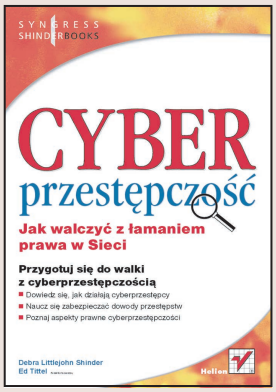
Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci



Autorzy: Debra Littlejohn Shinder, Ed Tittel (Technical Editor)
Tłumaczenie: Jarosław Dobrzański (wstęp, rozdz. 6 – 11, dod. A, B), Krzysztof Masłowski (rozdz. 1 – 5)
ISBN: 83-7361-436-2
Tytuł oryginału: Scene of the Cybercrime. Computer Forensics Handbook
Format: B5, stron: 656

Przygotuj się do walki z cyberprzestępczością

- Dowiedz się, jak działają cyberprzestępcy
- Naucz się zabezpieczać dowody przestępstw
- Poznaj aspekty prawne cyberprzestępczości

Jeszcze całkiem niedawno termin „cyberprzestępczość" kojarzył się wyłącznie z powieściami, filmami i grami komputerowymi o tematyce science-fiction. Dziś cyberprzestępczość to coś, z czym spotykamy się niemal codziennie. Wirusy, dialery, włamania do sieci korporacyjnych, nielegalne kopiowanie oprogramowania i danych to przejawy cyberprzestępczości, które stały się powszechne. Rozpowszechnienie internetu i możliwość zachowania w nim anonimowości tworzą idealne warunki dla wszystkich, którzy chcą wykorzystać komputer niezgodnie z prawem.

„Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci" to książka przeznaczona zarówno dla informatyków, jak i dla przedstawicieli prawa. Pokazuje, w jaki sposób można zabezpieczyć się przed atakami komputerowych przestępców, jak z nimi walczyć i jak zapobiegać szerzeniu się cyberprzestępczości. Dzięki niej informatycy zrozumieją aspekty prawne walki z komputerowymi przestępcami, a pracownicy wymiaru sprawiedliwości dowiedzą się, w jaki sposób działają ci, których ścigają.

W książce opisano:

- Historię cyberprzestępczości
- Aspekty psychologiczne walki z cyberprzestępczością
- Podstawy działania komputerów i sieci komputerowych
- Techniki włamań do sieci i ataków na serwery sieciowe
- Sposoby zapobiegania cyberprzestępstwom
- Metody zabezpieczania danych
- Techniki wykrywania cyberprzestępstw i zabezpieczania ich dowodów
- Podstawy prawne oskarżenia o cyberprzestępstwo

Włącz się do walki z komputerowymi przestępcami –; przyszłość internetu jest również w Twoich rękach.

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

Spis treści

Rozdział 1.

Twarzą w twarz z problemem cyberprzestępczości

Oto tematy, którymi zajmiemy się w tym rozdziale:

- Definiowanie cyberprzestępstwa
- Kategoryzacja cyberprzestępstw
- Walka z cyberprzestępczością
- Podsumowanie
- Najczęściej zadawane pytania
- Źródła

Wstęp

Obecnie żyjemy i pracujemy w świecie globalnej łączności. Z osobą na drugim końcu świata szybko i tanio możemy zamienić parę słów lub przeprowadzić z nią wielomilionową transakcję. Rozpowszechnienie komputerów osobistych, łatwy dostęp do Internetu i boom na rynku nowych urządzeń komunikacyjnych odmieniły nasz sposób życia i spędzania wolnego czasu oraz metody prowadzenia interesów.

Kryminaliści również zmienili sposoby popełniania przestępstw. Powszechna dostępność do sieci daje nowe możliwości osobom, które nie mają skrupułów. Ich komputerowa biegłość powoduje, że konsumenci i firmy tracą miliony dolarów. Co gorsza, komputery i sieci mogą służyć do nękania ofiar, a nawet wystawiają je na gwałtowne ataki, a także mogą zostać użyte do koordynowania i przeprowadzania, budzących w nas grozę, ataków terrorystycznych. Niestety w wielu przypadkach instytucje pilnujące

przestrzegania prawa pozostają w tyle za kryminalistami z powodu braku nowoczesnych technologii i wyszkolonego personelu zdolnego stawić czoła nowej, narastającej fali zagrożeń, które zaczęliśmy nazywać cyberprzestępstwami.

Jeszcze do niedawna liczni specjaliści z dziedziny technologii infomatyczno-informacyjnych (IT) nie przywiązywali wagi do zjawiska cyberprzestępczości. W wielu przypadkach przedstawicielom sprawiedliwości brakowało narzędzi do radzenia sobie z tym problemem: stare prawa nie pasowały do obecnie popełnianych przestępstw, nowe nie obejmowały wszystkiego, co się zdarza, a niewiele było spraw precedensowych, do których można by się odwołać. Ponadto debaty na temat prywatności ograniczały możliwości zbierania dowodów koniecznych do formułowania aktów oskarżenia. Na koniec, istniała pewna antypatia, a przynajmniej brak zaufania między przedstawicielami sprawiedliwości i specjalistami od komputerów. A ich współpraca jest konieczna, jeżeli chcemy, aby cyberprzestępstwa nie wymknęły się spod kontroli, a Internet pozostał dla jego użytkowników miejscem spokojnym i bezpiecznym.

Przedstawiciele prawa znają sposób myślenia i predyspozycje kryminalistów, potrafią zebrać dowody w celu postawienia przestępców przed sądem. Personel IT rozumie działanie komputerów i sieci, wie, w jaki sposób wyśledzić w nich potrzebne informacje. Każda z tych grup ma „połowę klucza", czyli dysponuje połową środków potrzebnych do skutecznego zwalczania cyberprzestępczości. Celem tej książki jest połączenie tych połówek i pokazanie, w jaki sposób obie grupy mogą i muszą współpracować, by była możliwa obrona przed cyberprzestępcami oraz ich aresztowanie i stawianie przed sądem za działania na szkodę osób prywatnych, organizacji, firm i całego społeczeństwa.

Ocena wielkości kryzysu

Słowo „cyberprzestępstwo" brzmi egzotycznie, trochę jak z futurystycznych powieści science fiction. Jednakże pracownicy instytucji pilnujących przestrzegania prawa, administratorzy sieci i inni, którzy stykają się z przestępstwami i (lub) cyberprzestrzenią, zauważają, że cyberprzestępstwa są znacznym problemem i ich liczba wciąż rośnie. Oto przykłady.

- Według Internet Fraud Complaint Center[1] (IFCC), utworzonego w wyniku współpracy Federal Bureau of Investigation (FBI), i National White Collar Crime Center[2] od maja 2000 do maja 2001, czyli w pierwszym roku działania tej instytucji, wpłynęły do jej serwisu WWW 30503 skargi na oszustwa internetowe (pełny raport w formacie .PDF można ściągnąć z: *www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf*).

[1] Centrum Skarg na Oszustwa Internetowe — *przyp. tłum.*

[2] NW3C — w prasie polskiej używa się czasem nieformalnej nazwy: agencja zwalczania przestępczości „w białych rękawiczkach", chociaż sam termin „white collar crime" jest na ogół tłumaczony jako „przestępstwo urzędnicze", bowiem w USA „white collar" (biały kołnierzyk) to popularna nazwa urzędnika, „blue collar" (niebieski kołnierzyk) jest określeniem pracownika fizycznego — *przyp. tłum.*

- Według sondażu „Computer Crime and Security Survey”[3] za rok 2001, przeprowadzonego i wydanego przez Computer Security Institute[4] przy współpracy z FBI Computer Intrusion Squad[5], 186 respondentów — firm i agencji rządowych — zgłosiło straty na ogólną sumę 3,5 miliona dolarów, spowodowane głównie kradzieżą informacji i oszustwami finansowymi (patrz: *www.gocsi.com/press/20020407.html*).
- Według Cybersnitch Voluntary Online Crime Reporting System[6] przestępstwa związane z Internetem obejmują zakres od fałszerstw dokonywanych za pomocą komputerów osobistych po dziecięcą pornografię i przestępstwa bardziej gwałtowne, takie jak electronical stalking[7] i groźby terrorystyczne (pełna lista zgłoszonych cyberprzestępstw jest dostępna pod adresem *www.cybersnitch.net/csinfo/csdatabase.asp*).
- Według Meridien Research[8] oczekiwane koszty przestępstw internetowych w roku 2005 będą się mieścić w przedziale od 5 do 15 miliardów dolarów (patrz: *www.epaynews.com/statistics/fraud.html*).

Choć rezultaty cyberprzestępstw mogą być odczuwalne przez każdego, najczęściej muszą sobie z nimi radzić dwie grupy osób:

- ci, którzy zajmują się zawodowo technologiami informatycznymi, często odpowiedzialni za pierwszą linię obrony i śledzenie sprawców cyberprzestępstw,
- służby pilnujące przestrzegania prawa, odpowiedzialne za porządkowanie przepisów, określanie jurysdykcji i praktyczne działania mające doprowadzić do osądzenia cyberprzestępców.

Cyberstatystyka

Eksplozja populacji on-line

Według Nua Internet Surveys[9] w lutym 2002 roku 544 miliony ludzi korzystały z połączeń on-line. W przyszłości wzrost populacji „obecnych w sieci” będzie zwiększał pole działania cyberprzestępców i łamanie przez nich prawa dotknie większą liczbę osób.

[3] Doroczny sondaż na temat przestępstw komputerowych i bezpieczeństwa sieci — *przyp. tłum.*

[4] Instytut Bezpieczeństwa Komputerów — *przyp. tłum.*

[5] Oddział ds. Włamań Komputerowych FBI — *przyp. tłum.*

[6] Ochotniczy system on-line rejestracji przestępstw — *przyp. tłum.*

[7] Wywieranie nacisku, śledzenie i zastraszanie za pomocą środków elektronicznych. W ten sposób firmy, różne organizacje i czasami władze osaczają obywateli, lecz jest to proces działający też w drugą stronę, gdyż dzięki internetowi posiadająca odpowiednie umiejętności „zwierzyna łowna” może łatwo zamienić się w „myśliwych” — *przyp. tłum.*

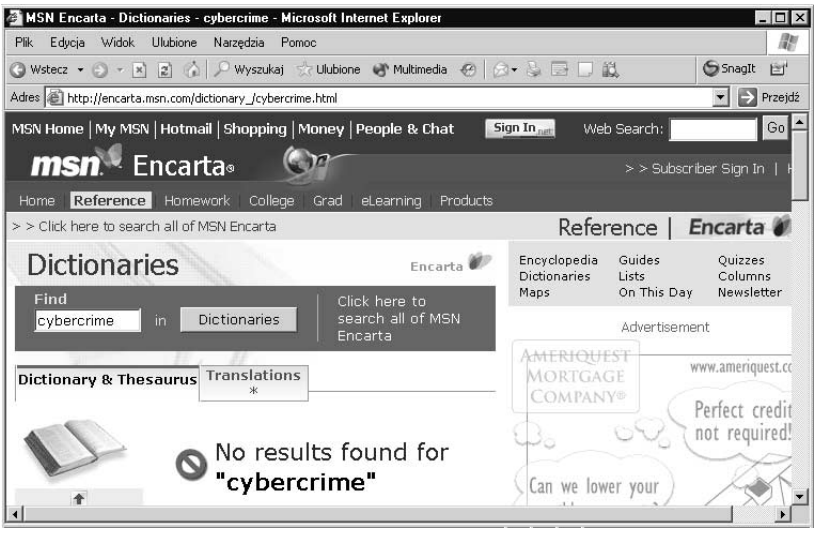
[8] Amerykańska firma analityczno-badawcza — *przyp. tłum.*

[9] Irlandzka firma publikująca w internecie przeglądy (zestawienia) dotyczące różnych działów życia i gospodarki — *www.nua.ie/surveys — przyp. tłum.*

Do wygrania wojny z cyberprzestępcami konieczne jest współdziałanie tych dwóch grup zawodowych, a dotychczasowe rozbieżności między nimi wynikają z wzajemnego niezrozumienia działań drugiej strony i własnej roli w walce z cyberprzestępczością.

Definiowanie cyberprzestępstwa

Definicji cyberprzestępstwa być może nie znajdziecie w słowniku (jak na ironię, nie ma jej nawet w słowniku internetowym Microsoftu „Encarta World Dictionary 2003, co widać na rysunku 1.1.), ale użycie wyszukiwarki Google daje odniesienia do ponad 140 000 miejsc w sieci.



Rysunek 1.1. *Słowa „cybercrime" (cyberprzestępczość) nie ma w wielu słownikach, również w „Encarcie" Microsoftu*

Możemy oficjalnie nie wiedzieć, czym jest cyberprzestępstwo, ale w rozmowach używamy tego określenia. Prawnicy i prawodawcy na całym świecie, mimo braku definicji, wierzą w istnienie cyberprzestępstw, gdyż „muszą uwierzyć w to, co widzą" (cytujemy tu Pottera Stewarta, sędziego Sądu Najwyższego USA, który w roku 1964 tak wypowiedział się na temat „nieprzyzwoitości"). Prawa dotyczące przestępstw dokonywanych on-line przechodzą przez procedury legislacyjne, a po powolnym starcie prace ich dotyczące nabierają tempa.

Departamenty policji w Stanach Zjednoczonych i w innych krajach na całym świecie tworzą specjalne jednostki do zwalczania przestępstw komputerowych, a znaczną część ich pracy stanowi walka z cyberprzestępczością. National Cybercrime Training Partnership[10] (NCTP) obejmuje lokalne, stanowe i federalne organy wymiaru sprawiedliwości Stanów Zjednoczonych. Raz do roku International Association of Chiefs

[10] W wolnym przekładzie „narodowe partnerstwo ds. szkoleń w dziedzinie cyberprzestępczości". Więcej informacji można znaleźć pod adresem *www.nctp.org — przyp. tłum.*

of Police (IACP)[11] organizuje konferencję szkoleniową Law Enforcement Information Management, poświęconą zagadnieniom IT i cyberprzestępczości. Unia Europejska utworzyła Forum on Cybercrime[12] i wiele krajów europejskich podpisało Europejską Konwencję o Cyberprzestępczości[13], której zadaniem jest standaryzacja prawa europejskiego dotyczącego przestępczości w Internecie.

Każda organizacja i każdy prawodawca nieco inaczej pojmuje cyberprzestępczość. Niektóre definicje różnią się bardzo, inne niewiele. Aby w tej książce efektywnie omawiać cyberprzestępczość, potrzebujemy definicji roboczej. Dopiero pod koniec spróbujemy podać definicję ogólną i określić różne rodzaje cyberprzestępstw.

Od ogółu do szczegółu

Cyberprzestępczość należy uznać za podkategorię przestępczości komputerowej. Pojęciem tym określamy wszelkie rodzaje przestępstw, do popełnienia których użyto Internetu lub innych sieci komputerowych. Komputery i sieci komputerowe mogą służyć do popełniania przestępstw na kilka sposobów.

- Komputer lub sieć mogą być narzędziem przestępstwa (zostaną użyte do jego popełnienia).
- Komputer lub sieć mogą być celem przestępstwa (ofiarą).
- Komputer lub sieć mogą być użyte do zadań dodatkowych związanych z popełnieniem przestępstwa (na przykład do przechowywania danych o nielegalnej sprzedaży narkotyków).

Prawo, aby być podstawą egzekucji, musi być ścisłe i specyficzne. Ogólna definicja jest przydatna podczas dyskusji, ale przestępstwa to określone działania lub zaniechania wraz z określonym poczuciem winy.

W wielu przypadkach poszczególne elementy ustaw zawierają definicje pojęć. Jest to niezbędne w celu uniknięcia pomyłek, sprzeczności i dodatkowych procesów, które mogłyby wyniknąć ze stosowania tych praw lub przepisów. Definicje powinny być w miarę możności zawężone, ale zadanie to jest często źle wykonywane przez prawodawców (którzy czasami nie formułują dokładnych definicji terminów, pozostawiając odgadywanie ich znaczenia organom sprawiedliwości do czasu, aż sąd wyda wyrok).

---

[11] Międzynarodowe Stowarzyszenie Szefów Policji jest najstarszą i największą na świecie organizacją pozarządową skupiającą szefów policji z 89 krajów. Istnieje od roku 1893, ma ponad 19 000 członków i służy przede wszystkim badaniom i rozwijaniu (ulepszaniu) metod działania policji, patrz: strona *http://www.theiacp.org/ — przyp. tłum.*

[12] Lub European Forum on Cybercrime — Europejskie Forum dot. Cyberprzestępczości — *przyp. tłum.*

[13] Council of Europe Convention on Cybercrime, co bywa tłumaczone różnie, między innymi jako Europejska Konwencja o Cyberprzestępczości lub Konwencja Rady Europy o Cyberprzestępczości — *przyp. tłum.*

Jednym z głównych zarzutów wobec konwencji europejskiej jest wielka ogólnikowość definicji, na przykład definicja „dostawcy usług" (*service provider*) jest tak niejasna, że może odnosić się nawet do kogoś, kto zbudował sobie w domu sieć złożoną z dwóch komputerów, a definicja „danych komputerowych" (*computer data*) obejmuje każdą reprezentację faktów, informacji i pojęć zapisaną w dowolnej postaci, pozwalającej na przetwarzanie za pomocą komputera, co może dotyczyć prawie wszystkich sposobów komunikowania, łącznie z mową i pismem odręcznym (które mogą być przetwarzane przy użyciu oprogramowania przeznaczonego do rozpoznawania mowy lub pisma). Podobnie Departament Sprawiedliwości USA był krytykowany za definicję „przestępstwa komputerowego" (*computer crime*), za jakie uznano „wszelkie pogwałcenie prawa, które dotyczyło użycia wiedzy komputerowej na etapie dokonania przestępstwa, śledztwa i oskarżenia" (według „Law Enforcement Bulletin", sierpień 2002). Zgodnie z tą definicją każde przestępstwo może być uznane za przestępstwo komputerowe po prostu dlatego, że detektywi badający sprawę podczas śledztwa przeglądali komputerowe bazy danych.

