AUTOMATYKA • 2007 • Tom 11 • Zeszyt 3

Statystyki odnośnie do włamań i odporności systemów to najgorszy doradca przy wyborze platformy systemowej. Tu potrzebne są zdrowy rozsądek oraz mentalna zdolność do wyjścia poza stereotypy, bajki i mity.

Krawczyk P.: *Niebezpieczne statystyki*.
Computerworld z 10 stycznia 2005 r.

Maciej Szmit*, Izabela Politowska**

Mierniki bezpieczeństwa informatycznego a niektóre przestępstwa komputerowe

1. Wprowadzenie

Mówiąc o bezpieczeństwie systemów informatycznych definiuje się zazwyczaj (por.: [4]) pojęcia:

- zagrożenia – rozumianego jako potencjalna przyczyna szkody,
- podatności – rozumianej jako możliwa do wykorzystania przez zagrożenie słabość chronionego systemu,
- ryzyka – rozumianego jako iloczyn prawdopodobieństwa zajścia nieporządanego zdarzenia (incydentu bezpieczeństwa) i jego negatywnych skutków, czyli mówiąc prościej, jako wartość oczekiwana strat związanych z urzeczywistnieniem się potencjalnego zagrożenia.

Aby zatem móc szacować ryzyko, co jest niezbędną częścią procesu zarządzania bezpieczeństwem, konieczne jest oszacowanie zarówno potencjalnych skutków incydentu, jak i prawdopodobieństwa jego zaistnienia. Mowa tu zarówno o zagrożeniach endo- jak i egzogenicznych, takich jak klęski żywiołowe, niepokoje społeczne czy wreszcie – poziom zagrożeń natury informatycznej (cyberterroryzm, epidemie robaków internetowych[1)] itd.). O ile ryzyko pochodzące z wnętrza firmy czy organizacji udaje się szacować stosounkowo łatwo na podstawie wiedzy dostepnej w organizacji, o tyle ryzyka zewnętrzne, w szczególności związane z zagrożeniami technologicznymi, bywają trudne do oszacowania. Dostępne źródła prezentują zazwyczaj albo skrajny pesymizm (co jest charakterystyczne dla go-

* Katedra Informatyki Stosowanej, Politechnika Łódzka w Łodzi
** Wyższa Szkoła Finansów i Informatyki w Łodzi

1) Według [23] straty poniesione w wyniku epidemii wirusów i robaków internetowych wyniosłóy odpowiednio (w nawiasach rok wystąpienia epidemii): Jerusalem (1990) – ok 50 mln. USD, Concept (1995) – ok. 50 mln USD, Melissa (1993) – ok 93 mln USD, Love Bug (2000) ok. 700 mln USD, Nimda (2001) – ok 531 mln USD.

niących za snesacją mediów), albo – przeciwnie – daleko idącą niefrasobliwość. Rzetelne próby oceny rozmiaru tego rodzaju zjawisk podejmowane są przez niektóre duże firmy i instytucje zajmujące się zabezpieczeniami lub consultingiem informatycznym oraz wyspecjalizowane działy dużych korporacji (na przykład dominujących na rynku providerów Internetu), jakkolwiek jakość tych ocen pozostawia czasami sporo do życzenia. Pewne nadzieje można łączyć z przygotowywaną obecnie przez ISO/IEC serią norm dotyczących systemów zarządzania bezpieczeństwem informacji (*Information Security Management Systems*, ISMS) oznaczonych numerami 27001–27006, wśród których znajdować się będzie norma ISO/IEC 27004 *Information Security Measurements and Metrics*. Norma ta ma pomóc organizacjom posiadających systemy zarządzania bezpieczeństwem informacji w ocenie efektywności ISMS zbudowanych w oparciu o normę [2] (a dokładniej – o jej planowanego następcę – normę ISO/IEC 27002). Pojęcie „zarządzanie" jest tu – podobnie w ogóle w naukach o zarządzaniu – rozumiane w skali mikro: pojedynczego przedsiębiorstwa, organizacji gospodarczej czy też ich systemów informatycznych.

Niniejszy artykuł zawiera przegląd źródeł, które zdaniem autorów, mogą być pomocne w szacowaniu poziomu zagrożeń bezpieczeństwa informacji w skali makro.

2. Definicje

Polska Norma [2] definiuje pojęcie przestępstwa komputerowego jako naruszenie przepisów popełnione w wyniku wykorzystania, modyfikacji lub niszczenia sprzętu komputerowego, oprogramowania lub danych (zob.: [3] s. 24). Z oczywistych powodów definicja taka byłaby nieużyteczna z punktu widzenia prawa. W polskojęzycznej literaturze prawniczej rozróżnia się zazwyczaj przestępstwa komputerowe (przez które rozumie się niektóre z przestępstw przeciwko ochronie informacji – art. od 267 do 269b KK oraz oszustwo komputerowe – art. 287 KK) oraz przestępstwa dokonane przy użyciu komputera, na przykład nagłaśniane w mediach przypadki dystrybucji pornografii dziecięcej czy molestowania seksualnego przy użyciu komunikatorów internetowych (por. np. [32, 34, 42, 44], inne klasyfikacje przestępstw komputerowych można znaleźć na przykład w pracy [41] s. 7 i nast.). Rozważania niniejsze dotyczyć będą wyłącznie zagadnień związanych z niektórymi przestępstwami komputerowymi.

Przyjęcie części z wymienionych wyżej artykułów (art 268a, 269, 269a oraz 269b, a także modyfikacja artykułu 287 §1) stanowiło próbę implementacji Konwencji o cyberprzestępczości Rady Europy [1], podpisanej przez Polskę w dniu 23 listopada 2003 roku. Warto wspomnieć, że już na etapie poprzedzajacym uchwalenie zmian w k.k., a także później proponowane rozwiązania budziły kontrowersje[2)]. Z krytyką spotkało się w szczegól-

---

[2)] W opini prawnej [40] napisano wręcz: „Proponowane rozwiązania prawne odbiegają bowiem znacznie od zaleceń znajdujących się w tekście konwencji. Wprowadzenie niektórych nowych przepisów zdaje się również pogłębiać chaos w treści Kodeksu nie służący oczywiście poprawnej wykładni nowych przepisów" (s. 3). Druga ze zporzadzonych opinii prawnych [39] ogranicza się do stwierdzenia zgodności proponowanych zmian z prawem Unii Europejskiej oraz wyżej wymienioną konwencją Rady Europy pod warunkiem zgłoszenia odpowiednich zastrzeżeń:

ności rozwiązanie proponowane w odniesieniu do tzw. przestępstwa hackingu[3] (pod którym to pojęciem w polskojęzycznej literaturze prawniczej rozumie się zazwyczaj[4] uzyskanie nielegalnego dostępu do danych przechowywanych w systemie informatycznym).

