CERT Polska

Raport 2007

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2007

1 Wstęp

1.1 Informacje dotyczące zespołu CERT Polska

CERT Polska (Computer Emergency Response Team Polska – http://www.cert.pl/) jest zespołem, działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (http://www.nask.pl/), zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. CERT Polska działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams - http://www.first.org/) - największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENA TF-CSIRT (http://www.terena.nl/tech/task-forces/tf-csirt/) i działającej przy tej inicjatywie organizacji Trusted Introducer[1] (http://www.ti.terena.nl/). W ramach tych organizacji współpracuje z podobnymi zespołami na całym świecie zarówno w działalności operacyjnej jak też badawczo wdrożeniowej.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń;
- współpraca z innymi zespołami IRT (Incidents Response Team) – m.in. w ramach FIRST i TERENA TF-CSIRT;
- prowadzenie działań informacyjno-edukacyjnych, zmierzających do wzrostu świadomości na temat bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie http://www.cert.pl/, organizacja cyklicznej konferencji SECURE);
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu;
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego;
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;

[1] Od 2001 r. zespół CERT Polska posiada najwyższy poziom zaufania Trusted Introducer Accredited Team.

2 Statystyki CERT Polska

Zgodnie z założeniami programowymi wymienionymi na wstępie, CERT Polska co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych[2], które zostały zgłoszone do naszego zespołu. Zespół prowadzi także prace w dziedzinie tworzenia wzorców rejestracji i obsługi przypadków naruszenia bezpieczeństwa teleinformatycznego (zwanych dalej incydentami), a także wzorców klasyfikacji incydentów oraz tworzenia statystyk.

Jednym z ważniejszych celów tych prac jest wypracowanie i stałe korzystanie z tego samego sposobu klasyfikowania incydentów, co umożliwi porównywanie danych, zarówno w kolejnych latach, jak i różnic pomiędzy naszymi obserwacjami i obserwacjami innych zespołów reagujących. W tym roku po raz piąty z kolei przygotowaliśmy statystyki zgodnie z klasyfikacją wypracowaną w ramach projektu eCSIRT.net (http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7).

3 Statystyka incydentów

3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2007 odnotowaliśmy 2108 incydentów. W następnych rozdziałach znajduje się szczegółowa klasyfikacja zgłoszonych do nas incydentów.

3.2 Typy odnotowanych incydentów

Poniższa tabela przedstawia zbiorcze zestawienie statystyk odnotowanych incydentów. Nasza klasyfikacja zawiera osiem głównych typów incydentów oraz kategorię „inne". Każdy z głównych typów zawiera podtypy incydentów, które najczęściej stanowią bardziej precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	0	544	25,81
Spam	531		
Dyskredytacja, obrażanie	10		
Pornografia dziecięca, przemoc[3]	3		

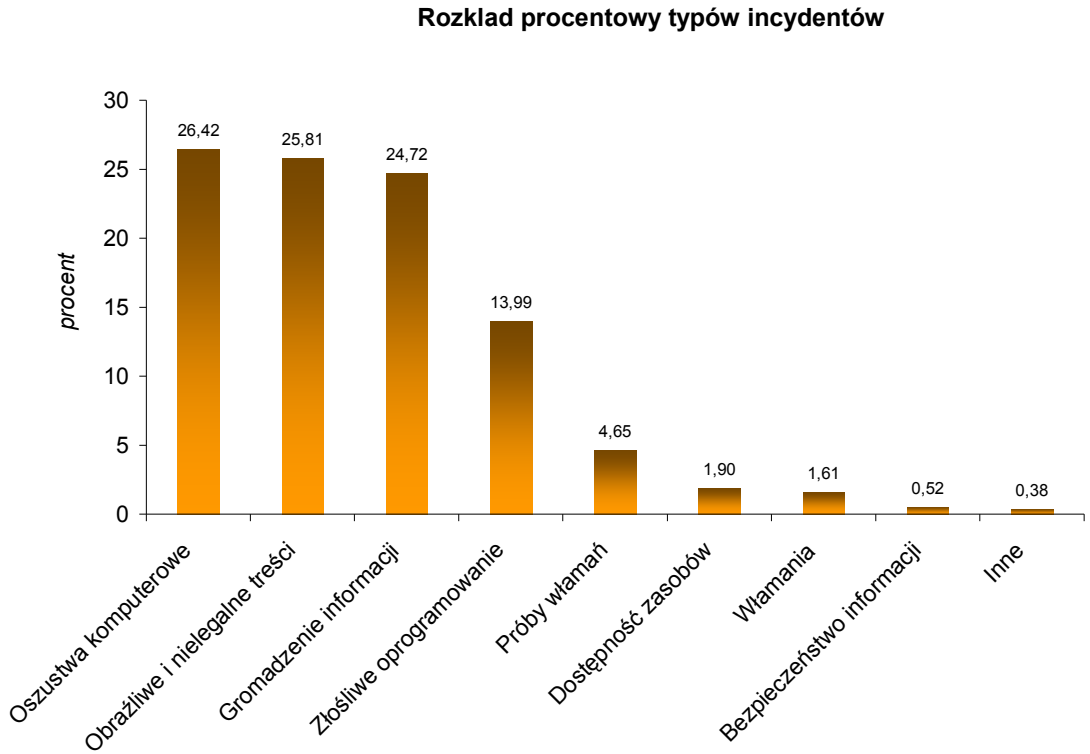
[2] Niniejszy raport jest dwunastym z kolei raportem rocznym naszego zespołu. Dotychczasowe raporty (począwszy od roku 1996) dostępne są na stronie CERT Polska (http://www.cert.pl/raporty/).