Przykłady te ilustrują trudności, z którymi należy się uporać przy tworzeniu użytecznych definicji cyberprzestępstwa i pojęć pokrewnych. W dalszej części tego rozdziału opracujemy własną roboczą definicję cyberprzestępstwa, wystarczającą na potrzeby tej książki.

Rozumienie ważności zagadnień jurysdykcyjnych

Innym czynnikiem utrudniającym stworzenie jednej obowiązującej definicji cyberprzestępczości jest jurysdykcja. W różnych kodeksach pojęcia bywają odmiennie definiowane, co jest ważne dla pracowników wymiaru sprawiedliwości prowadzących dochodzenia i administratorów sieci, którzy chcieliby uczestniczyć w przygotowywaniu aktów oskarżenia dotyczących cyberprzestępstw dokonanych na szkodę ich sieci. Obie grupy powinny znać prawa mające w danych sytuacjach zastosowanie. W większości przestępstw dokonywanych na terenie Stanów Zjednoczonych oznacza to zaznajomienie się z przepisami lokalnymi i prawami stanowymi dotyczącymi danego przestępstwa. Zwykle działalność przestępcza podlega jurysdykcji prawa w miejscu dokonania przestępstwa.

Ponieważ większość cyberprzestępstw jest dokonywana w miejscu „wirtualnym", nazywanym cyberprzestrzenią, bywa, że trudno ustalić, jakie prawa należy stosować. Często atakujący i ofiara są od siebie oddaleni o setki lub tysiące mil i być może nigdy nie przebywali w tym samym stanie lub nawet tym samym kraju. Ponieważ w różnych rejonach świata prawa mogą różnić się drastycznie, to, co w jednym miejscu jest przestępstwem, w innym może być działaniem zgodnym z prawem.

Co zrobić, gdy ktoś z Kalifornii, mającej liberalne prawa obyczajowe, udostępnia w Internecie zdjęcia pornograficzne, które można oglądać w Tennessee, gdzie obyczaje, od których zależą prawa stanowe, są o wiele surowsze? Jurysdykcji którego stanu podlega taka czynność? Czy można kogoś oskarżyć i skazać według prawa stanu, w którym nigdy nie był? Rzeczywiście było to problemem sporu w precedensowym procesie USA przeciw Thomasowi i Thomasowi[14] (patrz: „Przegląd cyberprawa" w ramce poniżej).

[14] U.S. v. Thomas and Thomas — *przyp. tłum.*

Przegląd cyberprawa

U.S. v. Thomas and Thomas

Mieszkający w Kalifornii Robert i Carleen Thomas zostali oskarżeni z powodu złamania praw obyczajowych stanu Tennessee, gdy urzędnik organów sprawiedliwości w Memphis ściągnął na swój komputer w Tennessee z ich BBS-u[15] materiały o wyraźnie seksualnej treści. Zdarzyło się wówczas po raz pierwszy, że oskarżenie dotyczące obsceniczności materiałów zostało wysunięte przez organa ścigania w miejscu ściągnięcia informacji, a nie w miejscu jej pochodzenia. Oskarżeni zostali skazani i złożyli apelację. Sąd apelacyjny podtrzymał oskarżenie i wyrok skazujący. Sąd Najwyższy apelację odrzucił.

Jeżeli nawet jakiś czyn jest przestępstwem w obu jurysdykcjach, zwykle nikt nie kwapi się z formułowaniem oskarżenia z powodu problemów geograficznych, które mogą się stać koszmarem w postępowaniu sądowym (patrz: ramka „Z życia wzięte" w dalszej części tego rozdziału).

Sprawy jurysdykcji omówimy bardziej szczegółowo w rozdziale 11.

Z życia wzięte

Doświadczenia Wesa Edensa oficera śledczego i komputerowego specjalisty sądowego

Oto typowy przykład, w jaki sposób procesy wielojurysdykcyjne komplikują życie detektywom policyjnym. Postawcie się na miejscu detektywa i wyobraźcie sobie, że mieszkający w Oklahomie i podlegający tamtejszej jurysdykcji Bob Smith zgłasza, że za pomocą jego karty kredytowej dokonano kilku oszukańczych zakupów. Ponadto informuje, że, podając dane przez Internet, otwarto na jego nazwisko konta w dwóch bankach: Netbanku, mającym siedzibę w Georgii i w Wingspan, który został ostatnio zakupiony przez Bank One.

Podejrzany(i) wystąpił(li) o kredyt na zakup samochodu w Dallas w Teksasie. W profilu jego karty kredytowej zmienili adres Boba na ul. Jakąśtam 123 w Dallas. Jest to oczywiście adres nieprawdziwy.

Podczas śledztwa kontaktujesz się z Netbankiem w Georgii, gdzie informują, że nie przechowują adresów IP (Internet Protocol)[16] osób otwierających konta on-line. Otrzymujesz kopię formularza kredytowego złożonego przez sieć. Zawiera on wszystkie dane Boba Smitha, tylko adres jest zmieniony.

[15] BBS (Bulletin Board Service) — popularny w latach 80. i wczesnych 90. elektroniczny system rozpowszechniania i wymiany informacji między komputerami. Aby skorzystać z zasobów BBS-u, użytkownik dzwoni za pomocą modemu na numer telefoniczny BBS-u i loguje się do serwera, który umożliwia m.in. wysyłanie listów e-mail, ściąganie plików oraz prowadzenie dyskusji na żywo. Pierwszy BBS powstał w Chicago w 1978 r. Obecnie stracił znaczenie z powodu rozwoju internetu — *przyp. tłum.*

[16] Adres IP — 32-bitowy adres komputera w sieci internetowej. Każdy komputer w internecie posiada unikalny adres IP służący do jego jednoznacznej identyfikacji — *przyp. tłum.*

Kontaktujesz się ze wszystkimi firmami, w których dokonano zakupów przy użyciu fałszywej karty Boba Smitha. Połowa firm nie chce rozmawiać bez papierowej „podkładki" wystawionej przez sąd stanu, w którym działają, a nie stanu, w którym się znajdujesz. Musisz więc w pięciu stanach odnaleźć departamenty policji skłonne pomóc w załatwieniu dokumentów zezwalających na sięgnięcie do rekordów firm. Ponieważ nie sformułowałeś jeszcze żadnych oskarżeń, a ofiara (i zapewne również podejrzany) mieszkają poza zasięgiem jurysdykcji instytucji, do których się zwracasz, nie palą się one do mieszania się w tę sprawę.

Wreszcie otrzymujesz dokumenty od mniej więcej połowy firm. Tylko jedna odnotowała adres IP. Jest to konto w American Online (AOL), co oznacza, że można było korzystać z niego w dowolnym miejscu na świecie, co jeszcze powiększa koszmar jurysdykcyjny. Mimo to nie rezygnujesz. Zdobywasz wezwanie sądowe dla AOL z żądaniem podania informacji o subskrybencie danego numeru IP z danego dnia i godziny. Trzy tygodnie później AOL informuję, że przechowuje logi tylko przez 21 dni, co oznacza, że nie masz szczęścia, gdyż wydarzenie miało miejsce dwa miesiące temu.

Sprawdziłeś 15 numerów telefonicznych używanych do obsługi podejrzanych rachunków. Każdy był inny. Trzy razy telefonowano z Dallas, dwa razy z Forth Worth, a pozostałe to numery już nieistniejące lub rozproszone po różnych miastach południowego Teksasu. Nic ich nie łączyło. Zająłeś się więc adresami, pod które wysyłano zakupione towary. I znowu każdy był inny: trzy w Dallas, dwa w Forth Worth. Kilka innych to adresy pokojów do wynajęcia opłacanych tygodniowo lub wynajmowanych przejściowo w domach, gdzie lokatorzy zmieniali się jak pasażerowie w autobusie. Kilka było adresami post restante. Zażądałeś dostarczenia tych rekordów tylko po to, by się przekonać, że są fałszywe.

Postanowiłeś zatem odwiedzić szefa i wyjaśnić, że musisz wyjechać na kilka dni do innego stanu, aby rozwiązać sprawę dowcipu za 1500 dolarów. Będzie słuchał z uwagą, dopóki nie zaczniesz mówić o odwiedzeniu Georgii, Marylandu i Teksasu. Powiesz mu wówczas, że masz także trzy inne sprawy, które dotyczą dziewięciu innych stanów i że prawdopodobnie nie unikniesz odwiedzenia każdego z nich. Zobaczysz jedynie, jak się zaśmieje, wychodząc z pokoju.

Spróbuj, choćby dla żartu porozmawiać z prokuratorem okręgowym. Gdy wytłumaczysz co i jak, usłyszysz pytanie: Jakie przestępstwo zostało popełnione? (odpowiesz: „Żadne, o którym wiedziałbym na pewno"). Czy podejrzany mieszka tutaj? (Zapewne nie). Czy możemy pokazać, że nastąpiło przekazanie pieniędzy lub jakiś fizyczny kontakt podejrzanego z ofiarą? (No nie, niecałkiem). Czy może pan określić, gdzie przebywa podejrzany? (Prawdopodobnie w Teksasie). Czy któryś z tych zakupów został dokonany w Oklahomie? (Nie). Dlaczego pan prowadzi dochodzenie? (Ponieważ ofiara siedzi w moim biurze).

Prokurator okręgowy powie, że ofiara powinna zawiadomić o tym przestępstwie władze Teksasu. Dajesz poszkodowanemu adresy siedmiu różnych urzędów w Teksasie, jednego w Georgii i jednego w Maryland. Mówisz mu, że powinien się z nimi skontaktować. Zadzwoni do Ciebie po trzech dniach i powie, że wszędzie chcą, aby się zgłosił i wypełnił formularze zawiadomienia o przestępstwie, ale on nie może udać się w dwutygodniową podróż liczącą 2000 mil tylko po to, by poinformować, że padł ofiarą przestępstwa. Proponujesz mu, by zgłosił sprawę do FBI, choć jesteś przekonany, że nie zajmą się sprawą fałszerstwa na sumę 1500 dolarów.

Rzucasz w kąt tę sprawę i zajmujesz się trzema innymi, które wylądowały na Twoim biurku, gdy zajmowałeś się tamtą. Dotyczą kradzieży danych personalnych, a przestępstw we wszystkich przypadkach — tak jak i w pierwszej sprawie — dokonano w całości przez Internet i wszystkie dotyczą wielu stanów.

Rozróżnienie przestępstw dokonywanych za pomocą sieci od przestępstw zależnych od sieci

Często przestępstwa, które zgodnie z naszą ogólną definicją możemy nazwać cyberprzestępstwami, są „klasyczne", lecz do ich popełnienia w jakiś sposób użyto sieci komputerowej. Ktoś na przykład użył sieci do budowania piramidy finansowej, łańcuszka listów, szukania chętnych do korzystania z usług erotycznych, przyjmowania zakładów w nielegalnej grze hazardowej lub ściągania zdjęć pornograficznych z serwerów lustrzanych (*mirrors*). Wszystkie te działania są przestępstwem, podlegają sądom na danych terytoriach i mogły być dokonane bez użycia sieci komputerowej. Sieć nie była tu istotnym elementem przestępstwa, a zaledwie środkiem działania. Sieci komputerowe umożliwiły popełnianie starych przestępstw na nowe sposoby. Prawa zakazujące takich działań mogą być z powodzeniem stosowane zarówno do tych, którzy robią to za pomocą sieci komputerowych, jak i do tych, którzy przy popełnianiu przestępstw w ogóle nie korzystają z sieci.

Przegląd cyberprawa

Kradzież własności niematerialnej

Kradzież własności niematerialnej, na przykład danych komputerowych, stanowi problem dla tradycyjnych ustaw prawnych obowiązujących w wielu jurysdykcjach na terenie Stanów Zjednoczonych. Powszechna ustawowa definicja kradzieży to „bezprawne przywłaszczenie sobie własności innej osoby bez wyraźnego przyzwolenia właściciela, z intencją pozbawienia właściciela jego własności" (ta definicja pochodzi z kodeksu karnego Teksasu, rozdział 31.03).

Taka definicja sprawdza się w odniesieniu do własności materialnej. Gdy ukradnę twoją kolię brylantową lub laptop Della, moje intencje pozbawienia ciebie twojej własności są oczywiste. Jednakże mogę „ukraść" dane finansowe twojej firmy lub cztery pierwsze rozdziały wielkiej amerykańskiej powieści, którą piszesz, bez pozbawiania cię twojej własności i możliwości korzystania z niej nadal.

Gdybym został oskarżony na podstawie ustawy o kradzieży, mój obrońca mógłby argumentować, że brak cech dokonania przestępstwa.

Z tego powodu ustawy muszą być napisane od nowa, tak aby obejmowały także kradzież własności niematerialnej lub intelektualnej, które nie są obiektami mogącymi w danym czasie pozostawać w posiadaniu tylko jednej osoby.

„Tradycyjne" prawa własności intelektualnej (prawa autorskie — *copywright*, prawa do znaku firmowego — *trademark* i podobne) są prawami cywilnymi, niestosowanymi do formułowania oskarżeń w sprawach karnych inaczej niż za pomocą niektórych nowych ustaw dotyczących wąsko zdefiniowanych typów własności intelektualnej oprogramowania i muzyki. Kilka ustaw federalnych zakazuje kradzieży danych, ale jurysdykcji FBI i innych agencji federalnych podlegają jedynie przypadki kradzieży danych z komputerów rządowych lub gdy dane te stanowią tajemnicę handlową. W większości przypadków oskarżenie musi być sformułowane przez organa stanowe, a stany nie mogą wnosić oskarżeń na podstawie ustaw federalnych. Do niedawna wiele stanów nie miało ustaw obejmujących kradzież danych, ponieważ takie przestępstwo nie pasowało do tradycyjnych ustaw dotyczących kradzieży, a ustaw o „kradzieży własności intelektualnej" nie było.

Inne przestępstwa są unikalne i pojawiły się przed nadejściem epoki Internetu. Przykładem jest nieautoryzowany dostęp. Choć przypomina fizyczne włamanie lub wejście do domu czy biurowca, cechy go charakteryzujące są inne. Według przepisów prawa włamanie lub nieprawne wejście wymagają fizycznej obecności w określonym miejscu, a taki element nie występuje w przypadku przestępstwa popełnianego w cyberprzestrzeni. Dlatego nowe prawa muszą być tak napisane, aby zakazywały takich specyficznych działań.

Zbieranie danych statystycznych dotyczących cyberprzestępstw

Kolejnym problemem przeszkadzającym w adekwatnym sformułowaniu definicji cyberprzestępstwa jest brak danych statystycznych dotyczących tego rodzaju występków. Na początku tego rozdziału podaliśmy niektóre statystyki zebrane przez agencje stworzone do walki z cyberprzestępczością. Jednakże przesyłanie do tych agencji informacji o cyberprzestępstwach jest dobrowolne. Oznacza to, że podane liczby są na pewno znacznie zaniżone i przestępstw dokonywanych w sieciach komputerowych jest znacznie więcej. Dzieje się tak nie tylko dlatego, że cześć cyberprzestępstw pozostaje nieznana (bo to dotyczy wszystkich przestępstw), ale również, a może przede wszystkim z tego powodu, że informacje o cyberprzestępstwach zgłaszanych policji nie są przesyłane do agencji tworzących statystyki.

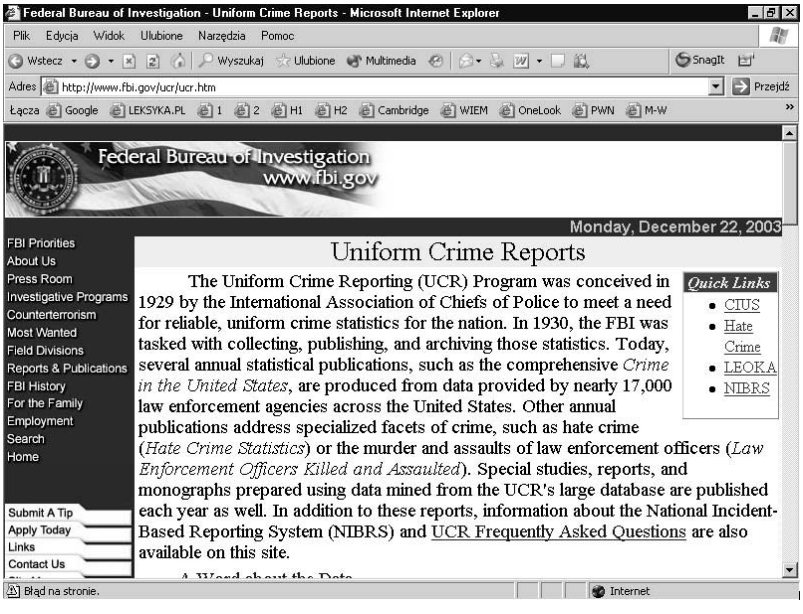
Obecnie nie można nawet ustalić, ile zgłoszeń o cyberprzestępstwach złożono na policji. Aby zrozumieć przyczynę, należy wiedzieć, w jaki sposób są zbierane dane kryminalne w Stanach Zjednoczonych.