Konsekwencją nienajlepszego tłumaczenia wspomnianej Konwencji – i zapewne nienajlepszej znajomości realiów technicznych wśród prawników i prawodawców – jest używanie w komentarzach, a nawet aktach prawnych terminologii quasi-technicznej, która dla informatyka może wydawać się momentami wręcz śmieszna. I tak hipoteza art 267 §1 kk mówi wręcz o „podłączaniu się do przewodu służącego do przekazywania informacji"[5], choć już w §2 tegoż artykułu mowa o „zakładaniu urządzenia podsłuchowego"[6], co sugeruje, że aby podsłuchiwać należy posłużyć się urządzeniem, natomiast sygnały elektryczne można odbierać bezpośrednio podłączając się do przewodu. Na dodatek wymieniony jest tamże explicite „przewód służący do przekazywania informacji". Wydaje się zatem, że ustawodawca przeoczył istnienie sieci bezprzewodowych.

„Natomiast proponowany nowy przepis art. 269b k.k. ma na celu realizację art. 6 Konwencji, który zobowiązuje do penalizacji produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania oraz posiadania urządzeń (w tym programów komputerowych), haseł komputerowych, kodów dostępu umożliwiających bezprawny dostęp do informacji przechowywanych w systemie informatycznym. Należy zwrócić uwagę, że projekt ustawy nie przewiduje karalności samego posiadania takich urządzeń. Przepis art. 6 ust. 3 konwencji zezwala na takie ograniczenie, pod warunkiem złożenia przez Państwo stosownego zastrzeżenia." [39]. W artykule [34] przedstawione zostały liczne zastrzeżenia miedzy innymi odnośnie do użytych w projekcie ustawy (a wynikających z nienajlepszego tłumaczenia oryginalnego tekstu konwencji) pojęć „danych informatycznych".

3) „Projekt nowelizacji nie usuwa podstawowego błędu, jaki popełniany jest w polskim prawie karny w zakresie penalizacji przestępstwa tzw. hackingu, czyli uzyskania nielegalnego dostępu do danych przechowywanych w systemie informatycznym. (...) Rozwiązanie to – w oczywisty sposób zakorzenione w historii polskiego prawa karnego – jest wzorowane na przepisie Art. 172 Kodeksu karnego z 1969 r., nie uwzględniając faktu, że uzyskanie dostępu do informacji (czyli wedle polskiego orzecznictwa możliwość zapoznania się z treścią) jest zapewne celem osoby otwierającej cudze listy, ale wcale nie jest głównym celem się hackera. Tzw. „czysty hacking" zakłada, że dla osoby dokonującej włamania do systemu nie jest ważna sama informacja, którą może uzyskać. Ważne jest jedynie przełamanie zabezpieczenia. To zaś wciąż nie jest w Polsce karalne. Przełamanie zabezpieczenia jest jedynie środkiem, który może – a nie musi – prowadzić do dokonania przestępstwa opisanego w art. 267 § 1 (inną sprawą jest trudność udowodnienia hackerowi, że zapoznał się ze skopiowanymi danymi). Tymczasem same włamania do systemów – powodujące konkretne straty dla administratorów i właścicieli systemów – są czynem na tyle szkodliwym, że penalizacji niewątpliwie wymagają" [40] s. 5

4) Na przykład w cytowanej powyżej opinii [40], jakkolwiek już w artykule [34] mówi się o „programach hakerskich" w odniesieniu do programów, o których mowa w artykule 269b k.k.

5) Art. 267. § 1. k.k. „Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

6) Art. 267. § 2. k.k. „Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym".

Co do kwestii „przełamywania zabezpieczeń" to stała się ona również przedmiotem dyskusji, niektórzy Autorzy próbują bowiem przeciwstawić „przełamywaniu" – „obchodzenie" zabezpieczeń (por. np. [7] oraz [46]). O ile w przypadku zabezpieczeń fizycznych ma to pewien sens (czy innym jest kradzież z włamaniem od przywłaszczenia sobie rzeczy niezbezpieczonej, być może celowo publicznie dostępnej[7)]), o tyle w przypadku technik informatycznych sprawa jest wątpliwa. Karalne byłoby bowiem, na przykład – jako próba „siłowa" włamanie do serwera przy wykorzystaniu słownikowego generatora haseł, natomiast niekaralne – wykorzystanie luki w zabezpieczeniach przy pomocy exploita, o ile ten nie unieruchomiłby programu zabezpieczającego, a jedynie otworzył tylne drzwi do systemu, jeśli otworzyłby je w sposób inny, niż wyłączając na chwilę tegoż systemu działanie. Kolejnym zagadnieniem jest sformułowanie art 269b penalizującego, między innymi, wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie urządzeń i programów komputerowych przystosowanych do popełnienia określonych przestępstw (między innymi mowa o urządzeniach podsłuchowych, wizualnych albo innych urządzeniach specjalnych a także hasłach komputerowych, kodach dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej). Liczni autorzy (por. np. [35, 45]) słusznie zauważają, że artykuł ten jest co najmniej kontrowersyjny, narzędzia tego typu (na przykład monitory ruchu sieciowego jak WireShark czy Etheral) są bowiem standardowo używane przez administratorów sieci czy pracowników serwisu. Część prawników (por. np. [46]) uważa, że w myśl tego artykułu karalne powinny być czynności przygotowawcze do popełnienia przestępstw (to znaczy osoby uprawnione mogłyby legalnie tego rodzaju programy, hasła, kody i urządzenia wytwarzać, pozyskiwać, zbywać i udostępniać), jakkolwiek problemem pozostałoby niedookreślenie kręgu osób uprawnionych. Wydaje się, że znacznie lepszym pomysłem byłoby jawne określenie przez prawodawcę warunków na jakich byłyby to czynności niekaralne. Stosunkowo interesująco wyglądają tu na przykład przepisy kodeksu karnego Republiki Białoruś [5], karzące przygotowanie w celu sprzedaży i sprzedaż specjalnych środków umożliwiających otrzymanie bezprawnego dostępu do systemu komputerowego lub sieci oraz przygotowywanie złośliwego oprogramowania[8)]. W polskim Kodeksie karnym [4] nie wprowadzono pojęcia złośli-

---

7) Jakkolwiek praktyka polskiego wymiaru sprawiedliwości zna przypadek orzeczenia kary za pobranie z publicznie dostępnego serwera www pliku muzycznego i zapisanie go płycie. Zob: [46].

8) „Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети — наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами — наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, – наказываются лишением свободы на срок от трех до десяти лет."

wego oprogramowania, co może powodować podobne jak powyżej wątpliwości, o ile bowiem przygotowywanie, a tym bardziej rozpowszechnianie, wirusów czy rootkitów należy ocenić jako jednoznacznie szkodliwe, o tyle już posługiwanie się monitorami ruchu sieciowego jest normalną czynnością administratora sieci, a ich wytwarzaniem zajmują się właściwie wszyscy producenci systemów operacyjnych[9)].

