informacje, które mogą okazać się użyteczne dla innych;
- trzeba pomagać w usprawnieniu działalności infrastruktury;
- trzeba przestrzegać zasad kultury hakerskiej.

Należy tu również podkreślić fakt niezwykle istotny dla właściwego zrozumienia problemu — kultura ta jest w dużej mierze tworzona przez ochotników i zapaleńców. Tych, którzy chcą „coś" zrobić. A wyzwań mają wiele, choć nie wszystkie są widowiskowe lub spektakularne. Często bowiem jest to ciężka praca, polegająca na administrowaniu e-mailowymi listami grup dyskusyjnych czy zarządzaniu dużymi archiwami oprogramowania. Ludzie wykonujący te czynności, cieszą się dużym szacunkiem.

I tak to właśnie jest z hakerami — stanowią grupę, w której każdy z uczestników wykonuje przypisane mu obowiązki. Bowiem kultura ta nie ma „Ojców Założycieli", nie posiada przywódców w typowym rozumieniu tego słowa. To nie licowałoby z ogólną niechęcią do władzy. Na czym się zatem opiera? Na dobrowolności i autorytetach. Można więc wyodrębnić spośród nich najważniejsze jednostki — bohaterów, idoli, postacie spełniające się niejako symbolicznie i nadające ton wszelkim poczynaniom grupy. Stanowi to niekwestionowaną wartość całej społeczności, którą nieco wcześniej określiłem mianem „współczesnych kowboi klawiatury". I zastanawiając się nad ich specyfiką, nie możemy po raz kolejny nie zadać pytania o motywację. Bo wciąż nie jest ona jasna i jak bumerang wracają postawione wcześniej pytania. Być może hakerzy nie tyle niszczą, ile starają się przywrócić hierarchię wartości? Może są ostatnimi Mohikanami? Albo Don Kichotami XXI wieku?

Osobowość hakera

Zanim ulegniemy magii gloryfikujących określeń, warto choć na moment przyjrzeć się psychologicznym badaniom przeprowadzonym na grupie hakerów. Z obserwacji specjalistów wynika — a potwierdza to wspomniany już wcześniej Winn Schwartau — że haker postrzegany jest jako osobnik cierpiący na swego rodzaju „kliniczną narcystowską osobowość". To spostrzeżenie pozwala wyodrębnić dwie przeciwstawne grupy: hakerów paranoidalnych oraz hakerów przyjaźnie nastawionych względem nieznanych osób.

Obydwie postawy znajdują uzasadnienie. Nie trudno jest zostać paranoikiem, kiedy pozostaje się stale pod obstrzałem. Bo wszyscy chcą ich znaleźć i zatrzymać — nie tylko własny rząd i wykwalifikowane służby, ale także wielu z ich byłych przyjaciół mogłoby zniszczyć im życie bez większego wysiłku.

To budzi zrozumiały lęk i ostrożność.

Z drugiej jednak strony haker, który chce utrzymać się na fali nie może pozwolić sobie na pełną alienację. Tym bardziej, że — jak twierdzi Peter Sommer (ukrywający się pod pseudonimem Hugon Cornwal), angielski prawnik, specjalizujący się w problematyce przestępczości komputerowej, autor najsłynniejszej książki poświęconej tej tematyce, a zatytułowanej *The Haker Handbook* — prawdziwy haker jest świadomy tego, że otrzymuje często wiele pomocy od zarządzających systemami komputerowymi, które atakuje. Wie, że w osiemdziesięciu procentach „wpuszczenie" do systemu jest zamierzone przez administratora i traktowane bywa jako łatwy sposób na przetestowanie ochrony systemu. Bardzo często jest to działanie dużo tańsze niż zatrudnienie drogich programistów sprawdzających działanie programu. Takie postawienie problemu staje się źródłem wzajemnego zaufania i przynosi hakerom dużo samozadowolenia. Pozwala im spojrzeć przyjaźnie w stronę otwierającego się przed nimi realnego świata, w którym — równie łatwo jak w wirtualnej przestrzeni — odnaleźć mogą szacunek i zaufanie.

Ale na tym zestawieniu nie wyczerpują się rozmaite metody klasyfikowania niepokornych użytkowników Sieci. Jako że hakera można rozpoznać po kilku specyficznych cechach — na przykład sposobie, w jaki zdobywa dostęp do numerów telefonów, gwarantujących połączenie z systemami komputerowymi i hasła, pozwalające na przechwycenie danych — można pokusić się o kolejny podział i odnaleźć granicę dzielącą hakera „leniwego" od „ambitnego". Przyjrzyjmy się im bliżej.

Haker — dajmy na to „leniwy" — zdobywa od innych ludzi numery telefonów lub hasła do systemu, wybiera numer, czeka na sygnał zgłoszenia (*dial tone*), wprowadza hasło, penetruje system przez kilka minut i rozłącza się. Z tego wszystkiego miał trochę zabawy, ale nie zrobił nic z wyjątkiem odbycia podróży drogą, którą ktoś już wcześniej podążał. Na tym kończą się jego marzenia.

W przeciwieństwie do minimalistycznych dążeń, haker „ambitny" dokonuje swoich własnych odkryć, nie wykorzystując zdobyczy innych. Jego mottem jest nieposkromione zdobywanie dziewiczego lądu. By posłużyć się drogowskazem wyznaczonym przez wieszcza — sięga on tam, gdzie wzrok nie sięga. Ale udana penetracja systemu zależy od wielu czynników. Przede wszystkim zaś — od cierpliwości hakera, który wie, że wokół niego znajdują się wszystkie materiały potrzebne do badań i wystarczy tylko uważnie słuchać i analizować kolejne fakty. Można więc „odwiedzić" kilka hakerskich BBS-ów, kilka grup dyskusyjnych czy też stron hakerskich, aby poskładać w całość wszystkie niezbędne szczegóły dotyczące nowego systemu lub nowej metody ataku.

Prawdziwy haker zdaje sobie sprawę z tego, że niezbędna literatura — dodajmy: fachowa — jest publikowana codziennie przez firmy komputerowe, domy wydawnicze czy specjalistyczne periodyki komputerowe. Wszystkie one zawierają ważne dla hakera informacje i wystarczy tylko umiejętnie z nich skorzystać...

Wyposażenie hakerów

Na potrzeby swojej działalności hakerzy wykorzystują różne typy mikrokomputerów, które wszakże spełniać muszą jeden podstawowy warunek. Powinny bowiem nadawać się do „prowadzenia rozmowy ze światem", czyli muszą być zaopatrzone w port seryjny lub modem. Często wystarczy dostęp do zwyczajnego terminalu danych. Kupując sprzęt, haker analizuje go pod kątem możliwości, które przydać się mogą w rozwijaniu jego umiejętności. Zapoznaje się z materiałami reklamowymi i dokumentacją techniczną urządzeń (stąd wynika częsta obecność na targach komputerowych). Prawie każdy mikrokomputer będzie dla hakera dobrym narzędziem pracy. Ważne, aby dawał on możliwość zachowania rezultatów „sieciowych przygód" w sposób szybki i sprawny.