Zrozumienie systemu zgłaszania informacji o przestępstwach

Lokalne organa sprawiedliwości — miejskie komisariaty policji i urzędy szeryfów w hrabstwach — są odpowiedzialne za przechowywanie zapisów dotyczących skarg składanych w tych urzędach, przestępstw i śledztw oraz dokonanych aresztowań. Nie ma żadnego obowiązującego standardu tworzenia i przechowywania tych zapisów; każdy urząd lub agencja może utworzyć własną bazę danych, używać jednego lub kilku komercyjnych systemów komputerowego przechowywania informacji lub nawet przechowywać zapisy tworzone ręcznie, co zresztą policja robiła przez lata przez okresem komputeryzacji lokalnych działań rządowych.

FBI, usiłując stworzyć ogólnonarodową statystykę przestępstw, wprowadziło program Uniform Crime Reporting (UCR)[17]. Lokalne organy sprawiedliwości wypełniają miesięczne raporty i przesyłają je do FBI. Te informacje są konsolidowane i publikowane jako oficjalny raport statystyczny o ogólnokrajowej przestępczości. Program ten działa od lat 60. XX w. i zbiera dane z ponad 18000 agencji bezpośrednio lub za pomocą raportów stanowych. Te statystyki są dostępne dla mediów oraz w serwisie internetowym FBI, co zostało pokazane na rysunku 1.2.

[17] Ujednolicone raportowanie przestępstw — *przyp. tłum.*



Rysunek 1.2. *FBI zbiera dane od lokalnych organów sprawiedliwości i upowszechnia je w postaci rocznych raportów statystycznych*

W latach 80. program UCR został rozszerzony i przekształcony w system raportujący dane statystyczne, w którym wszystkie przestępstwa są wprowadzane zgodnie z podziałem na predefiniowane kategorie. National Incident-Based Reporting System (NIBRS)[18] określa dane, które mają być przesyłane bezpośrednio do FBI i przygotowywane za pomocą systemu zgodnego ze standardem NIBRS (agencje, które nie posiadają odpowiedniego wyposażenia, nadal przesyłają raporty w postaci plików UCR).

Kategorie przestępstw w NIBRS

NIBRS pozwala na rejestrowanie większej liczby szczegółów i dzielenie przestępstw na więcej kategorii niż UCR, w którym było możliwe jedynie robienie podsumowań w poszczególnych kategoriach. Mimo wprowadzenia 22 kategorii w grupie A i 11 w grupie B, nie ma żadnej kategorii identyfikującej cyberprzestępstwa (lista kategorii została podana w ramce poniżej).

Cyberstatystyka

Kategorie przestępstw w NIBRS

Według *UCR Handbook* (*NIBRS Edition*, s. 1–2) przestępstwa są podzielone na następujące kategorie i grupy. Wiele danych znajduje się w grupie A, a w grupie B natomiast są tylko przekroczenia zagrożone aresztem.

Grupa A

1. Podpalenie.
2. Napaść (kwalifikowana, prosta, przez zastraszenie).

[18] W wolnym tłumaczeniu: narodowy system raportowania o przestępstwach — *przyp. tłum.*

3. Przekupstwo
4. Włamanie z kradzieżą/włamanie i wejście (najście)
5. Fałszowanie/podrabianie
6. Niszczenie/uszkadzanie/wandalizm
7. Przestępstwa dotyczące narkotyków (i sprzętu z nimi związanego)
8. Malwersacja
9. Wymuszenie/szantaż
10. Oszustwo
11. Przestępstwa dotyczące gier hazardowych
12. Zabójstwo
13. Porwanie/uprowadzenie
14. Złodziejstwo/kradzież (z wyjątkiem kradzieży pojazdów)
15. Kradzież pojazdów
16. Pornografia/nieprzyzwoitość
17. Przestępstwa dotyczące prostytucji
18. Rabunek
19. Przestępstwa seksualne (z użyciem siły)
20. Przestępstwa seksualne (bez użycia siły)
21. Przestępstwa dotyczące własności ukradzionej (bez kradzieży)
22. Pogwałcenie przepisów dotyczących broni

Grupa B

1. Przestępstwa czekowe
2. Godzina policyjna/wałęsanie się/włóczęgostwo
3. Nieodpowiednie zachowywanie się
4. Prowadzenie pojazdu pod wpływem alkoholu
5. Pijaństwo
6. Przestępstwa w rodzinie (bez użycia siły)
7. Nadużywanie silnych alkoholi
8. Podglądactwo
9. Ucieczka
10. Wtargnięcie
11. Pozostałe przestępstwa

Jak wynika z podanej wyżej listy, lokalny urząd, raportując o cyberprzestępstwie, musi albo znaleźć dla niego jedną ze standardowych kategorii (na przykład oszukańcza gra on-line, w której pod fałszywymi pretekstami wyciąga się od ludzi pieniądze niby na cele charytatywne, może być zaklasyfikowana jako *oszustwo*, zaś otwieranie przez Internet plików na czyimś komputerze i ściąganie danych stanowiących tajemnicę handlową może być zakwalifikowane jako *kradzież*), albo umieścić w mieszczącej wszystko kategorii *pozostałe przestępstwa*. Tak czy inaczej, w opracowywanych na podstawie tych danych narodowych raportach o przestępczości nie znajdzie się żadna informacja o cyberprzestępstwach.

Urzędy (agencje), które mają do czynienia z cyberprzestępstwami, muszą tworzyć odrębne kategorie służące do przechowywania informacji na własny użytek, pozwalające na dokładne określanie typów cyberprzestępstw podlegających ich jurysdykcji. Agencje mające wytrawnych specjalistów IT mogą to robić bez pomocy z zewnątrz. Jednak w wielu przypadkach personel lokalnych organów wymiaru sprawiedliwości nie ma technicznego wykształcenia i doświadczenia pozwalającego zrozumieć różnice między różnymi rodzajami przestępstw dokonywanych w sieci. Policjanci mogą rozumieć, co na przykład oznacza hakerstwo, ale trudno im odróżnić hakera, który uzyskuje nieautoryzowany dostęp do sieci, od tego, który doprowadza do załamania działania sieci przez przeprowadzenie ataku odmowy usług (DoS)[19].

Właśnie wtedy profesjonaliści IT powinni współpracować z pracownikami organów sprawiedliwości, aby jasno i dokładnie określić elementy przestępstwa, co umożliwi właściwe przeprowadzenie śledztwa i przygotowanie oskarżenia. Organy ścigania być może będą musiały zatrudniać ekspertów IT ds. bezpieczeństwa jako zewnętrznych konsultantów lub odpowiednio przeszkolić część własnych pracowników, aby potrafili zrozumieć techniczne elementy różnych cyberprzestępstw.

O wzajemnej zależności i współdziałaniu pracowników wymiaru sprawiedliwości i specjalistów IT powiemy dokładnie w rozdziale 11.

Robocza definicja cyberprzestępstwa

Dlaczego tak ważne jest opracowanie standardowej definicji cyberprzestępstwa? Jeżeli nie będziemy stosowali takiej samej — a przynajmniej w zasadzie podobnej — definicji cyberprzestępstwa, personel IT, użytkownicy i ofiary, policjanci, detektywi, prokuratorzy i sędziowie nie będą mogli porozumieć się między sobą. Bez tego nie będzie możliwe tworzenie mających wartość statystyk, przydatnych do analizowania wzorców i trendów popełnianych przestępstw.

Analizy przestępstw pozwalają organom sprawiedliwości lepiej gospodarować zasobami i przygotowywać plany strategiczne mające służyć rozwiązywaniu istotnych problemów. Kierującym urzędami i agencjami trudno ocenić zapotrzebowanie na

[19] Denial of service — celem ataku DoS jest zablokowanie możliwości świadczenia części lub wszystkich usług. Może to być osiągnięte przez wysłanie do serwera ofiary bardzo dużej liczby zapytań, co powoduje jego przeciążenie i znaczne spowolnienie pracy lub zawieszenie usług sieciowych, z których nie mogą wówczas korzystać uprawnieni użytkownicy — *przyp. tłum.*

dodatkowe środki budżetowe (wyspecjalizowany personel, szkolenia, sprzęt itp.) i przedstawić je odpowiednim komitetom i władzom do zatwierdzenia bez posiadania odpowiednich danych uzasadniających żądania. Definicje standardowe i wiarygodne dane statystyczne są także potrzebne w celu edukowania społeczeństwa w dziedzinie zagrożenia cyberprzestępstwami i wciągnięcia go do działań służących ich zwalczaniu. Analiza przestępstw jest podstawą prewencji; zrozumienie, jakie rodzaje przestępstw gdzie i kiedy się zdarzają, i przez kogo zwykle są popełniane, jest konieczne do tworzenia aktywnych planów działań prewencyjnych.

Choć nie możemy powołać się na standardową, obowiązującą definicję, zobaczmy, w jaki sposób cyberprzestępstwo definiują wybitne autorytety.

Amerykańskie ustawy federalne i stanowe

Wspomnieliśmy już o dość szerokiej definicji przestępstw komputerowych przygotowanej przez Departament Sprawiedliwości USA. Poszczególne agencje federalne (i oddziały (wydziały) specjalne tych agencji) stosują swoje własne definicje. Na przykład należący do FBI National Computer Crime Squad (NCCS)[20], powołany do prowadzenia dochodzeń dotyczących przestępstw łamania federalnej ustawy Computer Fraud and Abuse Act[21], dzieli przestępstwa komputerowe i sieciowe, którymi się zajmuje, na następujące kategorie:

- włamania do publicznej komutowanej sieci telefonicznej[22],
- włamania do głównych sieci komputerowych,
- naruszenia integralności sieci,
- naruszenia prywatności,
- szpiegostwo przemysłowe (korporacyjne),
- piractwo programowe,
- inne przestępstwa, w których dokonaniu komputery odgrywają istotną rolę.

Kodeks karny Stanów Zjednoczonych (Title 18, Chapter 47, Section 1030) wylicza działania oszukańcze i podobne dokonywane z użyciem komputerów, ścigane na mocy ustaw federalnych. Większość przestępstw dotyczy danych chronionych przez prawo federalne (takich jak informacje dotyczące bezpieczeństwa narodowego), agencji rządowych, systemu bankowo-finansowego, handlu międzystanowego lub międzynarodowego albo komputerów „chronionych". Definiowanie przestępstw i formułowanie oskarżeń dotyczących przestępstw niezaliczanych do powyższych kategorii pozostaje w kompetencji poszczególnych stanów.

[20] Narodowy oddział ds. przestępstw komputerowych — *przyp. tłum.*

[21] Ustawa z 1984 r. o Przestępstwach i Nadużyciach Komputerowych — *przyp. tłum.*

[22] Public switched telephone network (PSTN) — *przyp. tłum.*

W większości stanów istnieją prawa dotyczące przestępstw komputerowych. Ustawy, których przestrzegania pilnuje policja stanowa i lokalna, mogą zawierać własne definicje poszczególnych terminów. W teksańskim kodeksie karnym w dziale „Przestępstwa komputerowe" znajdujemy na przykład definicję tylko jednego sposobu łamania prawa — naruszenie bezpieczeństwa komputerowego (Breach of Computer Security — Texas Penal Code 33.02), zdefiniowane jako „świadome zdobycie dostępu do komputera, sieci komputerowej lub systemu komputerowego bez przyzwolenia właściciela". Klasyfikacja i kary związane z tym przestępstwem są zależne od wielkości spowodowanych strat finansowych właściciela bądź zysków przestępcy.

Z drugiej strony w kalifornijskim kodeksie karnym (California Penal Code — Section 502) mamy osiem definicji działań uznanych za przestępstwa komputerowe, w tym zmianę, uszkodzenie, skasowanie lub użycie w inny sposób danych w celu dokonania defraudacji; posłużenie się danymi w celu popełnienia oszustwa, wymuszenia, złego zarządzania lub nieuczciwego zdobycia pieniędzy, własności lub danych; korzystanie z usług komputerowych bez zezwolenia; zakłócanie i przerywanie usług komputerowych; asystowanie innej osobie przy uzyskiwaniu nieuprawnionego dostępu do komputera lub wprowadzanie zanieczyszczeń (na przykład wirusów) do systemu komputerowego lub sieci.

Tak więc definicje przestępstw komputerowych są różne w różnych stanach. Jeżeli multijurysdykcyjna natura cyberprzestępstw nie pozwoli nawet zdefiniować tego pojęcia, to nie możemy oczekiwać, że będzie możliwe sformułowanie efektywnego aktu oskarżenia.

Prawo międzynarodowe: ONZ-etowska definicja cyberprzestępstwa

Cyberprzestępstwa przekraczają granice narodowe równie łatwo jak stanowe. Być może to organizacje międzynarodowe powinny dostarczyć standardową definicję cyberprzestępstwa. Na Dziesiątym Kongresie Narodów Zjednoczonych w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców[23], podczas warsztatów poświęconych przestępstwom związanym sieciami komputerowymi, cyberprzestępstwa zostały podzielone na dwie kategorie.

a. **Cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe): wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych i procesowanych przez te systemy danych**.

b. **Cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów): wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych.**

Oczywiście te definicje komplikuje fakt, że działanie w jednym kraju nielegalne, w innym może być dozwolone.

[23] Tenth United nations Congress on the Prevention of Crime and Treatment of Offenders — *przyp. tłum.*

W dokumencie podano bardziej konkretne przykłady, w tym:

- nieautoryzowany dostęp,
- uszkodzenie komputera, danych lub programu,
- sabotaż komputerowy,
- nieautoryzowane przejęcie połączenia,
- szpiegostwo komputerowe.

Te definicje, choć nie do końca określone, stanowią dobry punkt startowy — są początkowym rozpoznaniem i uzgodnieniem w dążeniu do zdefiniowania, co rozumiemy przez termin „cyberprzestępstwo".

Specjalistom IT definicja cyberprzestępstwa jest potrzebna, aby wiedzieli, kiedy (i o czym) mają informować policję, zaś organy sprawiedliwości muszą dysponować ustawowymi definicjami przestępstw, aby oskarżać przestępców o przekroczenie prawa. Pierwszym krokiem do sformułowania specyficznych definicji poszczególnych cyberprzestępstw jest podzielenie na kategorie wszystkich działań mających cechy cyberprzestępstw.

Kategoryzacja cyberprzestępstw

Wysiłki podjęte w celu utworzenia definicji pokazują, iż cyberprzestępstwo jest pojęciem tak szerokim, że nie może zostać użyte w konkretnych przypadkach, a służy jedynie do prowadzenia dyskusji ogólnych.

Oczywiście jeżeli dzwonicie na policję, by powiedzieć, że ktoś się włamał do waszego domu, nie zaczynacie od stwierdzenia, że staliście się ofiarą przestępstwa „pozbawienia własności". Jednak policja, aby zidentyfikować przestępstwo i sporządzić oskarżenie przeciw osobie zidentyfikowanej, musi dokładnie wiedzieć, jakie prawo zostało złamane.

Dokonanie podziału na przestępstwa przeciw własności, przeciw osobom, z użyciem broni, oszukanie władz itd. jest pożyteczne, gdyż pozwala uporządkować nielegalne działania za pomocą podziału na grupy. Dzięki temu staje się możliwe opracowanie ogólnej statystyki, co pozwala organom sprawiedliwości tworzyć oddzielne jednostki przeznaczone do zwalczania przestępstw różnych typów. Ich pracownicy mogą doskonalić umiejętności zwalczania przestępstw należących do wybranych kategorii.

Podobnie pożyteczne byłoby podzielenie cyberprzestępstw na kategorie, by potem je porządkować. Po pierwsze, musimy sobie uświadomić, że cyberprzestępstwa mogą być, zależnie od ich natury, dopasowane do istniejących kategorii określających różne rodzaje przestępstw, na przykład wiele cyberprzestępstw (takich jak sprzeniewierzenie funduszy dokonane za pomocą technologii komputerowej) można zakwalifikować

do „przestępstw urzędniczych”[24], ogólnie zaliczanych do przestępstw bez użycia przemocy, popełnianych podczas wykonywania czynności biznesowych, zwykle (choć nie zawsze) w celu osiągnięcia zysku pieniężnego i często w połączeniu z kradzieżą, oszustwem i defraudacją. Z drugiej strony, uprawiający dziecięcą pornografię w Internecie są zwykle klasyfikowani jako przestępcy seksualni (pedofile) i traktowani jak przestępcy działający (potencjalnie) z użyciem siły.