Podobnych zastrzeżeń można wymienić więcej, jakkolwiek należy pozytywnie należy ocenić sam fakt, że Polska jest jednym z zaledwie 28 krajów, które dotychczas (kwiecień 2007) podpisały (ale nie ratyfikowały) konwencję. Ratyfikowało ją zaledwie 15 krajów [8]. Samo istnienie odpowiednich przepisów prawa karnego materialnego pozwala bowiem przede wszystkim na ściganie przynajmniej niektórych przestępstw, zaś jego ewentualne niedoskonałości mogą być – przynajmniej w jakiejś mierze – korygowne przez sądy, do dyspozycji których pozostaje cała gama środków poczynając od umorzenia sprawy aż do odstąpienia od kary.

3. Statystyki sądowe i policyjne

Niezależnie od oceny jakości obowiązującego prawa interesujące mogą okazać się statystyki związane z jego egzekwowaniem. Istnieją trzy źródła, z których można takie statystyki uzyskać: Komenda Główna Policji [9] (statystyki dotyczące wykrytych przestępstw), Ministerstwo Sprawiedliwości (statystyki dotyczace osądzeń [11]) oraz Służba Więzienna (statystyki dotyczące osób odbywających kary [10]). W ramach prowadzonych badań uzyskano szczegółowe statystyki z dwóch pierwszych źródeł, ponieważ liczba osób odbywających kary pozbawienia wolności z artykułów dotyczacych przestępstw komputerowych jest znikoma albo żadna[10)].

Z przyjętego dla potrzeb niniejszego artykułu punktu widzenia sposób prowadzenia statystyk wymiaru sprawiedliwości należy ocenić jako archaiczny i mający wątpliwą wartość badawczą[11)]. Przyjęty sposób naliczania statystyk (chronologicznie zamiast według sygnatur akt) nie umożliwia otrzymania rzeczywistego obrazu sytuacji. Dla przykładu, ze statystyk policyjnych [9] można dowiedzieć się na przykład, że w latach 2003–2005 stwierdzono popełnienie pięciu przestępstw z art 269 k.k. (niszczenie danych informatycznych). Ze statystyk Ministerstwa Sprawiedliwości. że w latach 2003–2005 ogółem osądzono z tegoż artykułu 10 osób i tyleż osób skazano. W oparciu o istniejące dane statystyczne

---

9) Na przykład Network Monitor wbudowany w system Windows czy tcpdump w systemach z rodziny linux.

10) Łącznie z przestępstw przeciwko ochronie informacji (art.265–269 k.k.) w 2006 karę pozbawienia wolności odbywało 14 osób, przy czym przestępstwa przeciwko ochronie informacji obejmują również ujawnienie tajemnicy państwowej (art. 265) służbowej i zawodowej (art. 266) oraz naruszenie tajemnicy korespondencji w odniesieniu do nieelektronicznych postaci informacji.

11) Znacznie lepiej wygladają na przykład statystyki przestępstw komputerowych niemieckiej policji kryminalnej [31] choć, niestety nie są one na bieżąco aktualizowane.

nie sposób stwierdzić jak zakończyły się sprawy przestępstw wykrytych przez Policję. Możliwych jest wiele sytuacji np. niewykrycie sprawcy, zwrócenie przez sąd aktu oskarżenia prokuratorowi celem jego uzupełnienia, umożenie postępowania sądowego (np z powodu śmierci podejrzanego) czy zmiana kwalifikacji czynu przez sąd. Może być również tak, że procesy ciągle jeszcze trwają. Wydaje się, że czytelny obraz sytuacji powinien obejmować informację o tym w jakim procencie popełnionych przestępstw udało się doprowadzić do skazania sprawcy (lub sprawców), w jakim – nie udało się go schwytać, w jakim – podejrzany okazął się niewinny itd. Niestety chronologiczny układ danych pozwala jedynie na obliczenie wątpliwej wartości wskaźnika liczba prawomocnie skazanych w stosunku do liczby przestępstw popełnionych. Na rysunku 1 przedstawiono wykresy stwierdzonych przestępstw i osób prawomocnie skazanych w kolejnych latach (wg przestepstwa głównego[12)]).

Dla porównania, oprócz przestępstw komputerowych zestawiono dane dla art. 196 k.k. (obraza uczuć religijnych), art. 290 k.k. (kradzież leśna), art 278 (kradzież) i art 197 (zgwałcenie). W tabeli 1 zebrano wskaźnik powstały przez podzielenie liczby prawomocnie skazanych przez liczbę przestępstw popełnionych (sumarycznie dla lat 1999–2005)[13)].

Biorąc pod uwagę, że w odniesieniu do artykułów 269a i 269b mamy do czynienia ze znikomo małą liczbą przypadków i będąc świadomym ryzyka stosowania tego rodzaju wskaźników, można jednak uznać za w pewnym stopniu symptomatyczne, że wyniki 13% dla art 278 i 18% dla art. 267 są istotnie mniejsze niż ponad czterdziestoprocentowe wartości dla zgwałcenia czy kradzieży leśnej. Może to świadczyć o trudnościach z ustaleniem sprawcy przestępstwa bądź z dowiedzieniem mu winy[14)].

Odczucie takie wydaje się być uzasadnione, jeśli weźmie się pod uwagę rzeczywistą liczbę aktów agresji, których doznaje codzinnie każdy użytkownik Internetu. Według danych [12] średni czas, jaki obecnie mija od momentu podłączenia niezabezpieczonego komputera do sieci publicznej do momentu jego zainfekowania złośliwym oprogramowaniem, wynosi mniej niż jedną minutę.