Istotny jest również fakt posiadania jak największego bufora pamięci operacyjnej, gdyż zwiększa to tempo wykonywanych operacji, a tym samym zapewnia komfort pracy. Często przydaje się drukarka, ponieważ pozwala szybciej analizować uzyskane informacje.

Komputer musi mieć port seryjny (RS 232C) i niezbędne oprogramowanie. Często przydają się różne testery, np. taki, który daje możliwość testowania połączeń 25 pinów portu RS 232C. Przydaje się także dobry analizator protokołów (przenośne urządzenie z pełną klawiaturą i oprogramowaniem sprzętowym, które bada linię telefoniczną lub port RS 232C i przeprowadza niezbędne testy).

Skąd hakerzy czerpią informacje

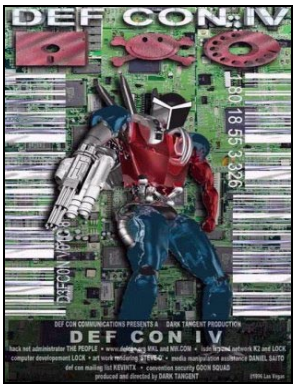
Najprostsze sposoby zdobywania informacji na temat włamywania się opisane są w tzw. *hak.faq*. Na IRC-u są wręcz kanały dedykowane włamaniom *(#hak, #crack*, etc.). Niektórzy hakerzy używają do kontaktów z początkującymi włamywaczami poczty anonimowej, co pozwala zachować anonimowość nawet w przypadku popełnienia przez „ucznia" błędu. Ale chyba najwięcej informacji i sposobów włamywania się można znaleźć na listach i stronach WWW, poświęconych bezpieczeństwu oraz na różnego rodzaju konferencjach i zlotach hakerskich.

DEF CON

Coroczny zlot hakerów — znany pod nazwą DEF CON — odbywa się w Las Vegas w lipcu każdego roku. Jesy to największy z istniejących zlotów hakerów, który przyciąga całe tłumy.

Trudno powiedzieć, dlaczego ten właśnie zlot skupia na sobie uwagę tak zróżnicowanej grupy ludzi. Tajemnica jego popularności tkwi pewnie w niekonwencjonalnym przebiegu. Bowiem hakerzy, którzy pracują równie niekonwencjonalny sposób,

nadają mu formę. Większość uczestników stanowi rozliczna grupa nastolatków w czarnych koszulkach. Rzadko który z nich używa prawdziwego imienia i nazwiska, gdyż preferowane są pseudonimy, takie jak White Knight, Se7en, Cyber czy Deth Veggie. W przeciwieństwie do innych zlotów organizatorzy DEF CON bardzo otwarcie zapraszają do uczestnictwa osoby zawodowo zajmujące się bezpieczeństwem informacji. Włączają w to nawet stróżów prawa.



Jako ciekawostkę warto dodać, że jedną z najpopularniejszych gier na konferencji jest „Spot the Fed". Jej uczestnicy są nagradzani koszulkami za wyśledzenie przedstawicieli prawa, którzy ukrywają się na konferencji.

Z roku na rok popularność DEF CON wzrasta. Bez wątpienia wielu uczestników zaspokaja tam swoją nieodpartą chęć poznawania. Inni po prostu próbują być na bieżąco poinformowani o nowych trendach pojawiających się wśród metod, jakimi posługują się hakerzy. Dla pozostałych dużą atrakcją może być spotkanie z legendami świata hakerskiego. Więcej informacji na temat DEF CON można znaleźć na stronie: *http://www.defcon.org/*.

Wiele informacji o hakerach, crackerach i włamaniach komputerowych dostępnych jest w Internecie. Oto kilka najlepszych adresów URL i grup dyskusyjnych, które odwiedzają hakerzy:

- *http://www.2600.com*;
- *http://www.l0pht.com*;
- *http://www.underground.pl*;
- *http://www.defcon.org/*;
- *http://www.haking.pl*;
- *http://security.zone.to/*;
- *http://phreak.zone.to/*;
- *http://crackpltools.prv.pl/*;
- *http://www.underpl.org/*;

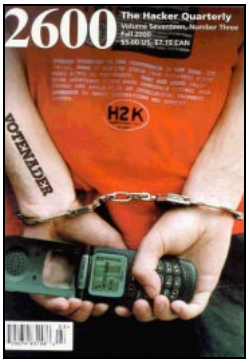
- *http://www.securityfocus.com/*;
- *http://www.securiteam.com/*;
- *http://www.ntsecurity.net/*;
- *http://astalavista.box.sk/*;
- *http://linux.box.sk/*;
- *http://rootshell.com/*;
- *http://www.insecure.org/*;
- *http://packetstorm.securify.com/*.

Nawet na polskich stronach WWW można znaleźć profesjonalnie zaprezentowane informacje na temat hakerstwa. Przykładem są strony *http://www.haking.pl*, *http://security.zone.to/*, *http://phreak.zone.to/*, *http://crackpltools.prv.pl/*.

Najsłynniejsze grupy dyskusyjne Usenetu to:

- *alt.2600.hakerz*;
- *alt.2600.codez*;
- *alt.2600.hope.tech*;
- *alt.2600hz*;
- *alt.haker*.

Czasopisma



Jednym z najsłynniejszych czasopism hakerskich jest kultowy „2600 Magazine" redagowany przez słynnego Emanuela Goldsteina. Teksty zamieszczane w tym piśmie są profesjonalne, a zarazem łatwe w odbiorze i — co warto podkreślić — bardzo aktualne. Jeden z ciekawszych działów poświęcony jest listom czytelników, w których przedstawiają szczegóły działań hakerów i crackerów.

Każdy kolejny numer magazynu zawiera wiele dokładnych informacji o określonych działaniach hakerów. Na ilustracji przedstawiona została okładka magazynu.

Jednak i polscy hakerzy nie próżnują, więc od września 2000 roku istnieje już polski kwartalnik hakerski wydawany pod nazwą: „Access Denied". Wszelkie informacje dotyczące dystrybucji, redakcji i zamówień znajdują się na stronie WWW pod adresem *http://www.ad–zine.org/*.

Pierwszy numer „Access Denied" zawierał następujące działy:

- Wstęp;
- Trudne początki;
- Quota — ograniczenie objętości konta;
- DNS ID Haking: co to jest DNS ID Haking?;
- Wyjaśnienie mechanizmu działania protokołu DNS;
- Pakiet DNS;
- Struktura pakietu DNS;
- Zapytania DNS;
- Odpowiedzi DNS;
- DNS ID hak/spoof.

Natomiast „How 2 cover your trakz (pl)" (opracowany głównie na podstawie „How to cover your tracks" by van Hauser/THC) składał się z następujących działów:

- Wstęp;
- Sytuacja prawna (Polska);
- Jak sobie radzić bez przywilejów superużytkownika;
- Maskowanie obecności w systemie — z przywilejami superużytkownika;
- Usuwanie śladów swojej obecności z logo tekstowych;
- Programy kontrolujące sumy kontrolne plików;
- Pliki *cron*;
- Dodatek specjalny — ukrywanie informacji.