To krzyżowanie się kategorii i wielkie różnicowanie form utrudnia zakwalifikowanie cyberprzestępstw do jednej własnej, wąskiej kategorii. Jednak większość urzędów i agencji mających do czynienia z cyberprzestępstwami dąży do takiej kategoryzacji, gdyż pomogłaby ona w identyfikacji typów poszukiwanych podejrzanych (charakterystyka kogoś zajmującego się w Internecie pornografią dziecięcą jest inna niż kogoś włamującego się do cudzego systemu komputerowego, a obie te osoby różnią się od trzeciej, która wykorzystuje pocztę elektroniczną do uruchomienia „łańcuszka św. Antoniego”).

Typy cyberprzestępców i ich ogólne charakterystyki omówimy szczegółowo w rozdziale 3. „Zrozumienie tych, którzy są na scenie”.

Tworzenie kategorii cyberprzestępstw

Cyberprzestępstwa możemy podzielić na kategorie na kilka sposobów. Rozpocznijmy od podziału na dwie bardzo obszerne kategorie: przestępstw dokonywanych (lub potencjalnie dokonywanych) przy użyciu przemocy i przestępstw bez przemocy.

Kategorie przestępstw dokonywanych rzeczywiście lub potencjalnie przy użyciu przemocy

Przestępstwa dokonywane za pomocą komputerów lub sieci komputerowych rzeczywiście lub potencjalnie przy użyciu przemocy są z oczywistych przyczyn najważniejsze, bo stanowią fizyczne zagrożenie dla poszczególnych osób lub całych grup. Do cyberprzestępstw z rzeczywistym lub potencjalnym użyciem przemocy zaliczamy:

- cyberterroryzm,
- napaść przez zastraszenie,
- cyberprześladowanie,
- pornografię dziecięcą.

Departament Stanu definiuje terroryzm jako „przemyślane, politycznie umotywowane stosowanie przemocy przez grupy mniejszości narodowych lub tajnych agentów, wymierzone przeciwko celom nieuczestniczącym w walce”. *Cyberterroryzm* to terroryzm dokonywany, planowany i koordynowany w cyberprzestrzeni, tzn. za pomocą komputerów i sieci komputerowych.

[24] White collar crimes — *przyp. tłum.*

Przegląd cyberprawa

Krajowe prawa dotyczące pornografii dziecięcej

W Stanach Zjednoczonych reklamowanie lub świadome korzystanie z pornografii dziecięcej jest uznane za przestępstwo federalne (18 USC 2251 i 2252). Child Pornography Prevention Act (CPPA)[25] z roku 1996 rozszerza pojęcie *pornografii dziecięcej* na każde wizualne przedstawienie czynności jawnie seksualnych, przy produkcji którego nieletnich zaangażowano do wykonywania tychże czynności, nawet jeżeli obraz tylko *sprawia wrażenie* udziału nieletnich w tych czynnościach lub jest reklamowany czy prezentowany jako przedstawiający udział nieletnich w tych czynnościach. Free Speech Coalition[26] zaskarżyła ten przepis jako niekonstytucyjny i federalny sąd apelacyjny zakazał jego stosowania. W październiku 2001 roku Sąd Najwyższy wysłuchał argumentów stron w procesie *Ashcroft przeciw Free Speech Coalition* (Ashcroft v. Free Speech Coalition) dotyczącym niekonstytucyjności CPPA. W kwietniu 2002 roku Sąd Najwyższy orzekł, iż zastrzeżenia USC 2256 zakazujące „wirtualnej pornografii dziecięcej" (generowanych komputerowo obrazów dzieci wykonujących czynności seksualne) są zbyt szerokie i niekonstytucyjne.

W Zjednoczonym Królestwie posiadanie fotografii lub „pseudofotografii" dziecka, którą można uznać za nieprzyzwoitą, jest uznane za przestępstwo kryminalne na mocy Protection of Children Act[27] (1978) i Section 160 Criminal Justice Act[28] (1998). Termin *pseudofotografia* oznacza obraz utworzony komputerowo lub w inny sposób, imitujący fotografię. Zwykle są to obrazy otrzymywane za pomocą manipulacji komputerowych, wykonywanych za pomocą programów graficznych w rodzaju Adobe Photoshop, w wyniku których głowa dziecka jest łączona z innym ciałem (tego samego rodzaju „fotografii wirtualnych dotyczyło orzeczenie Sądu Najwyższego USA z kwietnia 2002 roku).

W większości krajów istnieją ustawy dotyczące pornografii dziecięcej. Synopsis praw narodowych, przygotowany przez Interpol (International Criminal Police Organization)[29], można znaleźć na stronie WWW tej organizacji: „Legislation of Interpol member states on sexual offences against children"[30], pod adresem *http://www.interpol.int/ Public/Children/ SexualAbuse/NationalLaws*.

[25] Ustawa o zapobieganiu pornografii dziecięcej — *przyp. tłum.*

[26] Koalicja wolności słowa. Patrz: http://www.freespeechcoalition.com — *przyp. tłum.*

[27] W wolnym tłumaczeniu: ustawa o ochronie dzieci — *przyp. tłum.*

[28] Prawo karne — *przyp. tłum.*

[29] Międzynarodowa Organizacja Policji Kryminalnych założona w 1923 roku w Wiedniu jako Międzynarodowa Komisja Policji Kryminalnych. Od 1938 roku miała siedzibę w Berlinie. Po drugiej wojnie światowej wznowiła działalność w roku 1946 w siedzibie niedaleko Paryża. Pod obecną nazwą występuje od roku 1956. Polska była członkiem tej organizacji od początku jej istnienia do roku 1952 roku, kiedy to ówczesne władze zerwały z Interpolem wszelkie kontakty. Ponowne przyjęcie Polski do Interpolu nastąpiło w roku 1990. Obecnie do Interpolu należy 177 państw.
Patrz: *http://www.interpol.int — przyp. tłum.*

[30] Ustawodawstwo krajów członkowskich Interpolu dotyczące przestępstw seksualnych przeciwko dzieciom — *przyp. tłum.*

Do tej kategorii zaliczamy używanie e-maili do utrzymywania łączności między konspiratorami oraz dzielenia się informacjami służącymi do przygotowania aktów przemocy, a także używanie serwisów WWW do rekrutacji członków grup terrorystycznych. Można do tej grupy zaliczyć także sabotaż systemów komputerowego sterowania ruchem lotniczym w celu doprowadzenia do zderzeń samolotów lub ich rozbicia, infiltrowanie systemów komputerowych nadzorujących procesy uzdatniania wody pitnej w celu spowodowania jej zatrucia, włamania do szpitalnych baz danych i zmienianie bądź usuwanie danych w celu doprowadzenia do stosowania niewłaściwych procedur medycznych wobec pacjenta lub pacjentów, doprowadzanie do załamań systemów zasilania w energię elektryczną, które może prowadzić do wyłączenia klimatyzacji latem i ogrzewania zimą lub powodować śmierć ludzi podłączonych do respiratorów w prywatnych domach, niewyposażonych w zapasowe agregaty prądotwórcze.

Napaść przez zastraszenie może być dokonana za pomocą e-maila. To cyberprzestępstwo wywołuje u ludzi obawę o własne życie lub życie osób kochanych (przestępstwo to czasami bywa nazywane *groźbą terrorystyczną*). Za przestępstwo tego rodzaju uważa się również przesłanie e-mailem do firmy bądź urzędu groźby podłożenia bomby.

Cyberprześladowanie jest formą elektronicznego nękania, często połączonego z jawnym lub pośrednim wyrażaniem gróźb, które powodują strach ofiary, co może się przerodzić w rzeczywiste grożenie życiu i działanie przy użyciu przemocy.

Pornografia dziecięca ma kilka aspektów, dotyczących ludzi, którzy tworzą materiały pornograficzne z udziałem dzieci, tych, którzy te materiały rozpowszechniają oraz tych, którzy do tych materiałów uzyskują dostęp.

Pornografia dziecięca jest generalnie uznawana za przestępstwo przy użyciu przemocy (brutalne), nawet jeżeli część osób zaangażowanych w jego popełnienie nie miała z dziećmi żadnego kontaktu fizycznego. Przyczyną jest fakt seksualnego wykorzystywania dzieci do produkcji materiałów pornograficznych oraz to, że ludzie interesujący się materiałami tego typu często nie ograniczają się do oglądania zdjęć i snucia fantazji, lecz są praktykującymi pedofilami lub dążą do tego, by nimi zostać.

Z życia wzięte

Relacja detektywa Glena Klinkharta z policyjnego oddziału ds. przestępstw komputerowych w Anchorage

Nie tak dawno zadzwonił do mnie przyjaciel z FBI, mówiąc, że ma zapis z Internet Relay Chat (IRC)[31] i chce na ten temat porozmawiać. Jeden z uczestników dyskusji IRC-owej podał dokładny plan porwania z centrum handlowego i zgwałcenia młodego chłopca. Z treści wynikało, że dotyczyło to jednego z centrów handlowych w naszym mieście. Agent FBI pytał, czy interesuje mnie przeczytanie logów tej sesji IRC-owej i wyrażenie swojej opinii na temat zaistniałej sytuacji.

[31] Usługa internetowa umożliwiająca wymianę informacji w czasie rzeczywistym z kilkoma lub jedną wybraną osobą. Teksty wpisywane z klawiatury korespondujący widzą na ekranach swoich monitorów — *przyp. tłum.*

Gdy agent pojawił się, spojrzałem na zapis czatu i to, co przeczytałem, wprawiło mnie w przerażenie. Z zapisu wynikało, że była to sieciowa pogawędka dwóch osób. Było widoczne, że jeden, nazywany „PITH", przesłał log do FBI, zaś drugi — podejrzany — był znany tylko jako „Kimmo". PITH zachował plik z logiem czatu i poinformował organy sprawiedliwości o zdarzeniu. Zapis ukazywał budzący grozę obraz zdegenerowanego umysłu.

Na ośmiu strona zapisu czatowego został nakreślony ze wszystkimi seksualnymi szczegółami obraz specyficznych metod, jakie zamierzał stosować podejrzany, gwałcąc i torturując swą ofiarę. W dalszej części czatu Kimmo opisywał szczegółowo centrum handlowe, o którym myślał, i ogólnie podawał położenie chaty gdzieś na północ od miasta.

FBI wraz z naszym departamentem od razu zajęło się sprawą. Zdarzyło się, że nad nią pracowało jednocześnie 14 agentów i detektywów policyjnych. Staraliśmy się zlokalizować podejrzanego, podszywając się pod uczestników dyskusji czatowych odbywanych w różnych „pokojach" i szukając Kimmo i jego numeru IP, stosując nakazy rewizji i wezwania sądowe, byle tylko zdobyć informacje mogące doprowadzić do podejrzanego.

Ślady prowadziły do rozwiedzionego ojca mieszkającego na przedmieściu. Agenci rozpoczęli obserwację jego i jego domu. Inni zaczęli grzebać w jego przeszłości i zbierać informacje o metodach działania. Nie miał za sobą żadnej kryminalnej przeszłości, ale był bardzo biegłym użytkownikiem komputerów. Poza tym pasował do wielu szczegółów, które podał w sesji czatowej z PITHEM.

Zdobyliśmy nakazy rewizji jego domu i biura i rozpoczęliśmy przygotowania do przeprowadzenia przeszukania. Pewnego chłodnego poranka weszliśmy do domu i biura. Inna grupa rozpoczęła przesłuchanie podejrzanego.

Podczas konfrontacji podejrzany zachowywał się tak, jakby nie wiedział, o czym mówimy. Zaprzeczył, że coś wie o sesji czatowej PITHA z Kimmo. Gdy przedstawiono mu niepodważalny dowód, łącznie z elektronicznym śladem prowadzącym do jego domowego komputera, przyznał w końcu, że Kimmo to on. Stwierdził, że biorąc udział w tym czacie, był porządnie odurzony. Nigdy nie skrzywdził żadnego dziecka i nigdy by tego nie zrobił.

Jednak jego system komputerowy opowiedział całkiem inną historię. W komputerze i na różnych nośnikach medialnych znaleźliśmy setki obrazów pornografii dziecięcej, łącznie z obrazami dzieci niewolonych i gwałconych. Kimmo znajdował również przyjemność w kolekcjonowaniu setek grafik komputerowych przedstawiających dzieci cięte na plastry, poniżane oraz pokazywane w sposób poruszający, brutalny i krwawy.

Podejrzany został aresztowany. Potem oskarżono go o posiadanie i dystrybucję dziecięcej pornografii. Obecnie odsiaduje swój wyrok w więzieniu federalnym.

Czy był po prostu pijany w czasie czatu z PITHEM? Czy rzeczywiście, tak jak opowiadał, nigdy nie skrzywdził żadnego dziecka? Czy porwałby dzieciaka z centrum handlowego, by potem w odludnej chacie gwałcić go i torturować? Tego zapewne nigdy się nie dowiemy. Możemy być natomiast pewni, że przez kilka najbliższych lat nie będzie miał szansy na realizację swych planów, dzięki ciężkiej pracy wykonanej przez agentów FBI, biuro Prokuratora Stanów Zjednoczonych i grupę naszych detektywów.

Kategorie przestępstw bez użycia przemocy

Większość cyberprzestępstw dokonywana jest bez użycia przemocy, co wynika z faktu, że działanie on-line wyklucza kontakt fizyczny. Anonimowość i „nierzeczywistość" działania są elementami zachęcającymi do popełniania przestępstw w przestrzeni wirtualnej. Przestępstwa bez stosowania przemocy możemy podzielić na kilka podkategorii:

- cyberwtargnięcia,
- cyberkradzieże,
- cyberoszustwa,
- cyberzniszczenia,
- inne cyberprzestępstwa.

Wewnątrz każdej z tych podkategorii można dokonać bardziej szczegółowego podziału.

Cyberwtargnięcia

Cyberwtargnięcie jest przestępstwem polegającym na uzyskaniu przez kryminalistę nieautoryzowanego dostępu do zasobów komputera lub sieci komputerowej, ale bez przestępczego użycia lub zniszczenia danych. Powszechnym przykładem jest włamanie do systemu dokonane przez nastoletniego hakera albo hakerkę, którzy robią to głównie po to, aby pokazać swoje umiejętności rówieśnikom albo udowodnić sobie umiejętność sprostania postawionemu zadaniu.

Z radością uprawiają *snooping*, czyli szpiegowanie i wściubianie nosa w nieswoje sprawy. Czytają cudze e-maile i dokumenty, sprawdzają, jakie programy są zainstalowane w systemie, jakie strony WWW są odwiedzane przez użytkownika, ale nie robią nic ze zdobytymi informacjami. Mimo to cyberwtargnięcia w większości jurysdykcji są uważane za przestępstwa zwykle określane jako „uzyskiwanie nieautoryzowanego dostępu", „złamanie systemu bezpieczeństwa" lub podobnie.

Specjaliści z organów sprawiedliwości muszą znać prawa panujące w ich jurysdykcjach, aby uniknąć automatycznego oddalania skarg dotyczących włamania do sieci tylko dlatego, że ofiara nie jest w stanie wykazać żadnych szkód. Administratorzy sieci muszą mieć świadomość, że zgodnie z przepisami prawa jest to przestępstwo i firma może ścigać intruzów za samo uzyskanie nieautoryzowanego dostępu do sieci lub komputerów. W tym przypadku łatwiej założyć sprawę karną niż cywilną, gdyż ta ostatnia zwykle wymaga udowodnienia, że została wyrządzona szkoda, która może być podstawą żądania odszkodowania.

Cyberkradzież

Jest wiele różnych typów cyberkradzieży, czyli sposobów użycia komputera lub sieci do kradzieży informacji, pieniędzy lub czegoś innego. Cyberkradzieże są przestępstwami najczęściej popełnianymi, gdyż odniesienie korzyści zawsze było motorem nielegalnych działań, zaś kradzież na odległość zmniejsza możliwość wykrycia sprawcy. Oto lista przestępstw, będących odmianami cyberkradzieży.

- *Malwersacja* — polega na przywłaszczeniu sobie pieniędzy lub innej własności powierzonej sprawcy przez kogoś (na przykład malwersację popełnia pracownik, który, korzystając z legalnego dostępu do listy płac, zmienia dane w celu wypłacenia sobie ekstra poborów lub dokonuje nielegalnego przelewu funduszy z konta firmowego na swoje konto prywatne).
- *Nieuprawnione przywłaszczenie* — różni się od malwersacji tym, że przestępcy przywłaszczone walory nigdy nie zostały powierzone, ale uzyskał do nich dostęp z zewnątrz i dokonał przekazania funduszy, modyfikując dokumenty nadające mu prawo własności lub w inny podobny sposób.
- *Szpiegostwo korporacyjne (przemysłowe)* — oznacza, że osoba z firmy lub spoza niej kradnie tajemnice handlowe (na przykład przepis na produkcję konkurencyjnego napoju), dane finansowe, poufną listy klientów, opis strategii marketingowej lub inne informacje, które mogą służyć do sabotowania firmy lub uzyskania przewagi konkurencyjnej.
- *Popełnianie plagiatu* — jest kradzieżą czyjegoś oryginalnego tekstu z intencją opublikowania go jako własnego.
- *Piractwo* — jest nieautoryzowanym kopiowaniem oprogramowania, muzyki, filmów, sztuki, książek itd., co powoduje zmniejszenie dochodów legalnego właściciela praw autorskich (*copywright*).
- *Kradzież tożsamości* — to użycie Internetu w celu otrzymania danych osobistych ofiary, takich jak numer ubezpieczenia społecznego, numer prawa jazdy, w celu ich użycia do popełnienia przestępstwa polegającego na zdobyciu pieniędzy lub własności, użyciu kart kredytowych czy konta bankowego należącego do ofiary.
- *DNS cache poisoning* — jest formą nieautoryzowanego przejęcia pozwalającego intruzom manipulować zawartością pamięci podręcznej (cache) serwerów DNS[32], co pozwala na przekierowanie transmisji sieciowych na własne serwery.