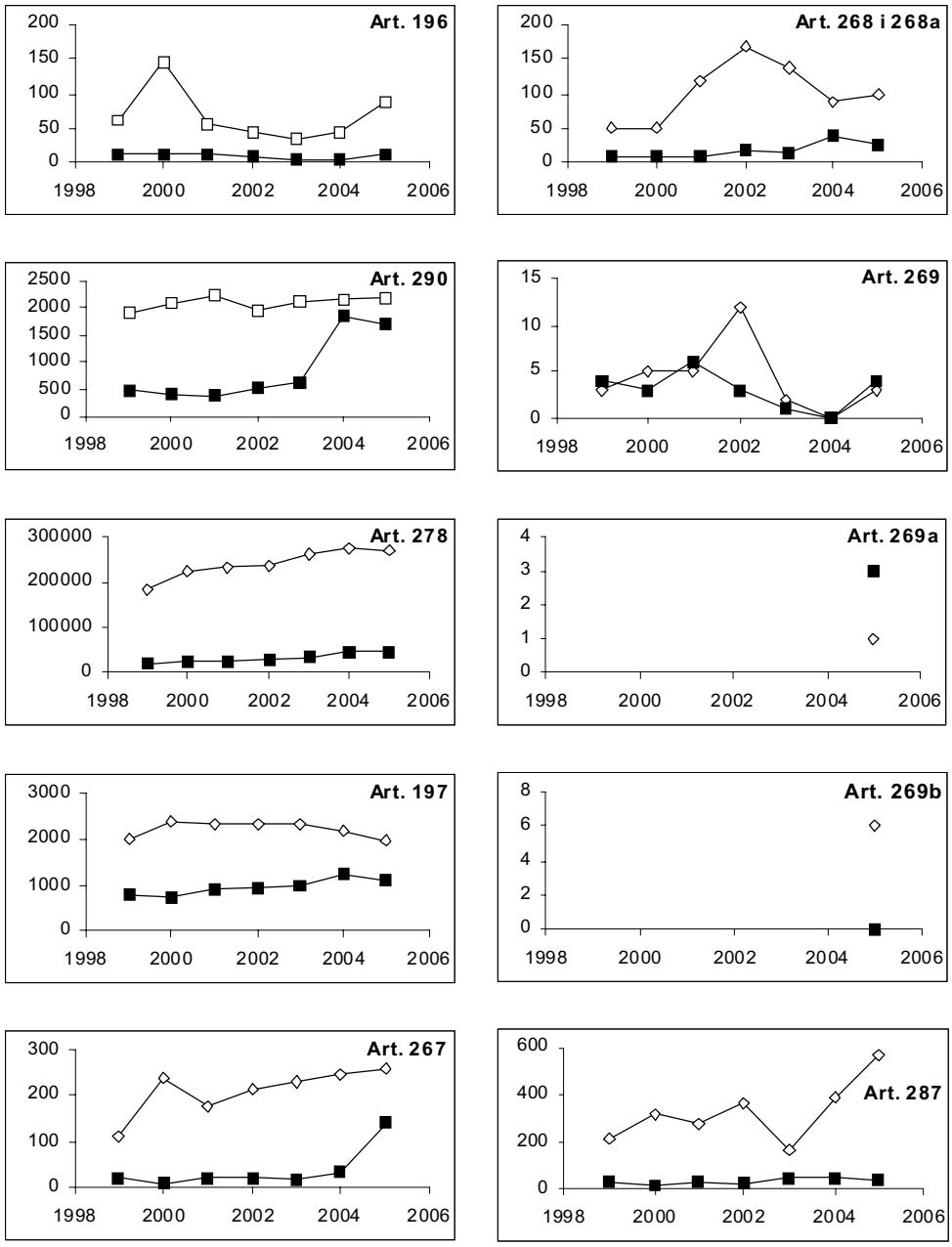
Można zatem zaryzykować twierdzenie, że w obecnym stanie prawnym (w którym większość przestępstw komputerowych ściganych jest na wniosek pokrzywdzonych, a nie z urzędu) i wobec niewielkiego (w stosunku do liczby stwierdzonych przestępstw) procentu skazań, przytłaczająca większość przestępstw komputerowych pozostaje bezkarna bądź niewykryta.

---

12) Oznacza to, że jeśli skazany został uznany winnym w ramach tego samego procesu przestępstwa poważniejszego (powodującego wyższą karę) to przestepstwo „lżejsze" nie jest ujęte w tej statystyce. Jakkolwiek jest to pewne ograniczenie, można jak się wydaje, uznać że przestępstwa komputerowe stosunkowo rzadko łączą się z przestępstwami poważniejszymi.

13) W przypadkach artykułów wprowadzonych po roku 1999 wskaźnik obliczono od momentu obowiązywania artykułu.

14) Należy zwrócić dodatkowo uwagę, że liczba osób osądzonych nie przekłada się w prosty sposób na liczbę przypadków, bowiem sprawców mogło być kilku, nie zmienia to jednak wyciągniętego wniosku, jeśli bowiem taki przypadek zaistniał, to wartość obliczonego ilorazu może być co najwyżej za wysoka.



Rys. 1. Liczba stwierdzonych przestępstw i liczba skazanych z powołanych artykułów k.k. w latach 1998–2005
(Źródło: tab. 1)

Tabela 1
Statystyki przestępstw komputerowych w Polsce w porównaniu z wybranymi innymi rodzajami przestępstw
(Źródło: opracowanie własne na podstawie [9] i [11])

Artykuł	287	269b	269a	269	267	197	278	290	196
Przestępstwa popełnione wg [9]	1686540	6	1	30	1483	15597	2313	14633	468
Skazani wg czynu głównego wg [11]	224341	0	3	21	263	6761	239	5969	61
Iloraz [%]*	13	0	300%	70%	18%	43%	10%	41%	13%

* Przestępstwa popełnione/Skazani wg czynu głównego.

4. Statystyki zespołów reagowania

Za kwestie związane z obsługą incydentów bezpieczeństwa w sieciach komputerowych odpowiadają zespoły CERT (*Computer Emergency Readiness Team lub Computer Emergency Response Team*)[15]. W szczególności za obsługę incydentów bezpieczeństwa odpowiadają zespoły CSIRT (*Computer Security Incident Response Team*). Zespoły takie tworzone są przez instytucje zarządzające dużymi sieciami komputerowymi w celu obsługi incydentów bezpieczeństwa oraz świadczenia pomocy użytkownikom (zasady tworzenia zespołów CERT precyzuje dokument [6]). Zespoły takie prowadzą często, między innymi, statystyki incydentów. Oprócz zespołów CERT istnieją wyspecjalizowane instytucje bądź zespoły mające za zadanie monitorowanie bezpieczeństwa sieci[16] i innych aspektów bez-

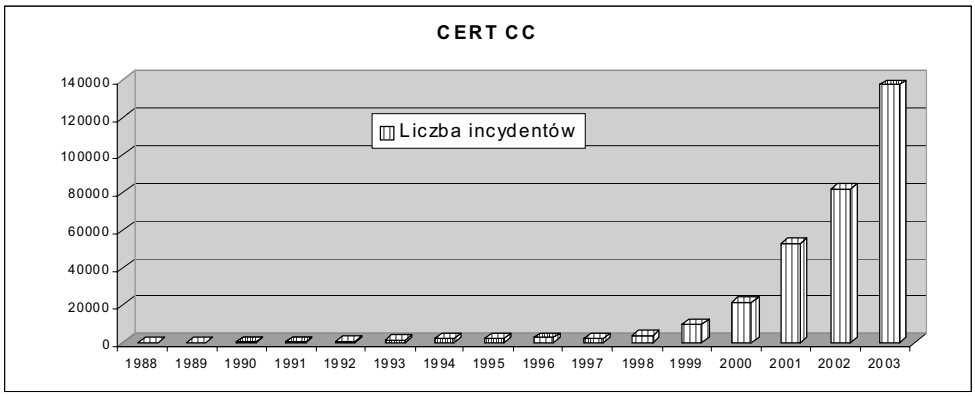
[15] Nazwy CERT and CERT Coordination Center są zastrzeżone w U.S. Patent and Trademark Office.

[16] W szczególności należy tu wymienić raporty The National White Collar Crime Center (NW3C) wykonywane wspólnie z the Federal Bureau of Investigation (FBI) w ramach porozumienia the Internet Crime Complaint Center [13] oraz analogiczny raport za rok 2005.

pieczeństwa. Z krajowych inicjatyw warto wymienić zespół dyżurnet (National Initiative for Children Polska) poświęcony problematyce zwalczania nielegalnych treści w Internecie (w szczególności pornografii dziecięcej) [26].