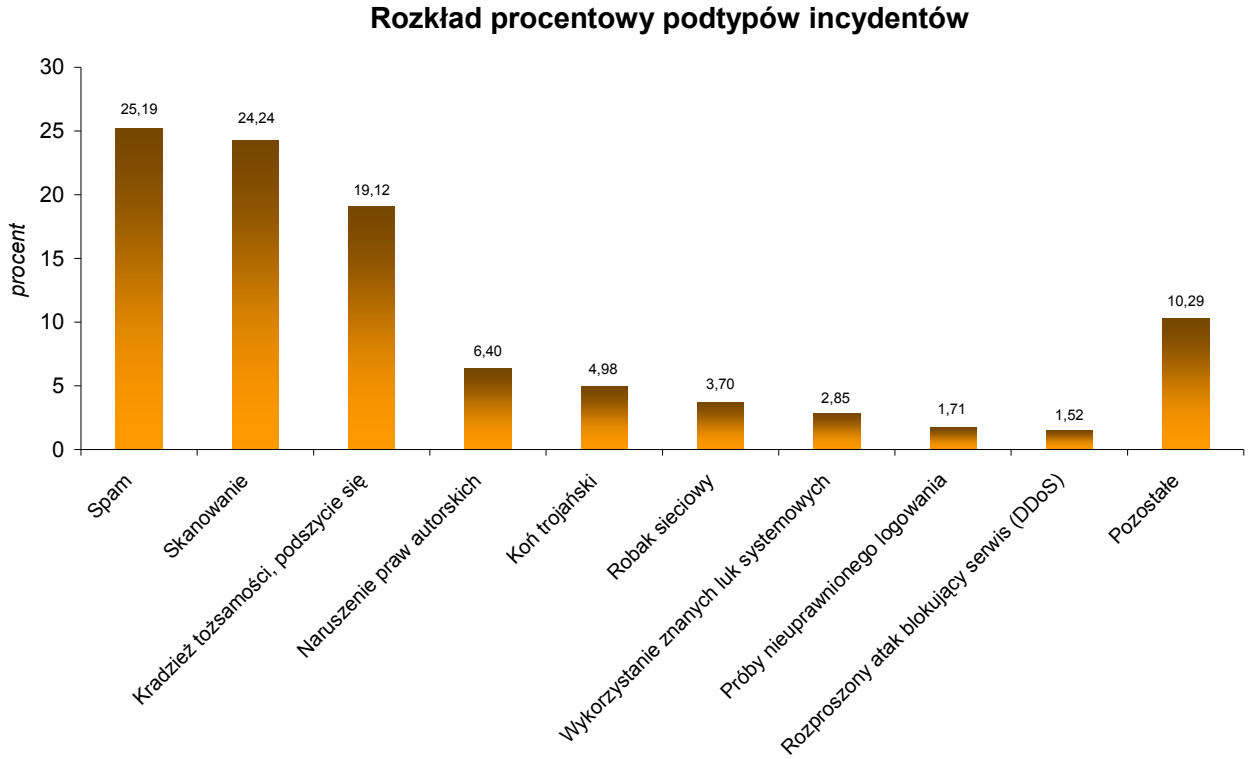
[3] Wszelkie zgłoszenia dotyczące nielegalnych treści, w rozumieniu polskiego prawa, kierowane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (http://www.dyzurnet.pl/)