Innym źródłem zdobywania informacji przez hakerów i crackerów są różnego rodzaju konferencje i spotkania. Można je podzielić na dwie części:

- konferencje, które sponsorują znane, profesjonalne organizacje rządowe lub przemysłowe;
- konferencje, które sponsorują grupy i organizacje hakerskie.

Najlepsze i najsłynniejsze z nich to:

- *RSA Data Security Conference*
  (konferencja dla specjalistów w dziedzinie kryptografii odbywająca się w Północnej Kalifornii);
- *DEF CON Conference*;

- *National Information System Security Conference*
  (kontrowersyjna konferencja, na temat której zdania hakerów są podzielone);
- *2600 Meetings*
  (spotkania, które odbywają się zawsze w pierwszy piątek każdego miesiąca od godziny 17.00 – 20.00 czasu lokalnego w różnych miejscach);
- *Hakers On Planet Earth (HOPE) Conference*
  (jedna z najlepszych konferencji hakerskich).

Hakerskie bestsellery

Haker korzysta z każdej szansy na zdobycie informacji (nawet zawartej w darmowym biuletynie informacyjnym). Odwiedza więc liczące się wystawy, gdyż dostępne są tam foldery z zapowiedziami nowych produktów. Prezentowane są również aktualnie używane komputery i oprogramowanie, które często można nie tylko obejrzeć, ale nawet sprowadzić. I zdarza się, że wykorzystując swą profesjonalną wiedzę, hakerzy są w stanie nakłonić wystawcę do sprezentowania im wersji demonstracyjnej software i wyjawienia tajników nowej technologii. Wystawcy, wyczerpani kilkudniowymi zmaganiami z klientami, zatracają bowiem czujność, wypisują hasła na papierze i podstawiają pod oczy dowolnego obserwatora. Wszystko, czego wówczas potrzebuje haker to szybkie spojrzenie i dobra pamięć.

Tak więc hakerzy bywają często na różnego rodzaju wystawach i konferencjach, lubią wynajmować się jako jednorazowi dziennikarze lub za takowych się podszywają. Większość komputerowych magazynów chytrze zatrudnia młodych, zdolnych ludzi. Jest to świetna okazja, gdyż haker zdobywa wtedy bez żadnego problemu pożądane informacje. Wielką pomocą w jego zmaganiach jest właściwa dokumentacja systemu komputerowego, którą uzyskuje na różne sposoby. Czasami korzysta z usług oferowanych przez sprzedawcę, który na przykład może polecić hakerowi dobry podręcznik. Bywa też tak, że niedoceniony pracownik firmy komputerowej dostarcza mu kserokopie poufnych dokumentów.

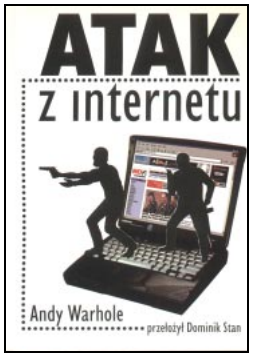
Innym źródłem zdobywania informacji są wewnętrzne numery telefonów firmy. Pod niektórymi z nich może odezwać się modem, a wraz z nim firmowy bbs z mnóstwem elektronicznych informacji. Wiele z nich cierpliwy haker znajduje w stertach śmieci wyrzuconych przez wielkie firmy, którym nie chce się tracić czasu na ich niszczenie w specjalnych do tego celu produkowanych urządzeniach.

Gromadzenie użytecznych wiadomości z pewnością stanowi jedną z głównych czynności hakera. Ale cóż znaczy dobra informacja bez możliwości jej wykorzystania? Prawdziwy haker nieustannie wyczekuje i selekcjonuje wszelkie dane i czeka, aż nadejdzie właściwy moment na ich zastosowanie. Zgłębia w tym czasie fachową literaturę. Poniżej znaleźć więc można nieco okrojoną listę hakerskich bestsellerów.

Internet Agresja i Ochrona

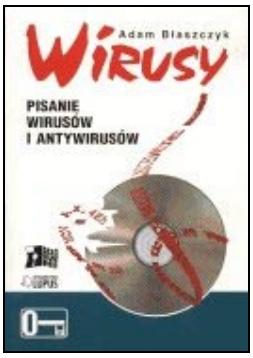
Książka ta jest tak naprawdę znanym już polskim przekładem książki *Maximum Security: A Hacker Guide To Protecting Your Internet Site and Network, 2nd Edition*. Można ją polecić wszystkim, którzy pragną przypomnieć sobie ciekawe informacje dotyczące systemów, takich jak Unix, NT czy NetWare lub w przypadku osób początkujących — poznać w stopniu podstawowym sposób ich działania. Pozycja ta jest zarazem świetną bazą adresów internetowych. Znaleźć można tam prawie wszystko — od IRC aż po SSH. Dodatkowo dołączony jest CD-ROM, na którym zawarta jest część programów wspomnianych w lekturze, cracki, łamacze, dokumenty i inne programy użytkowe.

Atak z Internetu



Jest to przekład książki Andy Warhole'a. Można tu znaleźć wiele ciekawych informacji dotyczących systemów i ich zabezpieczenia (z uwzględnieniem słabych punktów systemów oraz sposobów ataków). Jest to dobra lektura dla początkujących. Dobrze napisana, czyta się sprawnie i przyjemnie.

Wirusy — pisanie wirusów i antywirusów

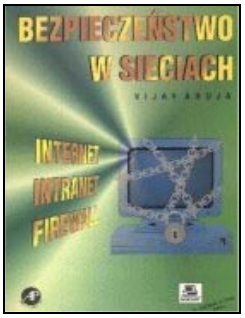


Jest to pierwsza polska książka tego typu. Prezentuje sposoby pisania wirusów i antywirusów, unieszkodliwienia wirusów „metodami domowymi", rozmaite zabezpieczenia. Dosłownie wszystko o wirusach. Sporo tam teorii, ale i praktyki. Dużo kodów źródłowych, dokładny opis ich działania. Najlepszą recenzją jest przedstawienie kilku rozdziałów. Będą to więc podstawowe wiadomości o wirusach, rodzaje wirusów, obiekty atakowane przez wirusy, instalacja w pamięci operacyjnej, przejmowanie przerwań, ukrywanie się w systemie, szyfrowanie kodu. Do książki dostarczona jest ponadto dyskietka z przykładami zamieszczonymi w tekście. Pozycja godna jest polecenia początkującym użytkownikom komputerów.