Zespół CERT Polska [19] działa w ramach Naukowej i Akademickiej Sieci Komputerowej (zob [24]). Zespoły CERT[17)] współpracują ze sobą w ramach FIRST (*Forum of Incidents Response and Security Teams* [22]), przy czym przynależność do FIRST nie jest dla CERT obowiązkowa. W chwili obecnej FIRST zrzesza 184 zespoły o charakterze zarówno ogólnokrajowym, jak CERT Polska, jak i firm komercyjnych (członkami FIRST są na przykład zespoły obslugi incydentów firm Apple, Oracle czy Deutsche Bank).

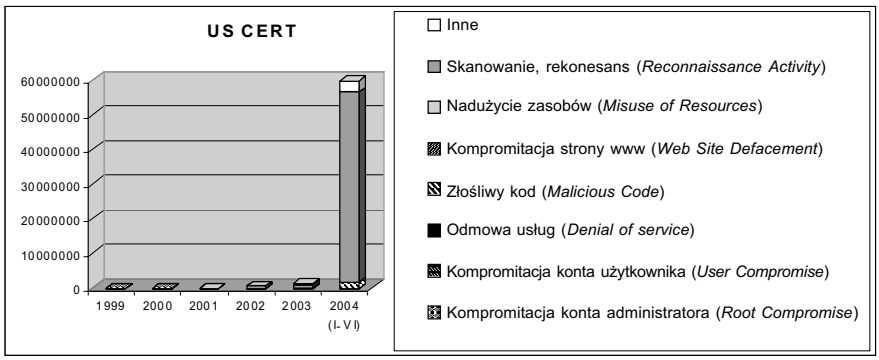
Część zespołów CERT udostępnia informacje na temat statystyk incydentów bezpieczeństwa w sieciach, nad którymi sprawują opiekę, przy czym nie ma jednolitego standardu klasyfikacji i opisu tego rodzaju zjawisk. Pewną popularność zdobywa klasyfikacja Common Language (zob [37]) używana między innymi od 2001 roku przez CERT Polska[18)]. Na rysunkach (2–9) i w tabelach (2–9) przedstawiono statystyki zebrane ze stron CERT Coordination Center oraz wybranych zespołów CERT/CSIRT (wszystkich zespołów krajowych lub zespołów obsługi incydentów w dużych sieciach o zasięgu krajowym zrzeszonych w FIRST, które takie statystyki publikują).



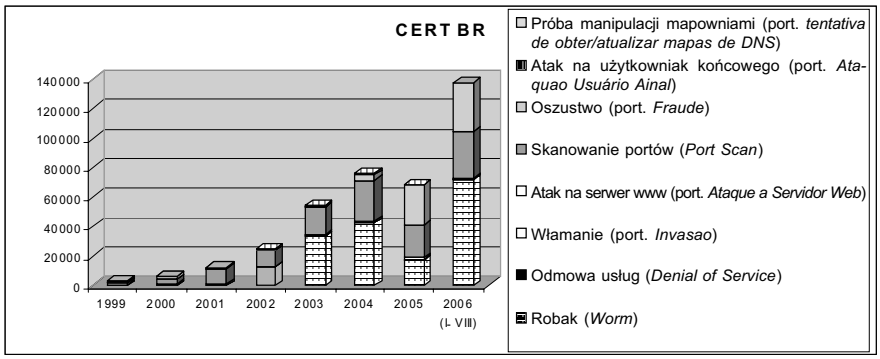
Rys. 2. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT CC
(Źródło: tab. 2)

17) Adres [14] należy do CERT Coordination Center działającego przy wsparciu rządu federalnego USA w Software Engineering Institute na Carnegie Mellon University.

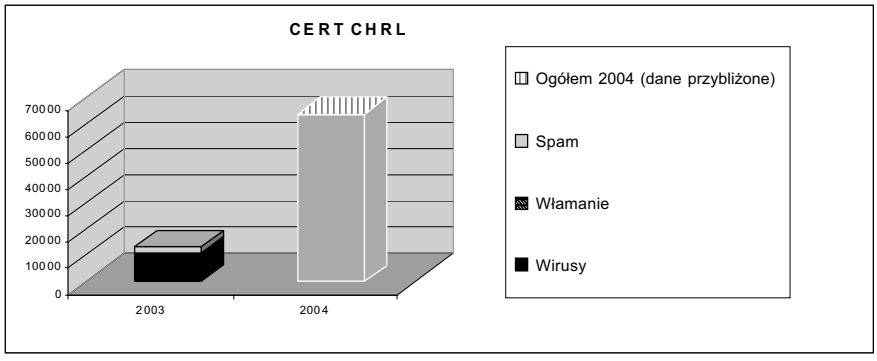
18) Inne próby standaryzacji nomenklatury z zakresu bezpieczeństwa zawierają na przykład dokument [25] czy praca [38]. Należy zwrócić uwagę, że różne klasyfikacje (a także ich tłumaczenia na język polski) są czasami daleko rozbieżne a nawet sprzeczne. Dlatego też w zamieszczonych dalej tabelach statystyk incydentów różnch zespołów CERT, wszędzie tam gdzie tłumaczenie mogło budzić wątpliwości, zamieszczone zostały również nazwy ataków oryginalnie użyte w raporcie (w języku angielskim lub w języku narodowym).



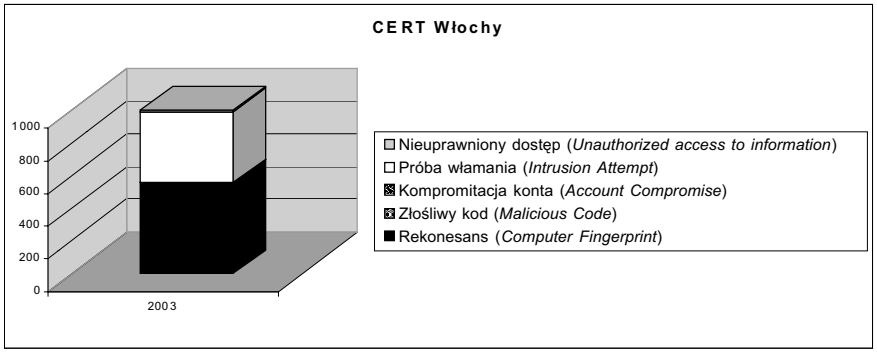
Rys. 3. Statystyki incydentów bezpieczeństwa zgłoszonych do US CERT
(Źródło: tab. 3)