Z życia wzięte

Notatka prasowa Departamentu Stanu USA

W marcu 2002 roku agenci federalni, pod zarzutem kradzieży tożsamości, aresztowali w Jaksonville na Florydzie mężczyznę, który ukradł dane personalne 60 000 pracowników Prudential Insurance Company — firmy, w której poprzednio był zatrudniony jako specjalista IT. Usiłował on za pośrednictwem Internetu sprzedać z ukradzionej bazy danych informacje, które pozwoliłyby na uzyskanie fałszywych kart kredytowych.

Administratorzy sieci powinni zdawać sobie sprawę, że włamania do sieci nie są niewinnymi psikusami, a cyberkradzieże corocznie kosztują firmy miliony dolarów. Pracownicy organów sprawiedliwości muszą zrozumieć, że kradzież niekoniecznie mu-

[32] DNS (Domain Name System — system nazw domenowych) — serwer DNS to program (system) wykonujący automatyczne tłumaczenie nazw domen na adresy IP. Pozwala nadawać komputerom nazwy zrozumiałe dla człowieka i tłumaczy je na numery adresów IP — *przyp. tłum.*

si mieć coś wspólnego z pieniędzmi — kradzione są również dane firmowe, a w większości jurysdykcji istnieją prawa (w kilku przypadkach federalne), które pozwalają na sformułowanie aktów oskarżenia przeciwko tym, którzy kradną „tylko" informacje.

Cyberkradzież jest blisko powiązana z cyberoszustwem i w niekiedy oba te przestępstwa nakładają się na siebie. Jest to widoczne zwłaszcza wtedy, gdy cyberoszustwo jest połączone z przywłaszczeniem pieniędzy lub własności.

Cyberoszustwo

Cyberoszustwo, ogólnie mówiąc, oznacza posługiwanie się kłamstwem w celu osiągnięcia konkretnych wartości lub korzyści. Choć w pewnym sensie można uznać, że jest odmianą kradzieży, oszustwo różni się tym, że ofiara świadomie i dobrowolnie oddaje wartości lub pieniądze przestępcy, ale nie zrobiłaby tego, gdyby nie została przez przestępcę wprowadzona w błąd.

Cyberoszustwo polega na korzystaniu z oszukańczych metod znanych na długo przed pojawieniem się komputerów i sieci komputerowych. Oszust na przykład wysyła e-mail z prośbą o przesłanie pieniędzy na pomoc dla ubogiego dziecka, którego rodzice zginęli w wypadku samochodowym albo obiecuje, że wysłanie niewielkiej kwoty na jego konto wraz z przesłaniem otrzymanego e-maila do 10 znajomych zaowocuje otrzymaniem tysięcy dolarów w ciągu 30 dni. Inne oszustwa polegają na przedstawianiu nieprawdziwych listów polecających ułatwiających uzyskanie zlecenia, które nigdy nie ma być zrealizowane. Po prostu Internet ułatwia i przyspiesza działanie oszustów i daje im dostęp do większej liczby potencjalnych ofiar.

Schematy oszukańczego działania, z wykorzystaniem komputerów lub bez nich, często opierają się na zachłanności lub dobrej woli ofiar. Pracownicy organów sprawiedliwości twierdzą, że często akty oskarżenia przeciw oszustom można sformułować na podstawie praw, które nie mają nic wspólnego z przestępstwami komputerowymi, takich jak ogólne ustawy dotyczące oszustw i kodeksy karny lub handlowy. Oszustwa są często wymierzone w pojedyncze osoby, ale administratorzy sieci muszą być świadomi, że oszuści często biorą za cel firmy, wysyłając prośby o wsparcie dobroczynne lub „schematy szybkiego wzbogacenia się" do instytucji, gdzie mogą liczyć na wielu odbiorców. O otrzymywaniu takiego spamu należy w firmach informować działy IT, które mogą powiadomić o tym odpowiednie władze i jeżeli to nie pomoże, zablokować pocztę napływającą spod adresów oszustów.

Z życia wzięte

Informacja prasowa Departamentu Sprawiedliwości, prokurator USA Emily M. Sweeney

W Miami na Florydzie we wrześniu 2001 pewien mężczyzna został oskarżony o przeprowadzanie fałszywych licytacji za pośrednictwem aukcyjnego serwisu internetowego eBay. Wystawiał na licytację rzadkie karty bejsbolowe i siatkówkowe, pobierał zapłatę i kart nie wysyłał. Na podstawie kodeksu karnego (Title 18 U.S. Code) został oskarżony i skazany na pięć miesięcy więzienia i pięć miesięcy aresztu domowego pod nadzorem elektronicznym.

Cyberoszustwo może przybrać inną formę. Uznajemy za nie każdą modyfikację danych w sieci dokonaną w celu uzyskania nieuprawnionych korzyści (choć w niektórych stanach do przestępstw komputerowych stosuje się specjalne ustawy). Pewnego rodzaju oszustwa dokonuje na przykład uczeń (student), który włamuje się do szkolnej sieci komputerowej, aby zmienić swoje oceny, albo ktoś, kto uzyskuje dostęp do policyjnych baz danych, by usunąć zapis o swoim aresztowaniu lub nałożeniu mandatu za przekroczenie prędkości.

Cyberzniszczenia

Cyberzniszczeniami nazywamy działania, w wyniku których przerywane jest wykonywanie usług sieciowych, a dane są raczej niszczone lub kasowane niż kradzione. Do przestępstw tego rodzaju zaliczamy:

- hakowanie (*hacking*) sieci komputerowych i usuwanie plików danych czy programów,
- hakowanie serwerów internetowych i uszkadzanie czy niszczenie stron WWW,
- wprowadzanie do sieci i komputerów wirusów, robaków i innych złośliwych kodów,
- przeprowadzanie ataków DoS powodujących zablokowanie serwerów i uniemożliwiających legalnym użytkownikom korzystanie z zasobów sieciowych.

Każde z powyższych przestępstw w pewien sposób pozbawia właścicieli i uprawnionych użytkowników możliwości korzystania z danych i (lub) sieci.

Cyberwandalizm to przypadkowe działanie, wykonane „dla zgrywy" przez znudzonych i złośliwych hakerów albo forma komputerowego sabotażu dokonywanego w celu osiągnięcia korzyści (na przykład zniszczenie plików danych konkurenta biznesowego). W niektórych przypadkach cyberwandalizm może być rodzajem osobistej lub politycznej manifestacji (na przykład *cybergraffiti*).

8 stycznia 2002 roku CNN poinformowało, że w latach 2000 – 2001 liczba „zdeformowanych" stron WWW wzrosła ponad pięciokrotnie. Natychmiast po rozbiciu się amerykańskiego samolotu szpiegowskiego w Chinach w roku 2001 rozpętała się tzw. „cyberwojna", podczas której hakerzy chińscy i amerykańscy wielokrotnie nawzajem niszczyli i uszkadzali strony WWW.

Nasilenie cyberwandalizmu wskazuje na konieczność nie tylko utworzenia ogólnego systemu wykrywania włamań sieciowych (IDS — *Intrusion Detection System*), lecz również śledzenia na bieżąco słabych punktów serwerów WWW, poznawania rodzajów przeprowadzanych ataków oraz przygotowywania przez dostawców sprzętu i oprogramowania narzędzi naprawczych, między innymi tzw. „łat" usuwających błędy istniejących systemów. Specjaliści IT muszą mieć świadomość, że starsze otwarte systemy i aplikacje nie były projektowane z myślą o zabezpieczeniach po prostu dlatego, że kiedyś ryzyko nie było tak duże i nie uświadamiano sobie, jak ważne jest stosowanie zabezpieczeń. Z drugiej strony, nowe systemy operacyjne i aplikacje mogą

mieć wiele słabych punktów, o których nikt jeszcze nie wie. Większość dostawców oprogramowania szybko sobie radzi z usuwaniem zagrożeń zaraz po ich wykryciu, ale rzadko się zdarza, aby następowało to przed wykryciem i wykorzystaniem błędów przez hakerów.

W wielu przypadkach cyberwandalizmu przedstawiciele wymiaru sprawiedliwości, aby postawić winnych w stan oskarżenia, potrzebują specjalnych ustaw dotyczących włamań sieciowych, gdyż nie wystarczają do tego stare prawa dotyczące zwykłych aktów wandalizmu.

Wirusy i inne złośliwe kody stanowią wielki problem i są zagrożeniem dla wszystkich komputerów połączonych z Internetem. Nawet wśród specjalistów nie ma zgody w zakresie terminologii stosowanej do opisu złośliwych kodów. *Wirus* komputerowy to program, który, działając, powoduje niechciane i często niszczące efekty. *Robak* to program, który tworzy kopie samego siebie (rozmnaża się). *Trojan* (*koń trojański*) to nieszkodliwy i jawnie działający program, wewnątrz którego został ukryty złośliwy kod; w ten sposób do komputerów są przemycane wirusy i robaki.

Złośliwe kody powodują uszkodzenia systemów komputerowych, których koszty idą w miliony dolarów, a twórcy wirusów są bardzo aktywni, tworzą coraz to nowe wirusy i robaki lub zmieniają stare wersje tak, aby były niewykrywalne dla programów antywirusowych (AV — *Antivirus Software*). Nadejście ery nowoczesnych programów e-mailowych obsługujących *Hypertext Markup Language* (HTML) i pozwalających na przesyłanie załączników (*attachments*) znacznie ułatwiło rozpowszechnianie wirusów. Aby umieścić w systemie złośliwy kod, nie trzeba już włamywać się do sieci — wystarczy przesłać go e-mailem do jakiegoś niezbyt biegłego użytkownika i poczekać, aż rozprzestrzeni się w lokalnej sieci (LAN — *Local Area Network*).

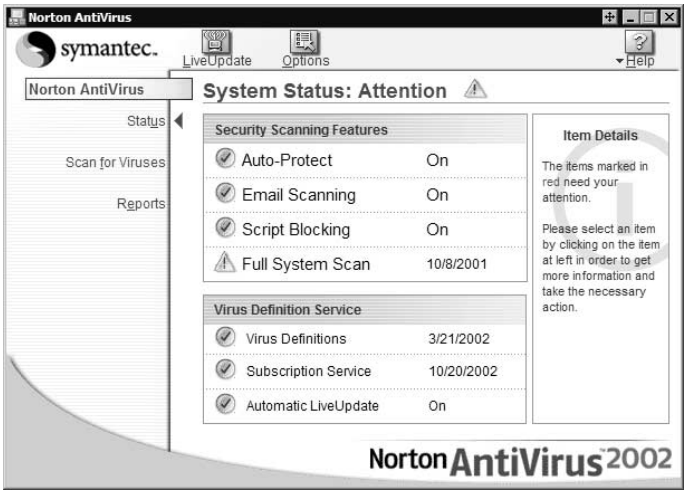
Zakup oprogramowania antywirusowego, sprzedawanego na przykład przez firmy Symantec (Norton AntiVirus został pokazany na rysunku 1.3) i McAfee, powinien być jednym z głównych elementów każdego planu zabezpieczenia sieci. Niezależnie od rodzaju stosowanego oprogramowania antywirusowego zadaniem nader ważnym jest częste uaktualnianie plików definicji wirusów (*virus definition files*), służących do identyfikowania złośliwych kodów i alarmowania w przypadku ich wykrycia.

Wirusy, robaki i konie trojańskie będą omówione szczegółowo w rozdziale 6.

Cyberstatystyka

Koszty powodowane przez złośliwe kody

Kalifornijska organizacja badawcza Computer Economics, doradzająca firmom w dziedzinie technologii, opublikowała raport oceniający światowe szkody spowodowane przez wirusy i inne złośliwe kody w roku 2001 na ponad 13 miliardów dolarów. Pytaniem krytycznym jest dokładność tej oceny, wszak — jak wszystkie inne — bierze ona pod uwagę jedynie przypadki zgłoszone i opiera się na ocenach strat dokonanych przez same poszkodowane firmy. Nie ulega jednak kwestii, że straty wywołane przez wirusy są daleko większe niż sama tylko utrata danych. Zmniejszenie efektywności pracy podczas awarii, utrata dobrej reputacji firmy oraz inne trudno mierzalne czynniki należy także brać pod uwagę (dyskusja i wnioski — patrz: *http://www.computereconomics.com/cei/press/pr92101.html*).



Rysunek 1.3. *Dobry pakiet często aktualizowanego oprogramowania antywirusowego stanowi podstawę pierwszej linii obrony*

Inne cyberprzestępstwa popełniane bez stosowania przemocy

Istnieje wiele cyberprzestępstw popełnianych bez stosowania przemocy. I znów, w wielu z nich Internet jest jedynie narzędziem ubocznym ułatwiającym ich popełnienie, a same przestępstwa nie są niczym nowym, gdyż istniały wcześniej przed powstaniem komputerów (włączając w to najstarszy zawód świata). Oto kilka przykładów:

- reklamowanie prostytucji i stręczycielstwo prowadzone w Internecie,
- internetowe gry hazardowe,
- internetowa sprzedaż narkotyków (nielegalna sprzedaż narkotyków i ich przepisywanie na receptę),
- internetowe pranie brudnych pieniędzy, czyli elektroniczne transferowanie funduszy w celu „uprania" pieniędzy pochodzących z nielegalnych źródeł,
- cyberkontrabanda, czyli nielegalne przesyłanie przez Internet obiektów, których przekazywanie w danej jurysdykcji jest zabronione, na przykład technologii szyfrowania.

Prostytucja jest nielegalna w Stanach Zjednoczonych (z wyjątkiem stanu Newada) i w wielu innych krajach. Ustawy wielu stanów są tak skonstruowane, że oferowanie usług seksualnych w Internecie jest ścigane na mocy prawa. Ponadto, jak twierdzi Mike Godwin z Electronic Frontier Foundation w wywiadzie zatytułowanym „Prostytucja i Internet" (*Prostitution and the Internet — www.bayswan.org/EFF.html*), przestępstwem federalnym jest handel międzystanowy, którego obiektem jest stręczenie „działalności niezgodnej z prawem", a kodeks karny USA (18 USC 1952) określa „prostytucję gwałcącą ustawy stanowe" jako działalność niezgodną z prawem.

Mimo to, zgodnie z publikacją w „E-Commerce Times" z 13 marca 2001, korzystające z najnowszych technologii prostytutki szeroko ogłaszają swe usługi w Internecie, często pod przykrywką „usług towarzyskich". Prostytucja on-line jest często połączona z podobnymi usługami pornograficznymi, które (jeśli nie angażują dzieci) są tak samo jak wolność słowa chronione przez Pierwszą Poprawkę do Konstytucji.

Ciekawym zagadnieniem dla organów sprawiedliwości jest „cyberprostytucja" polegająca na sprzedawaniu za pieniądze seksu wirtualnego. Ponieważ nie występuje tu żaden kontakt fizyczny, taka działalność nie może zostać podciągnięta pod paragrafy większości stanowych ustaw do walki z prostytucją. W roku 1996 Kongres Stanów Zjednoczonych wydał *Communications Decency Act* (CDA)[33], który zakazuje przekazywania przez Internet treści „nieprzyzwoitych" i „ewidentnie przestępczych". Potem w roku 1997 Sąd Najwyższy w sprawie *Reno v. ACLU* uchylił to prawo jako niekonstytucyjne (pogwałcenie wolności słowa z Pierwszej Poprawki). Zawodowi pracownicy wymiaru sprawiedliwości muszą uświadomić sobie, że prawo rządzące działalnością seksualną w sieci zmienia się nieustannie i to, co jest legalne dzisiaj, jutro może stać się nielegalne i vice versa.

Specjaliści sieciowi mają inny problem dotyczący seksu. Umieszczanie w sieci firmowej materiałów o treści seksualnej, nawet jeżeli nie stanowi przestępstwa, może stać się przyczyną procesu cywilnego o nękanie seksualne. Pracodawcy tworzący „nieprzyjazne miejsca pracy" mogą być oskarżeni na mocy Ustawy o Prawach Obywatelskich z roku 1964 (*Title VII of the Civil Rights Act*).

Internetowe gry hazardowe rozkwitły, gdyż pozwalają klientom za pomocą kart kredytowych stawiać on-line zakłady w kasynach internetowych. W lipcu roku 2000 Izba Reprezentantów odrzuciła w głosowaniu propozycje ustawy zakazującej gier hazardowych w Internecie (*Internet Gambling Prohibition Act*). Jednakże rząd federalny oskarża operacje hazardowe w Internecie na podstawie *Interstate Wireline Act*[34] z roku 1961 (18 USC 1084). Ustawa ta zakazuje oferowania zakładów w grach hazardowych za pośrednictwem linii telefonicznych i innych „urządzeń kablowych" (do których zaliczane są również komputery połączone z Internetem) bez specjalnego zezwolenia władz stanowych. Jak w przypadku wielu innych przestępstw internetowych, jurysdykcja jest problemem utrudniającym oskarżanie oferujących gry hazardowe on-line.