Nie tylko wirusy, haking, cracking, bezpieczeństwo internetu

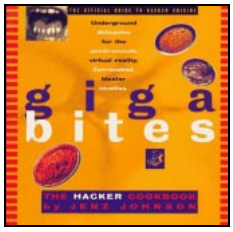
Jest to książka, będąca jedną z ciekawszych pozycji funkcjonujących obecnie na rynku. Obejmuje ona szeroki wachlarz tematyczny (poczynając od prezentacji typów wirusów, łamania haseł, zdobywaniu roota, sieci). Wszystko to opisane jest na przykładzie systemów, takich jak Windows, Novel, Linux. Ponadto książka przedstawia sposoby, jakie wykorzystują hakerzy przy swoich atakach i metody zabezpieczenia własnej sieci przed intruzami. Dołączony jest do niej CD-ROM z dużą ilością programów działających w systemie Windows czy Linux, jak i plikami źródłowymi oraz masą przydatnych tekstów, które autor zamieścił na płycie jako uzupełnienie. Ciekawostką jest tu także 15 MB słownik do łamania haseł.
Książka ta jest próbą przeglądu komputerowego „podziemia". Autor podejmuje bardzo szeroki zakres zagadnień — od wirusów poprzez bezpieczeństwo pojedynczych komputerów czy sieci lokalnych aż po współczesne metody omijania zabezpieczeń Internetu. Przedstawienie technik stosowanych przez włamywaczy komputerowych oraz opisanie błędów i „dziur" oprogramowania ma na celu uświadomienie administratorom rzeczywistego zagrożenia. Konkretne porady i zalecenia podsumowujące poruszane tematy z pewnością przyczynią się do zwiększenia bezpieczeństwa systemu.

Bezpieczeństwo w sieciach



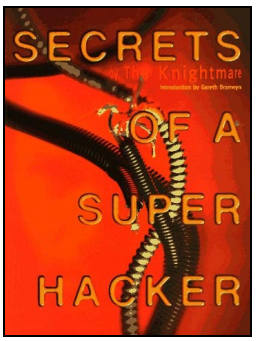
Jest to kolejna książka, w której autor Vijay Ahuja zwraca uwagę na tematykę związaną w bezpieczeństwem. Omawia w przystępny sposób funkcjonowanie sieci lokalnej, Intranetu, jak i sieci globalnej, czyli Internetu. Wraz z opisem możliwych zagrożeń, czytelnik otrzymuje antidotum — możliwości ochrony przed tymi zagrożeniami.

Giga Bites: The Hacker Cookbook



Jest to książka kucharska dla hakerów i na pewno spodoba się tym, których „lodówki" świecą pustkami. *Giga Bits* jest bowiem romantyczną podróżą po wnętrzu hakerskiej kultury i zawiera informacje dotyczące telegrafowania i ciągłego telefonowania bez uiszczania opłat za usługę.

Secrets of Super Hacker



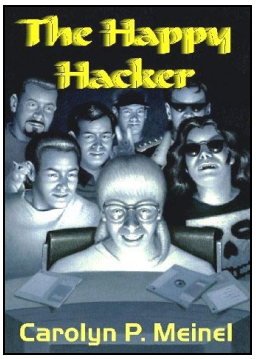
Jedna z najsłynniejszych książek hakerskich, a zarazem przewodnik przedstawiający sposoby naruszania komputerowych zabezpieczeń. Ukazane są tu poczynania szkodliwych superhakerów, takich jak na przykład Knightmare, który daje instrukcję manipulowania komputerem osobistym. Dołączono także rozdział o stanowym i federalnym prawie komputerowym, pozwalający potencjalnym hakerom zaznajomić się z sankcjami, jakie im grożą.

Jeden z rozdziałów prezentuje uporządkowany spis wyjaśnień technicznych i wskazówek, ułatwiających zrozumienie prezentowanego materiału i struktury systemu, a także dostarcza wyczerpujących wskazówek, które mogą okazać się przydatne w strategii poszukiwań. Za pomocą informacji zawartych w tej książce adept sztuki hakerskiej może dostać się do prawie każdego systemu. Dobrze jest jednak mieć świadomość, że prawie wszystkie informacje, które są zawarte w książce można łatwo odnaleźć w Internecie.

Pozycja ta kierowana jest nie tyle do hakerów, ile do społeczeństwa. Ale — jeżeli jesteś administratorem systemu i myślisz, że dowiesz się czegoś nowego o tym, jak chronić swój system przed hakerami — nie kupuj jej. Słabą stroną jest bowiem nadmierna ilość ogólników, a szczególnie „lista tymczasowych haseł" zamieszczona na końcu książki. Jest to rzecz karygodna, gdyż nie można opublikować takiej listy jako dodatku do książki.

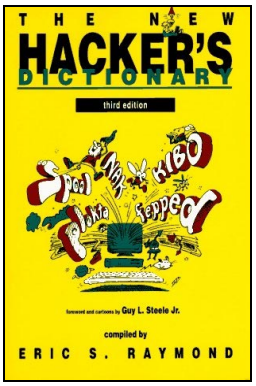
Trzeba również podkreślić, że ludzie, którzy nie mają pojęcia o hakerstwie, po lekturze tej książki mogą postrzegać hakerów w złym świetle. Pozycja ta wymaga zatem pogłębienia o kilka innych tekstów, które pozwolą zyskać obiektywizm.

The Happy Hacker



Wydana w 1998 roku książka — *The Happy Hacker* — jest czymś więcej niż przedrukiem wcześniejszych poradników nieszkodliwego hakowania, które można znaleźć na niezliczonych stronach WWW. Informacje zostały bowiem ulepszone i rozszerzone, dodano do nich całkiem nowy materiał. Książka powstała dzięki pracy setek hakerów, którzy wspomagali *The Happy Hacker* licznymi uwagami. Szczególne podziękowania należą się redaktorom technicznym książki: Johnowi D. Robinsonowi, Rogerowi A. Prata'owi, Danielowi Gilkersonowi, Damianowi Batesowi, Markowi Schmitzowi. Do listy tej należałoby dodać również nazwisko Marka Ludwiga, który jest wydawcą.

The New Hacker's Dictionary



W żadnej społeczności nowe terminy nie są tworzone i rozpowszechniane tak szybko jak w cyberkulturze. Niektóre słowa pojawiają się i znikają, czego przykładem może być najnowszy „upgrade software". Inne zostają na dłużej i funkcjonują w języku informatyki, co zdaje się potwierdzać „superautostrada informacyjna", termin, który został przyjęty jako nowe wyrażenie w 1993 roku przez American Dialect Society. Nikt nie śledzi przemian w obrębie tego dość specyficznego języka tak wytrwale jak Eric S. Raymond. Szczegółową analizę rozpoczął na początku 1990 roku, studiując żartobliwe słowa w cyfrowej kulturze, a następnie udokumentował zdobyte informacje w *The Hacker's Dictionary*. Najnowsze wydanie tej pozycji zawiera wyrażenia, które w większości utworzone zostały podczas ostatniego „wybuchu" World Wide Web (WWW). Jest to przewodnik dla wszystkich osób, które interesują się tym właśnie wycinkiem subkultury.