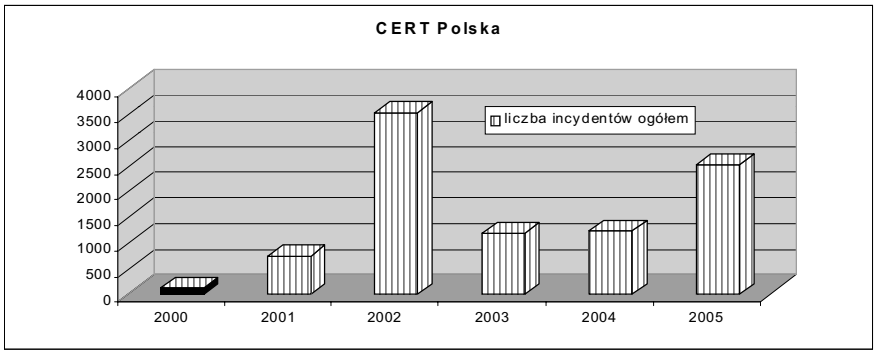
Rys. 4. Statystyki incydentów bezpieczeństwa zgłoszonych CERT BR
(Źródło: tab. 4)



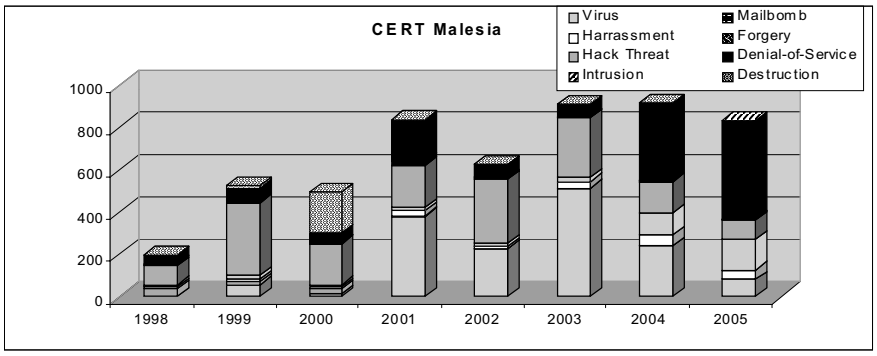
Rys. 5. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT ChRL
(Źródło: tab. 5)



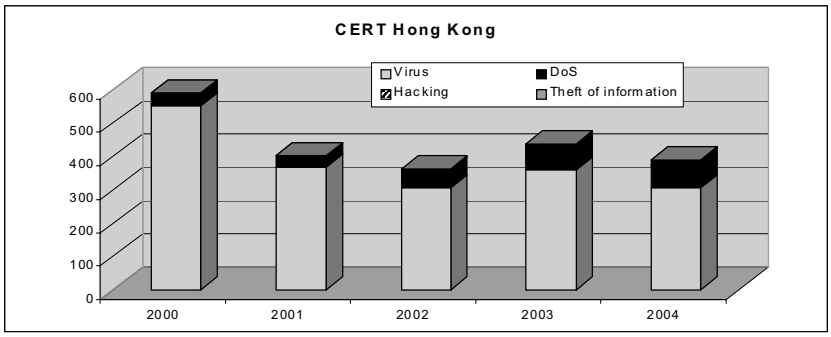
Rys. 6. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT Italy
(Źródło: tab. 6)



Rys. 7. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT Polska
(Źródło: tab. 7)



Rys. 8. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT Malezja
(Źródło: tab. 8)



Rys. 9. Statystyki incydentów bezpieczeństwa zgłoszonych do CERT Hong Kong
(Źródło: tab. 9)

Tabela 2
Statystyki incydentów bezpieczeństwa zgłoszonych
do Computer Emergency Readiness Team Coordination Center
(Źródło: [14])

Rok	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Liczba incydentów	6	132	252	406	773	1334	2340	2412	2573	2134	3734	9859	21756	52658	82094	137529

Tabela 3
Statystyki incydentów bezpieczeństwa zgłoszonych do US Computer Emergency Readiness Team
(Źródło: [20])

Rok	1999	2000	2001	2002	2003	2004
Kompromitacja konta administratora (*Root Compromise*)	113	157	101	125	137	73
Kompromitacja konta użytkownika (*User Compromise*)	21	115	127	111	587	183
Odmowa usług (*Denial of Service*)	34	36	760	36	25	435
Złośliwy kod (*Malicious Code*)	0	0	4764	265	191306	1559989
Kompromitacja strony www (*Web Site Defacement*)	0	0	236	46	90	28
Nadużycie zasobów (*Misuse of Resources*)	12	24	7	39	26	35
Skanowanie, rekonesans (*Reconnaissance Activity*)	222	71	452	488000	706441	54867634
Łącznie	454	412	6555	489890	1433916	59156555

Tabela 4
Statystyki incydentów bezpieczeństwa zgłoszonych do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
(Źródło: [15])

Rok	1999	2000	2001	2002	2003	2004	2005	2006 I-VIII
Robak (*worm*)	n.n.	n.n.	n.n.	12395	33415	42267	17332	71438
Odmowa usług (*Denial of Service*)	21	159	80	62	50	104	96	272
Włamanie (port. *invasão*)	128	127	143	140	120	248	448	451
Atak na serwer www (port. *Ataque a servidor Web*)	183	415	448	241	516	524	570	336
Skanowanie portów	1268	3538	10797	10996	18986	28158	22197	31448
Oszustwo (port. *fraude*)	4	18	43	99	593	4015	27292	33564
Atak na użytkownika końcowego (port. *Ataque ao usuário final*)	658	1540	780	1159	927	406	65	n.n.

n.n. – nie notowano

Tabela 5
Statystyki incydentów bezpieczeństwa zgłoszonych do National Computer Network Emergency Response Technical Team Coordiantion Center of China w 2003 roku
(Źródło: [16])

Wirusy	220
Włamanie	10893
Spam	2201
Łącznie	13314

Tabela 6
Statystyki incydentów bezpieczeństwa zgłoszonych
do Computer Emergency Response Team Italy w 2003 roku
(Źródło: [21])

Computer fingerprint	554
Malicious Code	3
Account Compromise	2
Intrusion Attempt	435
Unauthorized access to information	3
Łącznie	997

Tabela 7
Statystyki incydentów bezpieczeństwa zgłoszonych do CERT Polska
(Źródło: [19])

Rok	2000	2001	2002	2003	2004	2005
Liczba incydentów ogółem	126	741	3531	1196	1222	2516

Tabela 8
Statystyki incydentów bezpieczeństwa
zgłoszonych do CERT Malezja
(Źródło: [18])

	1998	1999	2000	2001	2002	2003	2004	2005
Virus	4	54	16	379	225	514	242	82
Mailbomb	32	18	20	5	1	1	2	
Harrassment	11	11	16	24	11	27	47	43
Forgery	6	17	3	10	16	28	106	149
Hack Threat	95	343	195	204	301	276	145	87
Denial-of-Service	10	10	3	19	11	5	5	7
Intrusion	37	63	48	198	60	60	368	467
Destruction	1	11	195	0	0	0	0	
Razem	196	527	496	839	625	911	915	835

Tabela 9
Statystyki incydentów bezpieczeństwa
zgłoszonych do CERT Hong Kong
(Źródło: [17])

	2000	2001	2002	2003	2004
Virus	551	370	307	357	305
DoS	7	0	19	22	69
Hacking	30	30	33	53	16
Theft of information	0	1	4	3	0
Razem	588	401	363	435	390