Internetowe gry hazardowe to jeszcze jedna dziedzina, w której prawo zmienia się szybko i zależnie od jurysdykcji. Niektóre stany same są zaangażowane w gry hazardowe on-line, sprzedając w Internecie losy na loterie.

Internetowa sprzedaż leków i narkotyków to następny wielki biznes. Prowadzony przez apteki on-line nielegalny handel narkotykami i receptami na nie staje się coraz większym problemem. Wejście Internetu na rynek międzynarodowego nielegalnego handlu narkotykami, na przykład opium, stało się przedmiotem studiów Organizacji Narodów Zjednoczonych i rządów wielu państw. W marcu roku 2000 roku ONZ wydało rezolucję na temat „powstrzymania używania sieci WWW do rozprzestrzeniania handlu narkotykami i ich nadużywania"[35], zachęcającą swych członków do przyjęcia zestawu standardów mających służyć zapobieżeniu lub zmniejszeniu nielegalnej sprzedaży narkotyków w Internecie.

---

[33] Tłumaczone jako „Prawo o przyzwoitości w telekomunikacji" lub jako „Ustawa o dobrych obyczajach w sieci" — *przyp. tłum.*

[34] W wolnym tłumaczeniu: ustawa o międzystanowych liniach telekomunikacyjnych — *przyp. tłum.*

[35] Deterring the use of the World Wide Web for the proliferation of drug trafficking and abuse — *przyp. tłum.*

Przegląd cyberprawa

Gry hazardowe on-line i off-line

W Stanach Zjednoczonych gry hazardowe poza siecią są w niektórych stanach legalne. Niektóre kraje, takie jak Antigua i inne państwa karaibskie, zezwalają i licencjonują operacje hazardowe w Internecie. Niektóre stany wprowadziły ustawy zakazujące gier hazardowych w Internecie. W roku 2000 w południowej Dakocie uchwalono Act to Prohibit the Use of the Internet for Certain Gambling Activities[36], który uznaje prowadzenie gier hazardowych w Internecie za przestępstwo stanowe (spod tych ograniczeń są w Południowej Dakocie wyłączone loterie stanowe i licencjonowane kasyna).

Apteki internetowe sprzedające substancje podlegające kontroli mogą działać legalnie, w sposób bardzo podobny do aptek realizujących zamówienia listowne, podlegając stanowym prawom licencyjnym i sprzedając leki na podstawie recept wystawianych przez lekarzy. Jednakże niektóre apteki działające on-line sprzedają leki tylko na podstawie formularzy wypełnianych przez „pacjentów", potem rzekomo sprawdzanych przez lekarzy, którzy „pacjentów" nigdy nie widzieli i nie sprawdzali ich tożsamości. Spammerzy bombardują skrzynki e-mailowe użytkowników niepożądanymi ogłoszeniami, nagabując do zakupu środków, takich jak Viagra, tabletki na odchudzanie, Prozac, pigułki antykoncepcyjne i inne popularne preparaty sprzedawane na recepty.

W Stanach Zjednoczonych komisja parlamentarna Izby Reprezentantów zaproponowała wprowadzenie Internet Pharmacy Consumer Protection Act[37], ale ustawa przepadła podczas głosowania w Izbie. Niemniej znajdują tu zastosowanie niektóre z już istniejących praw. Controlled Substances Act[38] oraz Food, Drug and Cosmetics Act[39] mogą służyć do oskarżenia przestępców łamiących prawo federalne, a każdy stan ma swoje prawa określające warunki licencjonowania aptek i zasady wystawiania recept i ich realizacji.

Departament Sprawiedliwości, Agencja do spraw Żywności i Leków[40] oraz Federalna Komisja ds. Handlu[41] pilnują razem ścisłego przestrzegania prawa przez firmy sprzedające w Internecie substancje kontrolowane, sprawdzając, by nie sprzedawano leków bez recept lekarskich. Ponadto kilku stanowych prokuratorów generalnych zaskarżyło do sądu apteki działające on-line, aby zapobiec prowadzeniu przez nie takiego procederu w ich stanach. W marcu 2001 władze federalne wspólnie ze stanowymi doprowadziły do zamknięcia apteki mającej swą siedzibę w Oklahomie, która przypuszczalnie nielegalnie sprzedawała on-line leki na receptę. Pracownicy wymiaru sprawiedliwości

[36] W wolnym przekładzie: ustawa zakazująca używania Internetu do prowadzenia pewnych działań hazardowych — *przyp. tłum.*

[37] Ustawa o Ochronie Klientów Aptek Internetowych — *przyp. tłum.*

[38] Ustawa o Substancjach Kontrolowanych — *przyp. tłum.*

[39] W wolnym przekładzie: ustawa o żywności, lekarstwach i kosmetykach — *przyp. tłum.*

[40] Food and Drug Administration (FDA) — *przyp. tłum.*

[41] Federal Trade Commission (FTC) — *przyp. tłum.*

powinni być obeznani z prawami regulującymi sprzedaż leków na receptę, a także sprzedaż i posiadanie nielegalnych narkotyków.

Internetowe pranie brudnych pieniędzy oznacza posługiwanie się Internetem do ukrywania źródeł, z których pochodzą nielegalne środki. Pranie pieniędzy to bardzo stare przestępstwo, ale pewna anonimowość działań w Internecie ułatwia przestępcom lokowanie „brudnych pieniędzy" w legalnych inwestycjach.

Pochodzenie zwrotu *pranie pieniędzy* sięga czasów słynnego chicagowskiego gangstera Ala Capone, który ukrywał swoje nielegalne dochody z hazardu, utrzymując sieć automatów pralniczych działających po wrzuceniu monety.

Omówione wcześniej operacje hazardowe w Internecie są jednym ze sposobów prania pieniędzy, bo przestępcy używają nielegalnie zdobytych pieniędzy w transakcjach hazardowych. Inne możliwości dają przestępcom usługi bankowe on-line, dzięki którym można otworzyć konto bez spotykania się z pracownikiem banku twarzą w twarz. Pieniądze mogą być złożone na tajnym koncie zagranicznym i przesyłane elektronicznie z banku do banku, aż prześledzenie przebytej przez nie drogi stanie się zbyt trudne. Choć przed przestępcami nadal stoi wyzwanie umieszczenia bez budzenia podejrzeń dużych sum w systemie bankowym, ale potem mogą tymi funduszami manipulować o wiele łatwiej i szybciej niż za pomocą stosowanych dzisiaj przekazów elektronicznych.

Cyberkontrabanda dotyczy danych, których legalnie nie wolno posiadać ani przekazywać. Na przykład w Stanach Zjednoczonych *International Traffic in Arms Regulations* (ITAR)[42] zabrania eksportowania do jakiegokolwiek kraju silnego oprogramowania szyfrującego pod karą więzienia i (lub) grzywny w wysokości do miliona dolarów. W roku 1997 sędzia okręgowy (*District Judge*) uznał te przepisy za niekonstytucyjne i niezgodne z Pierwszą Poprawką zapewniającą swobodę wypowiedzi. W roku 2000 administracja Clintona wprowadziła nowe, bardziej liberalne zasady eksportu oprogramowania szyfrującego.

Digital Millenium Copyright Act (DMCA) zabrania rozpowszechniania oprogramowania pozwalającego na obejście cyfrowych zabezpieczeń materiałów chronionych prawami autorskimi. Na jego podstawie w roku 2001 został aresztowany w Las Vegas rosyjski kryptograf Dymitr Sklarow, oskarżony o „nielegalne upowszechnienie" stworzonego przez Adobe programu łamiącego kody zabezpieczające dokumenty zapisane w formacie eBook. Oskarżenie przeciwko niemu zostało cofnięte w zamian za zeznania przeciwko firmie, dla której pracował i która była oskarżona o to samo przestępstwo. Podczas pisania tej książki sprawa toczy się dalej. Był to pierwszy proces wytoczony na mocy tego rozdziału przepisów DMCA i wywołał kontrowersje zwłaszcza z tego powodu, że kwestionowane oprogramowanie jest legalne w Rosji, ojczyźnie Sklarowa. W interpretacji wielu przepisów DMCA występuje wiele niezgodności i różnych interpretacji. Interesujące jest to, że ustawa ta nie zakazuje posiadania, a nawet używania oprogramowania przez końcowych użytkowników, a jedynie przekazywania go innym.

[42] Przepisy dotyczące Międzynarodowego Obrotu Oprogramowaniem Szyfrującym — *przyp. tłum.*

Przegląd cyberprawa

Czynienie oprogramowania nielegalnym

W roku 2002 senator Fritz Hollings przedstawił w Senacie propozycję ustawy zakazującej tworzenia, sprzedaży i rozpowszechniania oprogramowania, które nie spełniałoby zaaprobowanych przez rząd standardów bezpieczeństwa. Specjaliści IT spekulowali, że zatwierdzenie tej ustawy mogłoby uczynić nielegalnym całe oprogramowanie z otwartymi kodami źródłowymi, czyli nielegalnym stałby się na przykład system operacyjny Linux. W obecnym stanie troski o bezpieczeństwo narodowe i skupienia międzynarodowej uwagi na zabezpieczeniach antyterrorystycznych należy się spodziewać kolejnych propozycji ustaw, które uczyniłyby nielegalnymi kolejne programy, a nawet dane.

W Stanach Zjednoczonych większość danych jest obecnie chroniona przez Pierwszą Poprawkę, choć są oczywiste wyjątki, takie jak pornografia dziecięca (omówiona wcześniej w tym rozdziale). Pracownicy organów sprawiedliwości oraz prawodawcy nadal wyczuwają, jaką drogą należy postępować, aby zachować równowagę między wolnością i prawami użytkowników Internetu, a koniecznością chronienia społeczeństwa przed informacjami przynoszącymi szkodę.

Wprowadzanie priorytetów zwalczania cyberprzestępstw

Ponieważ cyberprzestępstwa stają się coraz powszechniejsze, organa sprawiedliwości nie mają wystarczająco dużo czasu na ściganie i formułowanie oskarżeń oddzielnie dla każdego przypadku różnej przestępczej działalności w Internecie. Podzielenie cyberprzestępstw na kategorie o różnym priorytecie ważności ułatwiłoby to zadanie.

Niżej przedstawiamy czynniki, które należy rozważyć przy nadawaniu poszczególnym cyberprzestępstwom różnych priorytetów.

- **Zakres szkodliwości**. Cyberprzestępstwa popełnianie (faktycznie lub potencjalnie) przy użyciu przemocy przeciwko ludziom (a zwłaszcza dzieciom) mają z natury wysoki priorytet. Także przestępstwa przeciw własności powodujące wielkie straty finansowe mają pierwszeństwo przed przestępstwami powodującymi mniejsze straty.
- **Częstość występowania**. Cyberprzestępstwa popełniane częściej od innych wywołują bardziej jednomyślne i lepiej skoordynowane działania niż te, które zdarzają się rzadziej.
- **Dostępność personelu**. Cyberprzestępstwami, do których ścigania wystarczy jeden detektyw, agencje będą się chętniej zajmować po prostu dlatego, że zwykle brakuje pracowników do zajmowania się skomplikowanymi śledztwami, wymagającymi udziału wielu detektywów.
- **Szkolenie personelu**. To, które cyberprzestępstwa są ścigane, a które nie, czasami zależy od tego, w jakich działaniach ścigający zostali przeszkoleni.

- **Jurysdykcja**. Urzędy i agencje generalnie wolą skupiać uwagę na przestępstwach wyrządzanych na szkodę lokalnych obywateli. Nawet jeżeli jest to legalnie możliwe, agencje wolą unikać spraw, w których dochodzi do krzyżowania się różnych jurysdykcji.
- **Trudności w prowadzeniu śledztwa**. Jest to czynnik zbliżony do dwóch poprzednio omówionych. Trudności w prowadzeniu śledztwa i żądza sukcesu zawsze mają znaczenie przy wyborze spraw, którymi należy się zająć w pierwszej kolejności.
- **Czynniki polityczne**. Sprzyjający klimat polityczny ma często wpływ na ustalanie priorytetów wewnątrz agencji. Jeżeli politycy zarządzający agencją są szczególnie zainteresowani jakimś szczególnym rodzajem przestępstw, zajęcie się tymi przestępstwami w pierwszej kolejności jest wielce prawdopodobne.

Jest istotne, aby specjaliści IT, kontaktując się z przedstawicielami prawa w sprawach cyberprzestępstw, rozumieli, w jaki sposób powyższe czynniki mogą wpływać na to, które przestępstwa będą ścigane z większym entuzjazmem, a akty oskarżenia formułowane z większym zapałem.

Walka z cyberprzestępczością

Cyberprzestępstwa, tak samo jak wszystkie inne, można skutecznie zwalczać po ich zrozumieniu. Niezależnie od rodzaju prowadzonej wojny, słuszny pozostaje stary nakaz: przede wszystkim poznaj swego wroga. Tworząc plan zwalczania jakiegoś przestępstwa, należy zacząć od jego zdefiniowania ogólnego i szczególnego. W tym rozdziale podajemy kilka definicji będących podstawą pierwszego kroku — określenia, czym jest cyberprzestępstwo, a czym nie jest.

Następnym ważnym elementem określania strategii zwalczania cyberprzestępstw jest zebranie danych statystycznych w celu przeprowadzenia analizy, poznania wzorców i trendów. Bez wiarygodnych danych statystycznych trudno ustalić zasady efektywnej prewencji i polityki zwalczania występku.

Statystyka jest podstawą następnego kroku, czyli napisania jasno określonych, egzekwowalnych praw odnoszących się do cyberprzestępstw, które nie są objęte prawami już istniejącymi.

W końcu, efektywna walka z przestępczością musi być wspierana przez szkolenie tych wszystkich, którzy z przestępcami walczą oraz tych, którzy przez nich zostali poszkodowani, a więc pracowników służb kryminalnych, specjalistów IT i szeroko pojętego społeczeństwa.

Określenie, kto ma zwalczać cyberprzestępczość

Do walki z cyberprzestępczością nie wystarczy zaangażowanie samej policji. Prawodawcy muszą ustanowić potrzebne prawa. Specjaliści IT i całe społeczeństwo muszą obserwować pojawianie się oznak cyberprzestępstw i zgłaszać takie przypadki władzom, a także zdobywać wiedzę na ten temat, aby nie zostać jedną z ofiar. Pracownicy organów sprawiedliwości muszą przeprowadzać dochodzenie, zbierać dowody i budować niemożliwe do obalenia oskarżenia przeciw cyberprzestępcom. Sędziowie przysięgli muszą te dowody i racje wyważać i sprawiedliwie, w sposób uzasadniony orzekać o winie bądź niewinności. Sądy muszą określać odpowiednie i efektywne kary. Musi także działać odpowiedni system resocjalizacji, pozwalający na skuteczną reedukację cyberprzestępców, którzy mogą nie pasować do ogólnego „profilu przestępcy".

Podstawowym problemem utrudniającym pisanie, przestrzeganie i interpretowanie praw dotyczących cyberprzestępstw jest brak wiedzy technicznej ludzi, którzy mają te zadania wykonywać. Ustawodawcy zwykle nie rozumieją technicznej strony zagadnień i nie wiedzą, co jest pożądane, a nawet w ogóle możliwe. Detektywi policyjni stają się coraz lepiej zorientowani, ale często w niewielkich jurysdykcjach lokalnych zdarza się, że w wydziale nie ma nikogo, kto byłby w stanie rozpoznać cyfrowe dowody mające krytyczne znaczenie.

Z życia wzięte

Oto przykład pokazujący, że przypadek technicznie skomplikowanego cyberprzestępstwa stanowi dla sędziów przysięgłych większe wyzwanie niż proces o morderstwo.

Dla stwierdzenia, czy oskarżony jest winny morderstwa, wystarczy, by naoczny świadek zeznał, że widział, jak wziął pistolet, wymierzył w ofiarę i wystrzelił, dostateczna będzie też opinia eksperta sądowego, który stwierdzi, że na pistolecie znaleziono odciski palców oskarżonego. Oczywiście można kwestionować prawdomówność świadka, a obrońca może dowodzić, że oskarżony trzymał pistolet wcześniej, ale nie użył go do zabicia ofiary, jednakże zasadnicza kwestia nie jest trudna do zrozumienia. Każdy sędzia przysięgły wie, czym jest pistolet i doskonale zdaje sobie sprawę z faktu, że odciski linii papilarnych są unikatowe dla każdego człowieka i ich przypisanie do osoby stanowi dowód sądowy.

Zaś w procesie dotyczącym hakerskiego włamania do sieci komputerowej sędziowie przysięgli mogą usłyszeć zeznanie na temat otwartych portów, wykorzystywania TCP/IP[43] oraz spoofingu[44] IP w celu zamaskowania źródła transmisji w sieci. Te terminy zapewne niewiele powiedzą sędziom, którzy są jedynie użytkownikami komputerów, a główne zagadnienia łączności i bezpieczeństwa sieci nie są tematami łatwymi do wyjaśnienia w krótkim czasie przeznaczonym na zeznania w trakcie procesu. Jeżeli sędziowie przysięgli nie zrozumieją, jak przestępstwo zostało popełnione, trudno im będzie zdecydować, czy oskarżony rzeczywiście je popełnił.