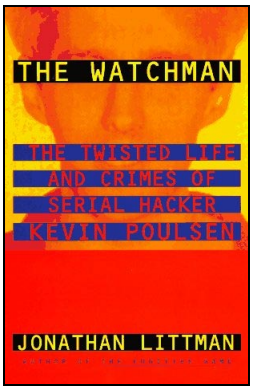
Jako rekomendację wystarczy przytoczyć fragment recenzji, która wyszła spod pióra jednego z redaktorów „Cyberkulture"*:*

„To już trzecie wydanie popularnego *The Hacker's Dictionary*, dodano w nim sto nowych terminów, a zaktualizowano dwieście. (...) Książka ta nie jest słownikiem terminów technicznych, ale na pewno znajdują się w niej dokładne definicje większości określeń pochodzących z technicznego żargonu. Jest to gwara i tajny język funkcjonujący wśród komputerowych jocks, którzy oferują największą zabawę. Większość ludzi nie czyta słowników dla zabawy, ale ten jest wyjątkiem".

The Jargon File, na jakim bazuje ta książka, był ostatnim przewodnikiem żargonu funkcjonującego w cyberprzestrzeni, ale od tamtej pory powstało mnóstwo nowych wyrażeń. Nawet ludzie, dla których „foobar" nie jest obcym słowem będą zadowoleni z esejów i żartów pojawiających się w *The New Hacker's Dictionary*.

Dobrze jest zatem posiadać własny egzemplarz tej książki. Jej główne przykazanie brzmi: zapomnij *Wired Style Guide*, zapomnij *The Dilbert Future*, bo, jeżeli chcesz pisać, mówić, lub po prostu komunikować się z kimkolwiek w sprawach komputerowych, potrzebujesz *The New Hacker's Dictionary*.

The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen



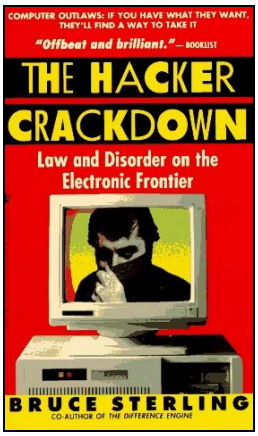
Książka ta w sposób zajmujący i zabawny przedstawia historię Kevina Poulsena — hakera i phreakera, który stał się w Ameryce pierwszym komputerowym przestępcą związanym ze szpiegostwem.

Niesamowita opowieść zaczyna się od przytoczenia dziejów dziecięcej miłości Kevina. Miłości dość specyficznej, której obiektem uczuć były... telefony. Stanowi ona podłoże całej opowieści o hakerstwie. Wyczyny Poulsena zdumiewają. Obok głównego bohatera pojawiają się również jego ekscentryczni przyjaciele, tacy jak: Ron Austin, Eric Heinz (AKA, Justin Peterson, Agent Steal), który ostatecznie pomógł FBI dorwać Kevina Mitnicka podczas ostatnich dni jego zwolnienia warunkowego. Littman przedstawia Kevina Poulsena w zdumiewający sposób — krytycznie i „współczująco". Jest całkowicie jasne, że Poulsen to przestępca (w przeciwieństwie do wielu innych postaci wspólnoty hakerskiej), który często czerpie zyski ze swoich przygód. Niemniej wątpliwe jest to, czy zasługuje na karę wymierzoną mu przez rząd Stanów Zjednoczonych.

Reasumując — jest to jest pierwszorzędne opowiadanie detektywistyczne, które opiera się na faktach, czyli historii pozornie niezwyciężonego elektronicznego włamywacza oraz ludzi, którzy go wyśledzili. Jonathan Littman wprowadza swoich czytelników do świata cyberpunkowej zbrodni ukazując początki, rozwój, i punkt kulminacyjny najbardziej dzikiej, najbardziej śmiałej znanej przestępczej działalności. Setki godzin wywiadów pozwalają Littmanowi ukazać historię oczami tych, którzy to przeżyli.

Wątpliwości budzić może jednak nieco jednostronne ujęcie sylwetki głównego bohatera. Zaraz po jej opublikowaniu sam Kevin Poulsen udzielił kilku wywiadów, w których podkreślał, że autor przedstawił go jako człowieka, który samodzielnie wykonał większość przestępstw, pomijając ludzi wplątanych w sprawę i często odgrywających większą rolę niż on sam. Mimo to pozycja ta jest godna polecenia.

The Hacker Crackdown: Law and Disorder on the Electronic Frontie



Klasyczna książka Bruce'a Sterlinga, która ujawniła w 1990 roku kulisy ataków wymierzonych przeciw hakerom. Wtedy to siły prawa aresztowały kilkoro podejrzanych hakerów. Obławy stały się symbolem sporu pomiędzy zwalczającymi poważne przestępstwa komputerowe a broniącymi wolności obywatelskich.

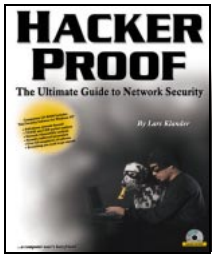
Niemniej jednak *The Hacker Crackdown* stanowi coś więcej niż opis serii operacji policyjnych. Jest to pełna życia opowieść o trzech cyberprzestrzennych subkulturach — podziemiu hakerskim, strefie cybergliniarzy oraz idealistycznej kulturze wolnościowej.

Sterling rozpoczyna swą historię od narodzin cyberprzestrzeni, czyli — wynalezienia telefonu. Przedstawia pierwszych hakerów-nastolatków, którzy byli zatrudnieni w charakterze operatorów telefonicznych i — używając mistrzowskich umiejętności — „pustoszyli" linie telefoniczne.

W książce pojawiają się również opisy działań wielu cybernetycznych rzezimieszków. Niektórzy z nich walczą dla sprawy, pozostali przedstawiają zabawę ponad wszelką ideologię, a jeszcze inni są pospolitymi przestępcami działającymi dla szybkiego zysku. Wyszczególnione są tu triumfy i niepowodzenia ludzi zmuszonych do kontrolowania poczynań hakerów, które dały podstawy powstaniu i rozwojowi subkultury zwanej „cybergliniarzami".

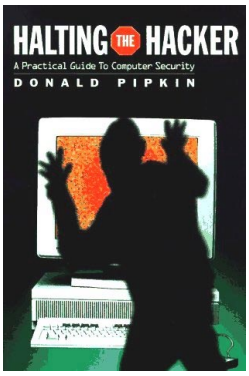
Ogólnie rzecz biorąc — książka ta umożliwia wgląd w życie i pracę ludzi wyjętych spod prawa. Zagłębia się w szczegóły rozmaitych metod używanych do crakowania. Rekomendowana wśród dziesięciu najlepszych pozycji służących do nauki hakerstwa, dostępna jest również w elektronicznej wersji.

Hacker Proof: The Ultimate Guide to Network Security



Hacker Proff : The Ultimate Guide to Netwoek Security przedstawia wiele szczegółowych pojęć, jakie muszą znać służby bezpieczeństwa, administratorzy sieci, programiści. Dołączono do niej CD-ROM zawierający oprogramowanie, którym użytkownicy mogą przetestować swój system. Pozycja ta jest świetną pomocą, którą można wykorzystać do crackowania programów. Ponadto pozwala zrozumieć zasady działania super hakerów, co w rezultacie daje szansę na obronę przed ich potencjalnymi atakami.