Statystyki zespołów CERT nie mogą być – jak zresztą zastrzegają same zespoły traktowane jako chronologiczny zapis aktywności agresorów, tym bardziej że prowadzona w taki czy inny sposób klasyfikacja zmusza zespoły CERT do przypisywania poszczególnych, niejednokrotnie złożonych – to jest wykorzystujących różne techniki – ataków, do jednej z wymienionych grup. W szczególności pojedyczy incydent bezpieczeństwa może dotyczyć zarówno jednej maszyny, jak i całej grupy obejmującej setki, czy nawet tysiące komputerów. Ponadto notowane są zazwyczaj tylko te incydenty, które zespoły CERT bezpośrednio zidentyfikowały i – mimo to – nie można mieć pewności, czy incydenty zostały poprawnie zakwalifikowane. Niemniej podane liczby mogą dawać pewne wyobrażenie, jeśli nie o bezwzględnej aktywności agresorów, to przynajmniej o jej dynamice (i dynamice zaangażowania zespołów CERT w obsługę incydentów) i preferowanych sposobach agresji. Rzucającym się w oczy spostrzeżeniem, które nasuwa się podczas analizy liczby zgłaszanych incydentów, jest stała tendencja wzrostowa. Wyjątki dotyczą zazwyczaj pojedynczych lat. Nietypowy jest tu jedynie Hong Kong, w którym liczba incydentów spada systematycznie Również porównanie liczby incydentów zgłoszonych do poszczególnych zespołów CERT ze statystykami przestępstw jest symptomatyczne (w samym tylko roku 2005 CERT Polska odnotował 2516 zgłoszeń incydentów, czyli więcej niż Policja wykryła przestępstw ze wszystkich artykułów „komputerowych" przez ostatnie pięć lat).

5. Wskaźniki syntetyczne

Oprócz statystyk udostępnianych czy to przez wymiar sprawiedliwości, czy też przez zespoły reagowania na incydenty można znaleźć wiele syntetycznych wskaźników aktualnego poziom bezpieczeństwa. Zazwyczaj operują one na kilkustopniowej skali opisującej ryzyko infomatyczne czy sieciowe, są dostępne on-line i aktualizowane na bieżąco, tak aby każdy użytkownik sieci w każdej chwili mógł sprawdzić aktualny poziom zagrożenia.

Wśród tych wskaźników można wymienić m.in.:

– Security Alert Level Enterprise State of Services przygotowany przez administrację stanową stan Alaska operujący na pięciostopniowej skali zagrożenia („zielony", „niebieski", „zółty", „pomarańczowy", „czerwony") [28].

- Current Internet Threat Level przygotowany przez przez IBM ISS [12] operujący na czterostopniowej skali zagrożenia („zielony", „niebieski", „żółty", „czerwony") https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp.
- Symantec Thread Con przygotowany przez firmę Symantec operujący na czterostopniowej skali zagrożenia („zielony", „żółty", „pomarańczowy", „czerwony") [29].
- CA Security Advisor Alert Level przygotowany przez firmę CA operujący na sześciostopniowej skali zagrożenia („szary", „błękitny", „żółty", „pomarańczowy", „czerwony") [30].
- Virus Alert firmy Kaspersky Lab [33].

Oczywistą wadą tychże wskaźników jest ich wielość oraz – przynajmniej w wypadku niektórych – brak jasnych kryteriów ustalania aktualnego poziomu zagrożenia.

6. Wnioski

Niejednorodność i wielość mierników i metryk dotyczących poziomu bezpieczeństwa informacji[19)], zarówno w mikro- jak i makroskali, jak również brak jednolitych (w skali świata) i dopracowanych (w realiach Polski) rozwiązań legislacyjnych powoduje, ze obecnie jest trudno rzetelnie oszacować rozmiar zagrożeń związanych z poszczególnymi rodzajami przestępczości komputerowej (por. [43]). W praktyce przyjmuje się zatem jedną z dwóch skrajności – albo uznaje się, że ryzyko jest niewielkie albo wręcz żadne (co prowadzi w krótszym bądź dłuższym czasie do kompromitacji systemu) albo – przeciwnie – że poziom zagrożenia jest bardzo wysoki, co powoduje konieczność wdrożenia wielostopniowych – i kosztownych – mechanizmów obrony (zapory przeciwogniowe, systemy wykrywania i przeciwdziałania włamanion, programy antywirusowe etc.). Oczywiście z tych dwóch wyjść w mikroskali zdecydowanie lepsze jest to ostatnie (mniej niebezpieczne jest zastosowanie zbyt dobrej ochrony niż zbyt słabej). W skali makro tego rodzaju rozumowanie nie jest prawidłowe, może bowiem prowadzić do nadmiernej represyjności prawa. Wydaje się, że z taką sytuacją już w jakiejś mierze mamy do czynienia w odniesieniu do nadmiernej ochrony autorskich praw majątkowych[20)].

Powstaje pytanie: czy polepszenie jakości statystyk miałoby jakikolwiek wpływ na praktyczną stronę zarządznia bezpieczeństwem? Niezależnie przecież od tego, czy ulubionym rodzajem ataku internetowych oszustów będzie np. DNS-spoofing czy phishing i tak

---

19) W niniejszym artykule nie ujęto licznych raportów bezpieczeństwa informacji (wyszukiwarka Google na zapytanie „ 'information security' report" zwraca ponad milion dwieście tysięcy stron, zaś na zapytanie „'information security' statistic" – ponad milion. Stan z maja 2007 r.). Takiej ilości informacji nie da się w rozsądnym czasie nie tylko przeanalizować ale nawet zapoznać się z nią. Tym bardziej wskazane wydaje się opracowanie jakichś standardów w tym zakresie.

20) Warto w tym miejscu przywołać świeży (kwiecień 2007) przypadek akcji policyjnej przeprowadzonej – bez wezwania przez władze uczelni. Działanie to spotkało się z krytyką Senatu Politechniki Koszalińskiej jako przeprowadzone z naruszeniem obowiązującego prawa (art. 4 ust. 1 i art. 227 ust. 3 Ustawy Prawo o Szkolnictwie Wyższym) [27].

należy w zabezpieczanym systemie zbudować mechanizmy obrony zarówno przed jednym, jak i przed drugim zagrożeniem. Niewątpliwie jest to poważny argument. Niemniej jednak wydaje się, że – nie tylko ze względów poznawczych – odpowiedniej jakości mierniki agresji informatycznej w skali makro byłyby bardzo przydatne. Nasuwającymi się instytucjami, dla których informacja taka byłaby użyteczna jest oczywiście wymiar sprawiedliwości, aparat ścigania czy ośrodki naukowe i dydaktyczne. Również firmy komercyjne mogą być zainteresowane tego rodzaju statystykami, zarządzanie ryzykiem zakłada bowiem zasadę redukowania bądź unikania w pierwszym rzędzie największych ryzyk, zatem znajomość skali zagrożenia ze strony poszczególnych czynników jest nie bez znaczenia.