[43] *Transmission Control Protocol/Internet Protocol* — podstawowe protokoły przesyłania danych (pakietów) w sieciach komputerowych. TCP/IP jest podstawą transmisji w internecie — *przyp. tłum.*

[44] Technika przyspieszania pracy niektórych protokołów transmisji lub podszywanie się pod inny komputer w sieci, patrz: *http://www.ssi.civ.pl/data/spoofing.php*. W tym przypadku chodzi oczywiście o drugie znaczenie — *przyp. tłum.*

Budżet może nie pozwalać na wynajęcie wysoko opłacanych ekspertów lub na przykład wysłanie dysku do wyspecjalizowanego centrum odzyskiwania danych (nie mówiąc już o tym, że w obu tych przypadkach może to wywołać uruchomienie procedury sprawdzania autentyczności pochodzenia i ostatecznego nieuznania odzyskanych danych jako dowodu w procesie).

Oskarżyciele często korzystają z możliwości zasięgnięcia rady ekspertów w celu wyjaśnienia zawiłości, ale powinni posiadać przynajmniej podstawową wiedzę pozwalającą na uchwycenie sensu technicznych zagadnień w stopniu pozwalającym na zadawanie tym ekspertom pytań. Gdy przychodzi do oceny zagadnień merytorycznych dotyczących cyberprzestępstw, często przerasta to również możliwości sędziów przysięgłych. Jeżeli członkowie ławy przysięgłych nie posiadają technicznej wiedzy wystarczającej do dokonania samodzielnej oceny wartości dowodów, decyzję o tym, czy popełnienie przestępstwa zostało udowodnione, muszą opierać na często niezgodnych opiniach ekspertów, bez zrozumienia istoty tych wypowiedzi.

Sędziom zawodowym również często brakuje technicznej biegłości, co utrudnia im wykonywanie naczelnego zadania sądu, jakim jest interpretowanie prawa.

Niemożność zrozumienia zagadnień technicznych doskwiera sędziom również wówczas, gdy trzeba wydać wyrok. Usiłując „dopasować karę do przestępstwa", sędziowie wielokrotnie w przypadkach procesów dotyczących cyberprzestępstw uprawiają „radosną twórczość". Zamiast zasądzać kary normalnie przypisane do różnych przestępstw, tzn. więzienie i grzywny, sędziowie orzekają oddanie oskarżonych pod kuratelę lub nakazują „nie używać komputerów i sieci" przez wyznaczony okres. W dzisiejszym świecie, gdzie komputery stają się wszechobecne, ścisłe przestrzeganie takich wyroków spowodowałoby niemożność korzystania przez skazanego z sieci telefonicznej i praktycznie uniemożliwiłoby mu funkcjonowanie i wykonywanie jakiejkolwiek produktywnej pracy.

Pracownikom zakładów penitencjarnych do postępowania z cyberprzestępcami nie jest potrzebna wiedza technologiczna, wyzwaniem dla nich jest rosnąca liczba więźniów innych od typowych dotychczasowych kryminalistów, do których przywykli — pochodzących z nizin społecznych i słabo wyedukowanych. Przestępcy-urzędnicy stanowią dla typowej społeczności więziennej spore zagrożenie, gdyż dostarczanie im specjalnych udogodnień może spowodować skargi różnych polityków i mędrków protestujących przeciw tworzeniu w więzieniach „klubów towarzyskich" i preferencyjnemu traktowaniu pewnych grup. Ta sytuacja może wywołać oskarżenia o praktyki rasistowskie, gdyż większość skazanych za cyberprzestępstwa, to biali — w przeciwieństwie do ogółu więźniów.

Na wszystkie te dylematy jest ta sama odpowiedź: edukacja i programy uświadamiające. Programy muszą obejmować wszystkich, którzy biorą udział w walce z cyberprzestępcami, a są wśród nich:

- prawodawcy i inni politycy,
- pracownicy organów sprawiedliwości,
- specjaliści IT,
- społeczeństwo ogólnie, a społeczność internetowa szczególnie.

Edukowanie walczących z cyberprzestępcami

Efektywna strategia zwalczania cyberprzestępczości wymaga edukowania i trenowania każdego biorącego udział w działaniach prewencyjnych, śledczych oraz mających na celu przygotowywanie raportów i oskarżeń w walce z cyberprzestępcami. Z kryminalnej drogi należy zawracać nawet potencjalnych cyberprzestępców.

Edukowanie prawodawców i pracowników wymiaru sprawiedliwości

Ci, którzy tworzą prawo, wprowadzają je w życie i pilnują jego przestrzegania, rozumieją podstawowe zasady legislacji, prowadzenia śledztw i stawiania w stan oskarżenia. Brakuje im podstawowej znajomości technologii informatycznych, elementarnej wiedzy o tym, jak działa komputer, sieć, co można i czego nie można wykonać za pomocą technologii komputerowej — a co najważniejsze — w jaki sposób komputery i sieci mogą służyć do popełniania przestępstw.

Aby to szkolenie przyniosło najwięcej pożytku, musi być przygotowane specjalnie z myślą o potrzebach audytorium złożonego z ludzi zwalczających przestępczość, a nie być odmianą kursu komputerowego dla informatyków, przedstawionego w innym „opakowaniu". Choć znaczna część informacji może być niezmieniona, należy położyć nacisk na inne zagadnienia i częściowo zmienić zakres. Prowadzącemu śledztwo w sprawie o cyberprzestępstwo nie są potrzebne dokładne informacje o instalowaniu i konfigurowaniu systemu operacyjnego. Powinien natomiast wiedzieć, w jaki sposób haker może użyć domyślnej konfiguracji systemu do uzyskania nieautoryzowanego dostępu.

Szkolenie przeznaczone dla prawodawców powinno im pomóc zrozumieć prawa, jakie tworzą, więc musi różnić się od szkolenia dla detektywów, których głównym zadaniem jest wyszukiwanie cyfrowych dowodów przestępstw. Tym ostatnim powinno się zapewnić szkolenie nie tylko teoretyczne, lecz również praktyczną naukę wyszukiwania i odzyskiwania danych, ich szyfrowania i deszyfrowania, a także odczytywania i interpretowania plików audytu i logów. Oskarżyciele powinni rozumieć znaczenie różnego typu dowodów cyfrowych i wiedzieć, w jaki sposób można je najlepiej zaprezentować na procesie.

Do podstawowych kursów technik śledczych w akademiach policyjnych powinny zostać włączone bloki nauki prowadzenia śledztw dotyczących przestępstw komputerowych. Pracownicy agencji powinni przechodzić bardziej zaawansowane kursy dotyczące tych przestępstw. Powstało wiele bardzo dobrych programów szkoleń komputerowych dla specjalistów sądowych, niestety w wielu rejonach prowadzone są jedynie kosztowne i krótkotrwałe seminaria, których organizację powierza się firmom biznesowym, działającym dla zysku, zaś wewnętrzne kursy policyjne zdarzają się jedynie w agencjach policyjnych w dużych miastach. Szkoli się przede wszystkim detektywów. W niektórych stanach szkolenia dotyczące przestępstw komputerowych zostały włączone do podstawowych kursów policyjnych, a także standardowych programów doszkalania.

W rejonach wiejskich i małych miasteczkach bardzo niewielu pracowników organów sprawiedliwości (a czasem żaden) było szkolonych w zakresie ścigania przestępców komputerowych, choć zaczyna się to powoli zmieniać. Tutaj też szkoli się przede

wszystkim detektywów lub wyższych urzędników, a przecież o przestępstwach zwykle pierwsi informowani są zwykli policjanci z patroli. W jaki sposób mają rozpoznać i zabezpieczyć (a nie nieodwracalnie zniszczyć lub dopuścić do zniszczenia) cenne, cyfrowe dowody przestępstwa.

Byłoby idealnie, gdyby wszyscy pracownicy wymiaru sprawiedliwości przeszli podstawowe szkolenie komputerowe, sieciowe i sądowe. Jednak tego celu nie uda się osiągnąć w najbliższym czasie. Drugim doskonałym rozwiązaniem jest utworzenie i przeszkolenie jednostek oraz zespołów wyspecjalizowanych w dziedzinie przestępstw komputerowych. Gdyby w każdym ciele prawodawczym istniała grupa członków przeszkolonych i skupiających uwagę na zagadnieniach technologicznych, a każdym wydziale policyjnym był wydzielony, odpowiednio przeszkolony i doświadczony oddział, prowadzący dochodzenia w sprawie przestępstw komputerowych, a ponadto w biurze każdego prokuratora okręgowego jeden lub dwóch oskarżycieli byłoby specjalistami od przestępstw komputerowych, bylibyśmy już daleko na drodze do stworzenia efektywnego, skoordynowanego mechanizmu zwalczania cyberprzestępstw.

Przez lata wszystkie instytucje wymiaru sprawiedliwości pozostawały daleko w tyle za innymi resortami w dziedzinie technologii komputerowych. Podczas ostatniej dekady nastąpiło nadrabianie tych zaległości. Agencje federalne, jak na przykład FBI, mają doskonałe możliwości sądowo-komputerowe. Wielkie organizacje policyjne, takie jak IACP i Police Futurists International (PFI)[45], świetnie opanowały nowoczesne technologie i są dla innych agencji doskonałym źródłem zasobów. Departamenty policji w metropoliach i stanowe agencje policyjne zdają sobie sprawę, jak ważna jest umiejętność rozumienia komputerowych technologii, więc utworzyły specjalne oddziały i programy szkoleniowo-treningowe dotyczące przestępstw komputerowych. Ale w Stanach Zjednoczonych i w innych krajach trzeba jeszcze poczekać, by agencje wymiaru sprawiedliwości posiadły umiejętność i biegłość w walce z cyberprzestępcami.

Na razie, z powodu braku doświadczenia, są zmuszone do korzystania ze współpracy z innymi, bardziej zaawansowanymi technologicznie agencjami rządowymi lub korzystania z usług starannie wybranych specjalistów z branży IT. Tą drogą zdobywają doświadczenie potrzebne do realizacji planów zwalczania cyberprzestępczości na ich terenie. Internet sięga do najbardziej oddalonych zakątków kraju i świata. Cyberprzestępstwa nie są wyłączną domeną wielkich miast, a cyberprzestępcy i ich ofiary są wszędzie — we wszystkich jurysdykcjach.

Edukowanie specjalistów technologii informatycznych (IT)

Specjaliści IT już rozumieją sprawy bezpieczeństwa komputerowego i sposoby dokonywania włamań. Należy ich edukować w dziedzinach, takich jak:

[45] Pełna nazwa brzmi The Society of Police Futurists International (w wolnym przekładzie: międzynarodowe stowarzyszenie futurystów policyjnych); jest to organizacja praktyków wymiaru sprawiedliwości, badaczy, ekspertów, szkoleniowców, pracowników agencji detektywistycznych itp., której zadaniem jest ulepszenie i unowocześnienie działania wszelkich instytucji dbających o porządek, bezpieczeństwo i sprawne działanie wymiaru sprawiedliwości. Więcej informacji można znaleźć pod adresem *http://www.policefuturists.org/ — przyp. tłum.*

- **Świadomość przestępstw komputerowych**. Zrozumienie, co jest, a co nie jest złamaniem prawa i różnice między przestępstwami karanymi na podstawie kodeksów cywilnego i karnego, a także zagadnienia dotyczące działania wymiaru sprawiedliwości.
- **Proces tworzenia prawa**. Uświadomienie, w jaki sposób specjaliści IT mogą uczestniczyć w pracach legislacyjnych za pomocą oświadczeń składanych przed komisjami parlamentarnymi oraz dzielenia się doświadczeniem przez dostarczanie ekspertyz i udostępnianie swoich opinii członkom ciał zarządzających.
- **Zasady prowadzenia dochodzeń**. Pokazanie, w jaki sposób specjaliści IT powinni uczestniczyć w prowadzeniu śledztwa, doradzając jako konsultanci policji ofiarom i innym stronom zainteresowanym.
- **Zasady oskarżania**. Nauczenie, w jaki sposób specjaliści IT mogą uczestniczyć w oskarżeniu jako świadkowie — eksperci.
- **Podstawowa teoria i cel prawa karnego i systemu sprawiedliwości**. Nauczenie, w jaki sposób specjaliści IT mogą wesprzeć prawo w walce z cyberprzestępczością.

Sprawą wywołującą kontrowersje jest stosunek wielu specjalistów IT do przedstawicieli prawa i wymiaru sprawiedliwości. Są oczywiście wyjątki, ale wśród znacznej części społeczności informatyków panuje niechęć do rządu i wszelkich oficjalnych osobistości.

Jest wiele przyczyn takiego stanu rzeczy. Biegłość w technologii ma wielką wartość, więc uzdolnieni hakerzy cieszą się szacunkiem nawet wśród zawodowych informatyków. Cały przemysł IT jest młodą dziedziną gospodarki w porównaniu z innymi jej gałęziami i w znacznej mierze nie jest jeszcze prawnie uregulowany. Specjaliści z tej dziedziny obawiają się, że nałożenie zbyt wielu ograniczeń prawnych spowoduje zmniejszenie efektywności pracy i stanie się przyczyną dodatkowych trudności, co przydarzyło się już w innych zawodach. Wielu specjalistów IT nie zna procedur prawnych, a obawa przed nieznanym jest powszechną ludzką cechą. Na koniec, wielu informatyków podpisuje się pod hasłem, że „informacja musi być wolna" i nie zgadza się przynajmniej z częścią praw dotyczących cyberprzestępstw (szczególnie tych, które dotyczą technologii szyfrowania oraz tych, które pogwałcenie praw autorskich do oprogramowania, muzyki i filmów uznają za przestępstwo ścigane na mocy kodeksu karnego)[46].

Tak więc zaangażowanie społeczności specjalistów IT do walki z cyberprzestępczością wymaga przekonania ich, iż regulacje prawne działają na ich korzyść. Nie dokonamy tego, jeżeli nie będziemy umieli pokazać, że prawo jest uczciwe, obiektywnie wprowadzane i egzekwowane, a działania specjalistów spotkają się z rzeczywistym poparciem. Administratorzy sieci i inni specjaliści IT są zwykle ludźmi zajętymi. Jeżeli

[46] Postawa części środowiska informatyków wobec ograniczeń prawnych, zwłaszcza dotyczących praw autorskich, została ciekawie naświetlona w wydanej przez Helion książce Sama Williamsa pt. „W obronie wolności. Krucjata hakera na rzecz wolnego oprogramowania" — *przyp. tłum.*

nawet uwierzą, że cyberprzestępcy powinni być stawiani przed obliczem sprawiedliwości, nie będą chcieli przesyłać informacji o podejrzeniach włamań, ani współpracować z wymiarem sprawiedliwości, jeżeli nie będą mieli zaufania do kompetencji i prawości systemu karnego.

Jednym ze sposobów oswojenia specjalistów IT z systemem prawnym i zasadami procesów jest wciąganie ich do prowadzonych działań. Pracownicy instytucji prawnych powinni na tyle, na ile to możliwe aktywnie zabiegać o pomoc informatyków w walce z cyberprzestępcami i otwarcie stawiać na wyniki ich pracy.

Edukowanie i angażowanie społeczeństwa

Na koniec pozostaje jeszcze sprawa szerokiego edukowania społeczeństwa, a zwłaszcza końcowych użytkowników systemów komputerowych i sieci. To właśnie oni stają się często bezpośrednimi ofiarami cyberprzestępstw. Inni, choćby nie ucierpieli bezpośrednio, również tracą, gdyż ponoszą koszty, gdy zostają zaatakowane firmy, w których pracują, lub jako zwykli podatnicy zmuszeni są corocznie do pokrywania strat spowodowanych przez przestępstwa komputerowe.

Tak jak organizowanie sąsiedzkich grup pilnujących porządku w okolicy przyczynia się do aktywnego włączenia obywateli w walkę z przestępcami, tak programy edukacyjne mogą nauczyć członków wirtualnej społeczności metod chronienia się on-line. Celem tych programów powinno być zapoznanie korzystających z sieci z powszechnymi rodzajami cyberprzestępstw, sposobami rozpoznawania, kiedy istnieje niebezpieczeństwo stania się ofiarą, a także jak należy postępować w wypadku zetknięcia się z cyberprzestępcą. W kilku dziedzinach, takich jak wyłudzenia i oszustwa, edukacja tego typu może przynieść doskonałe rezultaty, znacznie zmniejszając szanse powodzenia cyberprzestępców. W tym celu utworzono specjalne organizacje, na przykład Cyberangels (*www.cyberangels.com*).

Pracownicy wymiaru sprawiedliwości i informatycy powinni bardziej współpracować ze społeczeństwem (z firmami, rodzicami, studentami, nauczycielami, bibliotekarzami i innymi), aby tworzyć zwalczające cyberprzestępstwa grupy, posiadające do tego odpowiednie umiejętności, środki i uprawnienia potrzebne do znacznego zmniejszenia liczby przypadków łamania prawa w Internecie.