Halting the Hacker: A Practical Guide to Computer Security

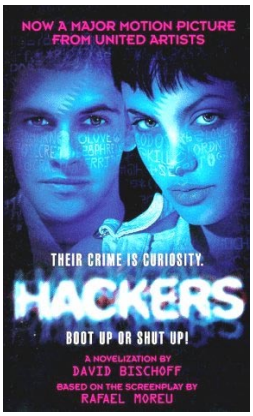


Nowa książka technicznego doradcy do spraw zabezpieczeń Hewlett-Packarda — L. Pipkina jest bardzo ciekawą pozycją dotyczącą problemu zabezpieczenia sieci opartej na Uniksie przed niebezpiecznymi atakami. Wyszczególnia ona liczne „podejścia" i techniki, których hakerzy używają w celu uzyskania dostępu do systemu, przywilejów i przejęcia pełnej kontroli. Jej głównymi zaletami są wyliczone jasno i zwięźle środki zaradcze (zarówno aktywne, jak i bierne), które mogą powstrzymać większość hakerów.

Do książki dołączono CD-ROM z biblioteką narzędzi służących do wykrywania i eliminowania problemów zagrażających bezpieczeństwu systemu.

Jest to dobrze przemyślane kompendium, pełne informacji skierowanych do osób odpowiedzialnych za zabezpieczenie systemu Unix. Zawiera zbiorcze „archiwum informacji", opowieści hakerów i dodatki periodyków drukowane on-line. Ukazuje, w jaki sposób hakerzy przekształcają pomniejsze przeoczenia w główne wady systemu i naruszają zabezpieczenia, jak ukrywają pozostawione ślady opuszczając system „tylnymi drzwiami", jak można wykryć włamania i jak im zapobiegać.

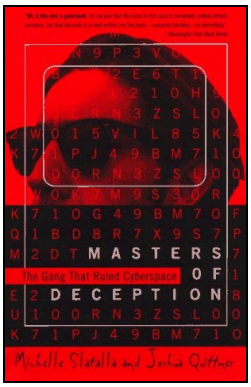
Hackers



Kanwą tej książki był film o tym samym tytule emitowany we wrześniu 1995 roku. Przedstawiał on losy grupy nastoletnich cyberpanków, która wykonała o jeden krok za dużo i została wciągnięta w sidła zagrażającej życiu pajęczyny przemysłowego szpiegostwa.

Lektura przypomina oglądanie filmu, gdyż jest to dobra adaptacja scenariusza. Wartością jest natomiast pogłębienie psychologicznego realizmu każdej z postaci. Biorąc pod uwagę skomplikowaną akcję, książka ta w wielu miejscach przypomina powieść sf z szybko toczącą się akcją. Jest więc wspaniałą lekturą dla każdego hakera lub po prostu — osoby lubiącej komputery.

Masters of Deception: The Gang That Ruled Cyberspace

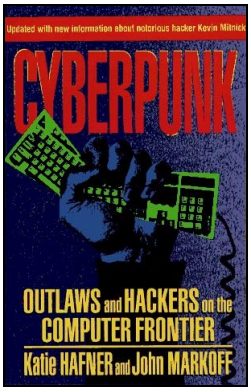


15 stycznia 1990 roku „padła" długodystansowa sieć telefoniczna AT&T. Chociaż ostatecznie było to zrządzenie losu, wypadek ten zainicjował szereg rozmów prowadzonych pomiędzy spółkami telefonicznymi i stróżami prawa. Ich tematem była niska odporność systemów, od których jesteśmy uzależnieni. Federalni zdecydowali, że nadszedł czas na rozprawienie się z grupą obserwowanych od pewnego czasu hakerów.

Dwa rywalizujące gangi — *The Legion Of Doom* (Legiony Losu) i *Masters Of Deception* (Mistrzowie Podstępu) — wstąpiły zatem na wojenną ścieżkę. Wydarzenia doprowadziły do konfliktu, którego punkt kulminacyjny przykuwa wciąż uwagę i... bawi.

Książka *Masters of Deception: The Gang That Ruled Cyberspace* znakomicie przedstawia sylwetki kilku sław hakerskiej sceny (Acid Phreaka czy Phiber Optika), jak również opowieści o ich wyczynach i rywalizacji. Slatalla i Quittner wykonali dobrą robotę przedstawiając szefów gangów jako potężnych władców cyberprzestrzeni, za których się uważają, a jednocześnie jako wystraszonych, młodych ludzi, którymi są w rzeczywistości. Autorzy stworzyli dzieło tak klarowne i trzymające w napięciu, że nawet laicy mogą cieszyć się akcją.

Cyberpunk: Outlaws and Hackers on the Computer Frontier

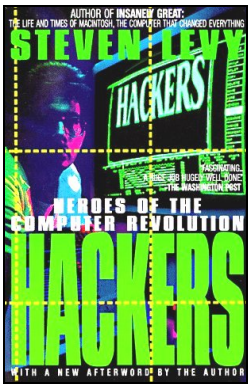


Pozycja ta prezentuje klasyczne spojrzenie na subkulturę crackerów, cyberpunków. Opowiada o losach znanych hakerów: Kevina Mitnicka, Robert T. Morrisa — ludzi z grupy „Chaos Computer Club". Opisuje początki Internetu. Przede wszystkim jest dobrze napisaną książką informacyjną.

Sprzyja temu przedstawienie historii otaczających „ciemną stronę" cyberprzestrzeni — włamania Kevina Mitnicka do Norad czy portret dwu członków Chaos Computer Club, który jest pamiętnym spojrzeniem w głąb umysłów młodszego pokolenia hakerów.

Książka znakomicie ilustruje wszelkie niebezpieczeństwa czające się w tajemniczym elektronicznym świecie.

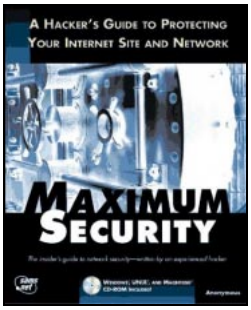
Hackers: Heroes of the Computer Revolution



Książka ta rekomendowana jest przez redaktora „Cyberculture".

To klasyczna pozycja Stevena Levy, która wyjaśnia, dlaczego słowo „haker" niewłaściwie używane do opisywania działań komputerowych przestępców, wyrządza szkody wielu ważnym twórcom cyfrowej rewolucji. Levy podąża za osiągnięciami członków MIT (*Moedel Railroad Club*) — grupą świetnie rozwijających się elektronicznych inżynierów i komputerowych innowatorów i prowadzi ich chronologią aż do połowy lat 80. Ci ekscentryczni osobnicy używali terminu „hak" do opisania sposobu ulepszania elektronicznego systemu, który napędzał ich ciężką kolej. Odkąd zaczęli wymyślać coraz to ciekawsze sposoby na poprawienie działania komputerowych systemów, „hak" podążał razem z nimi. Ci odszczepieńcy często byli fanatykami, którzy nie zawsze przestrzegali litery prawa. Książka przedstawia historię hakerów. Jest ona pełna błyskotliwych, ekscentrycznych i często zabawnych angdot, które stały się udziałem ludzi oddanych marzeniom o lepszym świecie. Stephen Levy zawarł w niej historię PC od korzeni w MIT do niezliczonych technologii skradzionych od Xerox PARC, a ponadto opisał kulturę komputerowych geeks. *Hackers: Heroes of the computer revolution* ma w sobie coś, co może sprawić przyjemność każdemu czytelnikowi — humor, historię i zabawę.

Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network

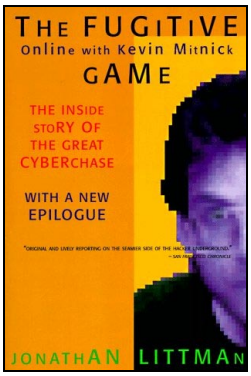


Książka napisana przez anonimowego hakera, przedstawia szczegóły wielu metod, jakimi hakerzy zdobywają kontrolę nad dowolnym systemem i sposoby, które mogą ich powstrzymać.

Pozycja ta nie tylko jest doskonałym źródłem odniesienia, ale też wskazówką techniczną dla tych, którzy zamierzają bezprawnie włamywać się do systemów. Dołączony do niej CD-ROM zawiera wybrane narzędzia zabezpieczające, takie jak SAFEsuite, wersję demonstracyjną PORTUS Secure Firewall, SATAN (*Security Administrator Tool for Analyzing Networks*).

Trzeba pamiętać, że jest to książka napisana przez zresocjalizowanego hakera. Stąd wynika jej niepokojąca dwuznaczność. Z jednej strony ukazuje dziury bezpieczeństwa, które znajdują się w systemach sieciowych, tym samym pozwalając administratorom odkrywać wady wewnątrz sieci, z drugiej jednak stanowi nieocenione źródło informacji dla potencjalnych włamywaczy.

The Fugitive Game: Online With Kevin Mitnick

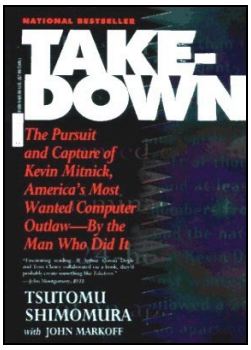


Książka przedstawia dzieje Kevina Mitnicka z czasów wczesnej młodości, zanim to poddał się agentom FBI, którzy zlokalizowali go z pomocą tak zwanego „cybersleuth" Tsutomu Shimomury. Jest dziennikarskim spojrzeniem na zdarzenia, które do tego doprowadziły. Zamieszczono w niej mnóstwo rozmów z Kevinem Mitnickiem.

Littman dokumentuje i analizuje dogłębnie publiczny wizerunek Mitnicka — wroga publicznego numer jeden, którym stał się głównie dzięki dziennikarzowi „New York Timesa" — Johnowi Markoffowi. Jest to interesujące spojrzenie nie tylko na indywidualność Condora, ale też na tworzone przez media mity i bezowocne wysiłki stróżów prawa.

Pozycja godna polecenia ze względu na rzadko spotykaną bezkompromisowość w potraktowaniu tego jakże kontrowersyjnego tematu.

Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw — By the Man Who Did It

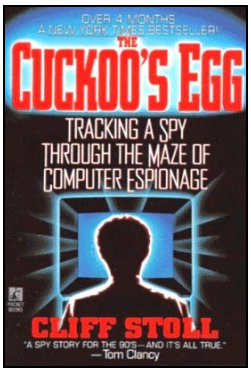


W Święta Bożego Narodzenia 1995 roku pewien cyberprzestępca użył nowej, niebezpiecznej metody, by zyskać dostęp do domowego komputera światowego znawcy w dziedzinie bezpieczeństwa komputerowego. Zaatakowany ujął się honorem i rozpoczął poszukiwania intruza, który naruszył jego prywatność i odkrył, że jest to nie kto inny, ale Wróg Publiczny Numer Jeden Cyberprzestrzeni.

Tak zaczyna się opisywana historia, która nadała wielki rozgłos sprawie ujęcia Kevina Mitnicka. Można się było spodziewać, że wersja stworzona przez Człowieka, Który Tego Dokonał będzie zabawna, ale styl pisania Tsutomu Shimomury pozostawia wiele do życzenia. Zbyt dużo pojawia się w tej całej historii szczegółów osobistego życia Shimomury, podczas gdy techniczne, prawne, i etyczne kwestie pobawione są komentarza. Nieustannie książka ta operuje półprawdami nadając im status faktów, ponieważ nadal nie ma dowodów na to, że Mitnick popełnił przestępstwo.

Książka jest mimo to interesująca.

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage



Pozycja ta zdaje się inspirować całą kategorię książek analizujących sylwetki komputerowych zbrodniarzy. Nawet w kilka lat po jej publikacji i po wielu naśladujących pozycjach, pozostaje dobrą lekturą.

Przedstawia proces przekształcania się Clifforda Stolla w jednoosobową siłę bezpieczeństwa próbującą wyśledzić bezimiennego zbrodniarza, który włamał się do komputera uniwersyteckiego laboratorium.

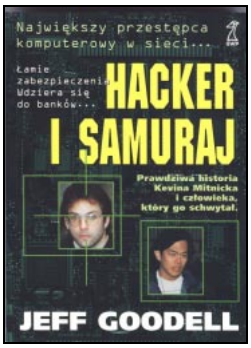
Co zaskakujące — problemy, które na początku wydają się 75% błędami systemu komputerowego, ostatecznie stają się pierścieniem przemysłowego szpiegostwa. A dzieje się tak głównie dzięki wytrwałości i intelektualnemu uporowi Stolla.

Stoll zakładał bowiem pułapki „na szpiega" w zarządzanych przez siebie sieciach i w ten sposób rozpoczął międzynarodowe poszukiwania, które ostatecznie pociągnęły za sobą FBI, CIA i niemieckie Bundespost.

Tak wytropił hakera o pseudonimie *Hunter* — tajemniczego włamywacza, który za cel obrał sobie U.S. ARMY komputera systemowego.

Książka ta jest obowiązkową pozycją, którą przeczytać powinien każdy haker i... administrator sieci. Niedawno ukazała się w Polsce.

Haker i Samuraj



Jest to kolejna pozycja poświęcona historii Kevina Mitnicka, który był najbardziej poszukiwanym hakerem na świecie. Nazywano go „Condorem" i „Obywatelem Cyberpunkiem". Był buntownikiem. Samotnikiem. Biednym dzieciakiem z Kalifornii, który grał na nosie społeczeństwu, wdzierając się do sieci telefonicznych central międzynarodowych korporacji. Nawet działania FBI nie stanowiły dla niego zagrożenia.

Kevin Mitnick dokonał bowiem „niemożliwego": wdarł się do osobistego komputera człowieka uważanego za mistrza cyberochrony. Tsutomu Shimomura — współczesny samuraj intelektu zawziął się i postanowił powstrzymać Kevina. Ale autostrada informatyczna to świetne miejsce do ucieczki bez końca. I tak zaczęła się wojna samuraja i cybernetycznego bandyty.