Literatura

Przepisy prawne i normy

[1] Convention on Cybercrime, Concil of Europe, Budapest, 23.XI.2001, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm tekst polskojęzyczny (tłumaczenie robocze): http://www.ms.gov.pl/ue/ue3in32.shtml
[2] Polska Norma PN-ISO/IEC 17799:2007: *Technika informatyczna. Techniki Bezpieczeństwa. Praktyczne zasady zarzadzania bezpieczeństwem informacji.* Warszawa, PKN 2007
[3] Polska Norma PN-ISO/IEC 2382-1:1996: *Technika informatyczna Terminologia Terminy podstawowe.* Warszawa, PKN 1996
[4] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny - Dz. U. z 1997 r., Nr 88, poz. 553 z późn. zm
[5] Уголовный кодекс Республики Беларусь http://www.levonevski.net/pravo/kodeksy/uk/031.html

Portale, witryny www i dokumenty elektroniczne[21)]

[6] Brownlee N., Guttman E., „ Expectations for Computer Security Incident Response", The Internet Society, 1998 (RFC 2350, BCP 0021) ftp://ftp.rfc-editor.org/in-notes/rfc2350.txt
[7] Prawa nowych technologii http://www.prawnik.net.pl/pwi/faqhack.htm
[8] Strona Rady Europy o ratyfikacjach Konwencji o Cyberprzestępczości http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=9/26/2006&CL=ENG
[9] Informacje statystyczne na serwerze Komendy Głównej Policji http://www.policja.pl/portal/pol/2/1239/
[10] Informacje statystyczne w portalu Służby Więziennej http://www.sw.gov.pl/index.php/statystyki
[11] Informacje statystyczne na serwerze Ministerstwa Sprawiedliwości http://www.ms.gov.pl/statystyki/statystyki.shtml
[12] IBM Internet Security Systems – strona główna http://www.iss.net/
[13] Internet Crime Report 2006, the NW3C and the FBI, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf
[14] Computer Emergency Readiness Team Coordination Center CERT CC http://www.cert.org
[15] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil http://www.cert.br
[16] National Computer Network Emergency Response Technical Team Coordiantion Center of China http://www.cert.org.cn
[17] Cert Hong Kong https://www.hkcert.org

[21)] Wszystkie adresy www i ftp zostały sprawdzone 15 maja 2007 r.

[18] CERT Malezja http://www.mycert.org.my
[19] Computer Emergency Readiness Team Polska http://www.cert.pl
[20] United States Computer Emergency Readiness Team http://www.us-cert.gov/
[21] Computer Emergency Readiness Team Italy http://security.dico.unimi.it
[22] Forum of Incidents Response and Security Teams FIRST http://www.first.org
[23] ICSA http://www.icsalabs.com ICSA Labs
[24] NASK Naukowa i Akademicka Sieć Komputerowa http://www.nask.pl
[25] Shirey R., „Internet Security Glossary (RFC 2828)", The Internet Society, 2000, ftp://ftp.rfc-editor.org/in-notes/rfc2828.txt
[26] National Initiative for Children Polska http://www.dyzurnet.pl/
[27] Stanowisko Senatu Politechniki Koszalińskiej z dnia 18 kwietnia 2007 r. w sprawie wkroczenia policji do domów studenckich PK i przeszukania pomieszczeń http://www.tu.koszalin.pl/open.php?menu=b&file=s-s-pk_070418
[28] Security Alert Level Enterprise State of Services przygotowany przez administrację stanową stan Alaska http://state.ak.us/admin/info/security/ThreatIndicatorSOA.shtml
[29] Symantec Thread Con http://www.symantec.com/index.jsp
[30] CA Security Advisor Alert Level http://www.ca.com/us/securityadvisor/virusinfo/collateral.aspx?cid=56855
[31] Statystyki Przestępstw Komputerowych Niemieckiej Policji Kryminalnej http://md.hudora.de/stats/PKS/
[32] Wikipiedia hasło „Przestępczość komputerowa" http://pl.wikipedia.org/wiki/Przest%C4%99pczo%C5%9B%C4%87_komputerowa
[33] Kaspersky Lab http://www.kaspersky.com
[34] Piotr Waglowski „Historia oceni rok po wycieku „Precious"" http://prawo.vagla.pl/node/6496

Publikacje

[35] Adamski A.: *Cyberprzestępczość – aspekty prawne i kryminologiczne.* Studia Prawnicze, Zeszyt 4/2005, 59–61
[36] Bukowski S.: *Projekt zmian Kodeksu karnego – Dostosowanie do Konwencji o cyberprzestępczości.* Gazeta Sądowa, kwiecień 2004, http://www.prawo.lex.pl/czasopisma/gs/pzmiankk.html
[37] Howard J.D., Longstaff T.A.: *A Common Language for Computer Security Incidents.* Sandia National Laboratories, 1998 http://www.cert.org/research/taxonomy_988667.pdf#search=%22%22Common%20Language%22%20security%22
[38] Lindqvist U., Jonsson E.: *How to Systematically Classify Computer Security Intrusions.* Departament of Computer Engineering Chalmers University of Technology, 1996
[39] Pawłowski B.: *Opinia prawna o zgodności przedstawionego przez Radę Ministrów projektu ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (druk nr 2031) z „prawem europejskim".* http://orka.sejm.gov.pl/rexdomk4.nsf/Opwsdr?OpenForm&2031
[40] Płachta M.: *Opinia w sprawie projektu ustawy o zmianie Kodeksu karnego, Kodeksu postępowania karnego oraz Kodeksu wykroczeń.* Gdańsk, 12 stycznia 2004 r. (druk sejmowy nr 2031). http://orka.sejm.gov.pl/rexdomk4.nsf/Opwsdr?OpenForm&2031
[41] Płaza A.: *Przestępstwa komputerowe.* Praca magisterska napisana na Wydziale Prawa i Administracji UMCS pod opieką prof. dra hab. Zbigniewa Ćwiąkalskiego, maszynopis http://vagla.pl/skrypts/mgr_a_plaza.pdf
[42] Politowska I., Szmit M.: *Prawne aspekty bezpieczeństwa informacji przechowywanych i przesyłanych w systemach i sieciach informatycznych.* [w:] Boston IT Security Review Nr 2/2007, 20–23
[43] Siluszek A.: *Przestępstwa komputerowe.* PC Kurier 2000/8/42 http://www.pckurier.pl/archiwum/artykuly/siluszek_andrzej/2000_08_42/

[44] Warylewski J.: *Przestępstwo oszustwa komputerowego (art. 287 k.k.) – podstawowe zagadnienia teoretycznoprawne i praktyczne.* http://panda.bg.univ.gda.pl/%7Ewaryl/ok.htm
[45] Wróblewski W.R.: *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych.* [w:] Bezpieczeństwo sieci komputerowych a haking. Materiały z konferencji naukowej Lublin 4–5 marca 2005 r. Wyd. UMCS, Lublin 2005
[46] Zoll A. (red.), Wróbel W.: *Kodeks karny. Część szczególna. Komentarz, T. II.* Zakamycze 2006, 1311–1314