Aktywne zwalczanie cyberprzestępczości

Walka z cyberprzestępcami będzie miała największe szanse powodzenia, jeżeli rozpoczniemy działania z różnych stron. Procesy sądowe to tylko jedna z dróg prowadzących do celu. Akcja jest lepsza od reakcji, co oznacza, że lepiej przeciwdziałać, zanim dojdzie do popełnienia przestępstwa. Dlatego teraz omówimy kilka metod, pozwalających pojedynczym osobom i firmom zabezpieczać się w sposób aktywny przed konsekwencjami cyberataków, jeżeli takie nastąpią.

Przeciwdziałanie

Organizacje zwalczające cyberprzestępczość

National Cyber Security Alliance[47] jest wspólną inicjatywą przemysłu i rządu mającą na celu promowanie zagadnień bezpieczeństwa sieci za pomocą działań edukacyjnych i powszechnego uświadamiania zagrożenia cyberprzestępczością. Więcej informacji można znaleźć pod adresem *www.staysafeonline.info*.

National Infrastructure Protection Center (NIPC)[48] zostało utworzone w roku 1998 w siedzibie głównej FBI w Waszyngtonie. Skupia przedstawicieli władz federalnych, stanowych i lokalnych, wojska oraz prywatnego sektora gospodarki w celu ochrony krytycznych zasobów narodowych, w tym również Internetu. Więcej informacji można znaleźć pod adresem *www.nipc.gov*.

Inational Association of Computer Investigative Specialists (IACIS)[49] jest międzynarodową, pozarządową organizacją wolontariuszy pochodzących z lokalnych, stanowych i federalnych organów sprawiedliwości. IACIS zajmuje się szkoleniami (treningami) i edukacją z dziedziny sądowej wiedzy komputerowej. Więcej informacji jest dostępnych pod adresem *http://cops.org*.

Wykorzystywanie nacisku rówieśników do zwalczania cyberprzestępczości

Jednym ze sposobów zwalczania przestępczości w Internecie jest wspieranie grup rówieśniczych, aby wywierały presję na swoich członków. Jeżeli cyberprzestępcy są zawstydzani, a nie podziwiani, stają się mniej skłonni do występku. Ta metoda jest szczególnie skuteczna w odniesieniu do młodych ludzi. Wielu nastoletnich hakerów włamuje się do sieci w celu zaimponowania kolegom[50]. Im większą grupę technologicznie zaawansowanej młodzieży nauczymy zasad komputerowej etyki, kładąc nacisk na to, że poszanowanie cudzej własności w świecie wirtualnym jest tak samo ważne jak w świecie rzeczywistym, tym mniej hakerzy będą przez uczniów i studentów podziwiani, a bardziej traktowani jak łobuzy kradnące samochody i włamujące się do domów.

Zostało stwierdzone ponad wszelką wątpliwość, że zmiana nastawienia grupy rówieśników wpływa na zachowanie poszczególnych osób. W wielkim stopniu społeczne potępienie palących przyczyniło się do znacznego zmniejszenia liczby palaczy w Stanach Zjednoczonych.

Oczywiście ludzie będą nadal popełniali przestępstwa niezależnie od presji wywieranej przez rówieśników, ale taki nacisk ma znaczenie dla tych, którzy poza tym są normalnymi członkami społeczeństwa, a ich przestępcze działania on-line są odbiciem przekonania, że „przecież wszyscy tak robią".

[47] W wolnym tłumaczeniu: narodowy sojusz na rzecz bezpieczeństwa sieci — *przyp. tłum.*

[48] Centrum Ochrony Narodowej Infrastruktury — *przyp. tłum.*

[49] Międzynarodowe Stowarzyszenie Komputerowych Specjalistów Śledczych — *przyp. tłum.*

[50] O motywach działania młodocianych hakerów można się sporo dowiedzieć z wydanej przez wydawnictwo Helion książki Dana Vertona pt. „Pamiętniki hakerów" — *przyp. tłum.*

Z życia wzięte

Jorge Gonzalez, właściciel portalu internetowego Zeropaid.com służącego wymianie plików, rozpoczął innowacyjne działanie mające na celu ukrócenie wymiany plików pornografii dziecięcej za pośrednictwem jego serwisu. W swoim portalu, korzystającym z popularnego programu wymiany plików Gnutella, umieścił wiele fałszywych plików, identyfikowanych jako obrazy pornografii dziecięcej, choć nimi nie były. Użytkownicy pragnący uzyskać do nich dostęp wpadali w pułapkę; ich numery IP, mogące służyć do identyfikacji, były rejestrowane i umieszczane na „ścianie hańby" (która została utworzona przez użytkownika programu Gnutella określającego się jako Lexx Nexus). Jest to taktyka podobna do stosowanej przez pewną gazetę drukującą nazwiska ludzi aresztowanych za jazdę po pijanemu lub prostytucję. Przesłanką takiego działania jest przekonanie, że obawa przed publicznym podaniem nazwiska do wiadomości powstrzyma wielu ludzi przed popełnieniem przestępstwa.

Stosowanie technologii do zwalczania cyberprzestępczości

Zgodnie z zasadą „zwalczania ognia ogniem", jedną z najlepszych broni do zwalczania przestępstw technologicznych jest stosowanie technologii. Firmy zajmujące się bezpieczeństwem komputerów i sieci komputerowych włożyły wiele wysiłku w rozwój sprzętu i oprogramowania, którego zadaniem jest wykrywanie intruzów i obrona przed nimi. Dostawcy systemów operacyjnych wbudowują w nie coraz więcej zabezpieczeń. W styczniu roku 2002 Bill Gates stwierdził, że bezpieczeństwo otrzymało w Microsofcie najwyższy priorytet i zespoły tworzące produkty firmy przeszły dogłębne szkolenia i treningi w tej dziedzinie.

Na rynku znajdziemy wiele różnych zabezpieczeń pochodzących od niezależnych producentów — od biometrycznych systemów identyfikacji użytkowników po programowe „ściany ogniowe" (*firewalls*), mających zabezpieczyć nasze systemy i sieci przed cyberprzestępcami. Pakiety monitorujące i audytowe pozwalają zawodowcom na zbieranie informacji wspomagających śledzenie podejrzanych działań. Wiele tych pakietów posiada „sygnalizatory" alarmujące administratora natychmiast po odnotowaniu próby włamania.

Narzędzia do odzyskiwania danych pomagają pracownikom wymiaru sprawiedliwości zbierać dane, które cyberprzestępcy usiłowali zniszczyć, a policja po uzyskaniu nakazu rewizji może wejść do systemów komputerowych używanych przez przestępców za pomocą tych samych narzędzi, które hakerzy stosują do nielegalnych włamań.

Te zagadnienia technologiczne zostaną dokładnie omówione w rozdziałach 7., 8., 9. i 10.

Znajdowanie nowych zabezpieczeń przed cyberprzestępcami

Nigdy nie uda się zabezpieczyć przed wszystkimi cyberprzestępstwami. Jednak organizacje i poszczególne osoby mogą podejmować wyprzedzające działania mające zminimalizować skutki ewentualnego cyberprzestępstwa.

Na przykład „The Austin Business Journal" w wersji drukowanej z 28 kwietnia 2000 roku informuje, że firmy wykupują polisy ubezpieczeniowe na pokrycie szkód powodowanych przez cyberprzestępstwa. Ponieważ cyberprzestępczość staje się coraz większym problemem, potencjalne ofiary będą szukały nowych sposobów zabezpieczenia się przed stratami finansowymi.

Podsumowanie

Na całym świecie cyberprzestępczość jest wielkim problemem, którego znaczenie wciąż wzrasta. Organy sprawiedliwości szamoczą się z tym problemem; prawodawcy kreują prawa przeznaczone do zwalczania nowych rodzajów przestępstw, a agencje policyjne tworzą specjalne oddziały do zwalczania przestępstw komputerowych i wywierają nacisk na swych oficerów, aby ćwiczyli swą technologiczną biegłość.

Jednak cyberprzestępczość jest zbyt wielkim problemem i zbyt rozprzestrzenionym, aby jego rozwiązanie można było pozostawić politykom i policji. Pierwszym często brakuje znajomości problemów technologicznych, aby byli w stanie tworzyć odpowiednie prawa, zaś drugim — treningu, odpowiedniej liczby ludzi, a także, o czym trzeba wspomnieć, uwolnienia od konfliktów jurysdykcyjnych, niepozwalających na radzenie sobie z najbardziej skandalicznymi przestępstwami internetowymi.

Cyberprzestępstwa, tak jak wszystkie inne, są nie tylko problemem prawnym, lecz także społecznym. Skuteczna walka z nimi wymaga zaangażowania specjalistów IT (a wielu z nich woli trzymać się z daleka) oraz wszystkich tych, których przestępcza działalność, wijąca sobie ciepłe gniazdko w świecie wirtualnym, może wcześniej lub później dotknąć.

Do zwalczania cyberprzestępczości możemy stosować wiele taktyk i technik, wykorzystywać system prawny, presję rówieśników i najnowsze technologie, ale poniesiemy porażkę, jeżeli nie rozwiniemy formalnego i nieformalnego systemu oporu i informowania. Jedynie możliwie najszybsze wykrywanie cyberprzestępstw może przyczynić się do minimalizowania strat, gdyż im więcej będziemy wiedzieli o cyberprzestępstwie, tym większe będą szanse identyfikacji i osądzenia cyberprzestępcy.

Wszyscy płyniemy w jednej łodzi. Tylko wspólne działanie oraz dzielenie się wiedzą i doświadczeniem w różnych dziedzinach pozwoli na utworzenie najwyższej jakości oddziałów zdolnych do powstrzymania cyberprzestępców.

Najczęściej zadawane pytania

Na podane niżej pytania autorzy książki odpowiadają w sposób mający pomóc czytelnikom w ocenie stopnia zrozumienia omawianego materiału oraz w zastosowaniu opisanych koncepcji w praktyce. Jeżeli chcecie zadać autorom jakieś pytania dotyczące tego rozdziału, możecie to zrobić na stronie *http://www.syngress.com/solutions/* po kliknięciu formularza *Ask the Author*.

P: Czy społeczność pracowników wymiaru sprawiedliwości jest przeciwna stosowaniu szyfrowania?

O: Większość specjalistów zajmujących się cyberprzestępczością nie ma nic przeciwko stosowaniu szyfrowania w legalnej wymianie informacji. W oficjalnym stanowisku Departamentu Sprawiedliwości na stronie *www.cybercrime.gov* czytamy: „Nie sprzeciwiamy się stosowaniu szyfrowania — wprost przeciwnie, uważamy je za doskonałe narzędzie ochrony przed przestępcami. Uważamy, że stosowanie szyfrowania silnego jest sprawą krytyczną dla rozwoju „globalnej infrastruktury informatycznej", czyli GII. Zgadzamy się, że komunikowanie się i dane muszą być chronione zarówno podczas przesyłania, jak i przechowywania, jeżeli GII ma być wykorzystywana do komunikacji osobistej, transakcji finansowych, opieki medycznej, tworzenia nowych intelektualnych własności i w inny sposób. Jednak szerokie stosowanie niemożliwych do złamania kodów szyfrujących przez przestępców może stanowić poważne zagrożenie bezpieczeństwa publicznego".

P: Czy piractwo oprogramowania stanowi poważny problem?

O: Ocenia się, że złodziejowi wyszarpującemu torebkę każdy „skok" przynosi od 20 do 30 dolarów, a średni zysk z napadu to około 50 dolarów. Natomiast sprzedaż pirackiej kopii oprogramowania to strata od kilkuset do kilku tysięcy dolarów. Dlatego z ekonomicznego punktu widzenia akt piractwa programistycznego jest kilkakrotnie poważniejszym przestępstwem od kradzieży kieszonkowej lub rabunku.

P: Dlaczego więc wielu ludzi uważa, że piractwo oprogramowania nie jest poważnym przestępstwem?

O: Jest kilka powodów. Piractwo oprogramowania nie łączy się z emocjonalnym starciem twarzą w twarz z przestępcą, jak to ma miejsce w przypadku kradzieży z użyciem siły bądź rabunku. Oprogramowania nie można dotknąć; składa się z bitów elektronicznych danych, inaczej niż jakikolwiek fragment fizycznej własności. Piractwo oprogramowania nie jest kradzieżą w tradycyjnym rozumieniu tego słowa, ponieważ polega na kopiowaniu, więc nie pozbawia właściciela możliwości dalszego używania programu. Wielu ludzi uważa, że warunki licencjonowania oprogramowania są nieuczciwe i dlatego piractwo jest w jakiejś mierze usprawiedliwione. Panuje także powszechne przekonanie, że kopiowanie oprogramowania jest tak powszechne i zdaje się nie czynić żadnych szkód, więc nie jest „prawdziwym przestępstwem" (podobnie wielu ludzi nie uświadamia sobie, że przebieganie przez jezdnię na czerwonym świetle jest przekroczeniem dozwolonej prędkości).

P: Dlaczego systemy i sieci komputerowe nie są w pełni bezpieczne mimo istnienia na rynku tak wielu zabezpieczeń?

O: Mimo istnienia tych wszystkich doskonałych produktów, jedynym idealnie zabezpieczonym komputerem jest komputer wyłączony. Na ćwiczeniach ze strzelania policjantów uczy się używania „bezpiecznych kabur" mających

zabezpieczać przed wyszarpnięciem broni przez przestępcę i użyciem jej przeciwko policjantowi. Naukę zaczyna się od stwierdzenia, że bezpiecznej kabury trudniej używać i należy pilnie ćwiczyć, aby dojść do wprawy w wyciąganiu broni i umieć szybko jej użyć, gdy będzie potrzebna. Jednakże jedyną naprawdę bezpieczną kaburą jest taka, do której pistolet jest na stałe wklejony. Nie będzie mógł go użyć bandyta, ale policjantowi też się na nic nie przyda. Bezpieczeństwo komputerów i sieci jest oparte na zachowaniu takiej samej równowagi między przeciwstawnymi czynnikami, zabezpieczeniem i dostępnością. Im bardziej system jest bezpieczny, tym trudniej dostępny i vice versa. Ponieważ jedną z najważniejszych cech sieci komputerowej musi być jej dostępność, nigdy żadna sieć nie będzie w 100% bezpieczna.

Źródła[51]

- Internet Fraud Compliant Center (IFCC) — raporty statystyczne, *www1.ifccfbi.gov/index.asp*
- Computer Security Institute — „2001 Computer Crime and Security Survey", *www.gocsi.com/prelea/000321.html*[52]
- Cybersnitch Basic Crime Report Statistics, *www.cybersnitch.net/csinfo/csdatabase.asp*
- Meridien Research, *www.meridien-research.com*
- National Cybercrime Training Partnership (NCTP), *www.nctp.org*
- International Association of Chiefs of Police (IACP), *www.iacptechnology.org/2002LEIM.htm*
- Council of Europe Convention on Cybercrime Treaty, *http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185*
- Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Wiedeń, kwiecień 2000 r., *www.uncjin.org/ Documents/congr10/4r3e.pdf*
- Texas Penal Code, Chapter 33, Computer Crimes, *www.capitol.state.tx.us/statutes/pe/pe0003300.html#pe001.33.01*

[51] Ponieważ wszystkie materiały wymienione poniżej są dostępne tylko w wersji angielskiej, pozostawiłem nazwy i tytuły w wersji oryginalnej, co znacznie ułatwia odszukanie informacji w internecie (na przykład po zmianie adresu strony). Przetłumaczyłem jedynie informacje redakcyjne, na przykład daty publikacji — *przyp. tłum.*

[52] Pod tym adresem nie udało mi się znaleźć wymienionego raportu, ale jest dostępny na stronie: *http://www.stealth-iss.com/english/pdf/COMPSECSURVEY1.pdf*

- California Penal Code, Section 502, Computer Crimes, *http://caselaw.lp.findlaw.com/cacodes/pen/484-502.9.html*
- *Cyberterrorism: Fact or Fancy*, Mark M. Pollitt, FBI : Laboratory *www.cs.georgetown.edu/~denning/infosec/pollitt.html*
- National Center for Victims of Crime Cyberstalking *www.ncvc.org/special/cyber_str.html*[53]
- Regulation of Child Pornography on the Internet — strona źródłowa *www.cyber-rights.org/reports/child.htm*
- CNN.com, 8 stycznia 2002 roku: raport: *Cybervandalism Jumped in 2001 www.cnn.com/2002/TECH/internet/01/08/cybervandal.jump.idg/?related*
- E-Commerce Times, 13 marca 2001 roku: *New Economy, Oldest Profession www.ecommercetimes.com/perl/story/8121.html*
- Understanding the Law of Internet Gambling I. Nelson Rose, profesor prawa *www.gamblingandthelaw.com/internet_gambling.html*
- Regulation of Pharmaceuticals Online, Amy Cassner-Sems *www.gase.com/cyberlaw/toppage1.htm*
- EduCause Current Issues: The Digital Millenium Copyright Act *www.educause.edu/issues/dmca.html*

[53] Po wpisaniu tego adresu pojawia się informacja o błędzie, ale wiele informacji na temat nękania sieciowego można znaleźć po wejściu na stronę główną: *http://www.ncvc.org/* i wpisaniu do wyszukiwarki hasła „cyberstalking" — *przyp. tłum.*