Warto podkreślić — historia autentyczna, którą poznajemy rzetelnie wpisaną w realia kroniki amerykańskiej hakerki ostatnich dziesięciu lat. Książka składa się z pięciu rozdziałów; pierwsze dwa: „Ucieczka" i „Grzech pierworodny" ukazują początki działania osób podobnych Kevinowi, sposoby ich działania, pozyskiwania informacji, motywy. Wzajemne animozje, które występują między nimi, powodują nie tylko narastanie konfliktów, ale doprowadzają w ostateczności do donoszenia składanych organom ścigania. Efektem tego jest konieczność ukrywania się. Te i inne przyczyny sprawiają, że zamknięte zostały drzwi wielkich firm przed takimi osobami jak Kevin. A dla hakerów jego pokroju celem było zdobycie pracy. Szczyt marzeń stanowiła praca programisty czy konsultanta do spraw bezpieczeństwa. W rezulacie Kevin i jemu podobni zamykali się we własnym świecie, gdzie byli idolami. Motorem ich działań z wolna stawała się myślą o tym tylko, by złamać jak najwięcej systemów, oszukać jak najlepsze firmy, jak najdłużej się ukrywać. Często posuwali się do szantażu zarówno wśród ludzi „ze środowiska", jak i ludzi pracujących w firmach, w których sami chcieliby być zatrudnieni.

Następne dwa rozdziały — noszące tytuły „Pościg" i „Wejście samuraja" — przedstawiają sposób tropienia przestępcy. Dodatkowo opisany jest sposób śledzenia Kevina. Haker, używający przenośnego laptopa i modemu komórkowego był śledzony, namierzany i podsłuchiwany przez FBI i inne osoby pomagające tej organizacji. A wszystko to działo się za pozwoleniem i w majestacie prawa.

Ostatni rozdział — „Śnieg w oczy" — jest swego rodzaju posłowiem. Nawiązuje on do tego, że Kevin został ukazany w masmediach jako uosobienie zła. Nie było to takie trudne, zważywszy na to, że kiedy Kevin zaczynał „bawić" się w hakera, świadomość komputerowa społeczeństwa była zerowa. Komputer był nadal symbolem, przysłowiową czarną skrzynką, a włamywacze komputerowi źle byli odbierani przez społeczeństwo.

Z biegiem czasu świadomość komputerowa wzrosła. Nie jest to takie trudne do zrozumienia, chociażby ze względu na stale rozwijający się rynek komputerów i malejące ceny produktów najnowszej techniki. Mimo to większość ludzi pokroju Mitnicka żyła cały czas z piętnem przestępcy, gdyż obciążano ich winą za bezprawie panujące w Internecie. Policja potrzebowała symbolu, a media takowy wykreowały. Idealny okazał się Kevin Mitnick, żydowski chłopak z Panorama City. Był zatem ścigany przez prawo i skończył w więzieniu, podczas gdy inni zbili fortunę.

Książka prowokuje do stawania charakterystycznych pytań, zaczynających się od „gdyby". Gdyby Kevin znalazł pracę w przemyśle, gdyby się nie włamał do komputera Shimomury, gdyby... Właśnie — co by było, gdyby... Często w życiu stawiamy to pytanie. Często na nie odpowiadamy najprościej jak można. Nic nie byłoby, gdyby, bo i tak wszystko jest, jak być powinno. Różnie to się tłumaczy. Czasem dlatego, że Bóg tak chciał, innym razem opatrzność, przypadek... Sedno w tym, że takie przypadki często decydują o losach ludzi. I podkreślają ich kruchość, nieprzewidywalność...

W trakcie rozwoju lektury pojawiają się znane wszystkim interesującym się techniką komputerową nazwy firm, organizacji, systemów operacyjnych, pośredników dostępu do Internetu, a także programów i osób znanych w Internecie. Co zatem można znaleźć? Przede wszystkim: Digital i jego produkt — VAX/VMS (Kevin był specem od tego systemu), SCO i jej wersja Unikaa, Netcom, wspomniane już Naczelne Dowództwo Armii Amerykańskiej i ich NORAD (spopularyzowane w filmie „Gry Wojenne"), elektroniczne magazyny hakerskie: 2600 — The Hacker Quarterly, Phrack, Wired, „Cyberpunk", przysłowiową biblię hakerów, CERT (*Central Emergency Response Team*), EFF (*Electronic Frontier Foundation*), Crack, SATAN.

Nie sposób nie zauważyć jednak pewnych uchybień czy nawet błędnych przekładów, które można znaleźć w tej książce. Na przykład logi systemowe zostały przetłumaczone jako „dzienniki systemowe" (po angielsku *logbook* to dziennik okrętowy). Ponadto często pojawia się wyrażenie „notatka e-mail", a IRC został przedstawiony jako kanał głosowy (!) w Internecie, program Crack został przedstawiony jako „Cracker", a Satan jako „Szatan"... Ale to są drobiazgi, które nie są w stanie zniekształcić idei książki.

Bo przede wszystkim jest to „żywo napisana historia wzlotów i upadków Kevina Mitnicka, jednego z negatywnych bohaterów naszych internetowych czasów".

Hacker's Black Book

Pozycja ta to kultowy tekst wszystkich fanatyków komputera i Internetu, którzy potrzebują narzędzi hakerskich dla zaspokojenia własnych potrzeb, a ponadto chcą zrozumieć przykłady i instrukcje CKH. Wydanie zawiera jeszcze dodatkowe supertematy, które autor starannie przestudiował. Dostarcza więc wyjaśnień na pytanie o to, jak można za darmo dzwonić z budki telefonicznej bez manipulowania numerami telefonicznymi czy obejść limit czasowy przeznaczony dla demo/trial/software. Książka jest bezcenna dla każdego użytkownika Internetu.

W dziewiętnastu obszernych rozdziałach autor szczegółowo przedstawia techniki profesjonalnych hakerów. Tak aktualnych informacji nie można znaleźć w żadnej innej książce dostępnej w aktualnie na rynku księgarskim.

Warto dodać, że przy opracowywaniu tej książki uczestniczyli legendarni hakerzy z byłych grup Thistar, Red Sector i Alphaflight. Dzięki temu skomplikowane techniki rozmaitych typów ataków wyjaśnione są w prosty sposób. Znaleźć tu można także informacje na temat penetracji obcych dysków twardych oraz sposoby na to, by zmienić lub obejrzeć za pomocą koni trojańskich i innych tricków zawartość innych dysków twardych komputerów podłączonych do sieci czy bezpłatnie oglądać TV lub wysyłać anonimowe maile i bomby mailowe.

Bonus dołączony do każdego zamówienia dodatkowo zawiera hasło dojścia dla chronionego działu, dostępnego tylko dla czytelników. Można w nim znaleźć wiele narzędzi do realizacji metod opisanych w książce. Ponadto dołączony jest także CD-ROM.