Złośliwe oprogramowanie	86	295	13,99
Wirus	16		
Robak sieciowy	78		
Koń trojański	105		
Oprogramowanie szpiegowskie	7		
Dialer	3		
Gromadzenie informacji	1	521	24,72
Skanowanie	511		
Podsłuch	0		
Inżynieria społeczna	9		
Próby włamań	1	98	4,65
Wykorzystanie znanych luk systemowych	60		
Próby nieuprawnionego logowania	36		
Wykorzystanie nieznanych luk systemowych	1		
Włamania	1	34	1,61
Włamanie na konto uprzywilejowane	10		
Włamanie na konto zwykłe	19		
Włamanie do aplikacji	4		
Atak na dostępność zasobów	0	40	1,90
Atak blokujący serwis (DoS)	8		
Rozproszony atak blokujący serwis (DDoS)	32		
Sabotaż komputerowy	0		
Atak na bezpieczeństwo informacji	3	11	0,52
Nieuprawniony dostęp do informacji	4		
Nieuprawniona zmiana informacji	4		
Oszustwa komputerowe	5	557	26,42
Nieuprawnione wykorzystanie zasobów	14		
Naruszenie praw autorskich	135		
Kradzież tożsamości, podszycie się (w tym Phishing)	403		
Inne	8	8	0,38
SUMA	2108	2108	100

3.3 Typy odnotowanych ataków

Poniższe wykresy przedstawiają rozkład procentowy typów i podtypów incydentów.





W tym roku trzy najczęściej występujące typy incydentów mają prawie identyczny udział procentowy (różnica poniżej 2%). Jest to sytuacje odmienna od zeszłorocznej, gdzie różnice wynosiły około

20%. Po raz pierwszy w historii publikowanych przez nas raportów, najczęściej pojawiającym się typem incydentów były *Oszustwa komputerowe* (26,42%). Niebagatelny wpływ na taki stan rzeczy miał wzrost liczby zgłoszeń dotyczących *Kradzieży tożsamości, podszycia się* (z 12,53% do 19,12% - są to głównie przypadki phishingu) oraz *Naruszenia praw autorskich* (z 0,99% do 6,4% - w większości zgłoszenia z systemów automatycznych skanujących sieci P2P).

Drugim pod względem liczebności typem incydentów były *Obraźliwe i nielegalne treści* (25,81 %), na co bezpośredni wpływ miała duża ilość zgłoszeń dotyczących *Spamu* (25,19%). Były to głównie, tak jak w roku 2006, zgłoszenia pochodzące ze SpamCopa (międzynarodowy projekt internetowy, mający na celu walkę ze spamem).

Kolejnym typem incydentów było *Gromadzenie informacji* (24,72%). Z roku na rok obserwujemy mniejszy udział tego typu zgłoszeń w statystykach, chociaż nadal utrzymuje się on na wysokim poziomie. Na taki stan rzeczy ma wpływ coraz mniejszy udział przypadków *Skanowań*. W przeciągu 5 lat spadek o 57 punktów procentowych, z 81,8% do 24,24%, w roku obecnym.

3.4 Zgłaszający, poszkodowani, atakujący

Na potrzeby statystyki odnotowywane są trzy kategorie podmiotów związanych z incydentami: zgłaszający incydent, poszkodowany w incydencie i odpowiedzialny za przeprowadzenie ataku, czyli atakujący. Dodatkowo kategorie te uwzględniane są w rozbiciu na podmiot krajowy i podmiot zagraniczny.

Poniższa tabela przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	283	**13,43**	266	**12,62**	83	**3,94**
CERT[4]	681	**32,31**	0	**0,00**	0	**0,00**
ISP Abuse	4	**0,19**	0	**0,00**	0	**0,00**
Inna instytucja ds. Bezpieczeństwa	555	**26,33**	0	**0,00**	0	**0,00**
Firma komercyjna	497	**23,58**	914	**43,36**	1240	**58,82**
Ośrodek badawczy lub edukacyjny	44	**2,09**	148	**7,02**	274	**13,00**
Instytucja niekomercyjna	11	**0,52**	11	**0,52**	69	**3,27**
Jednostka rządowa	33	**1,57**	46	**2,18**	51	**2,42**

[4] Zawiera zgłoszenia pochodzące z systemów automatycznych, w tym także z systemu ARAKIS

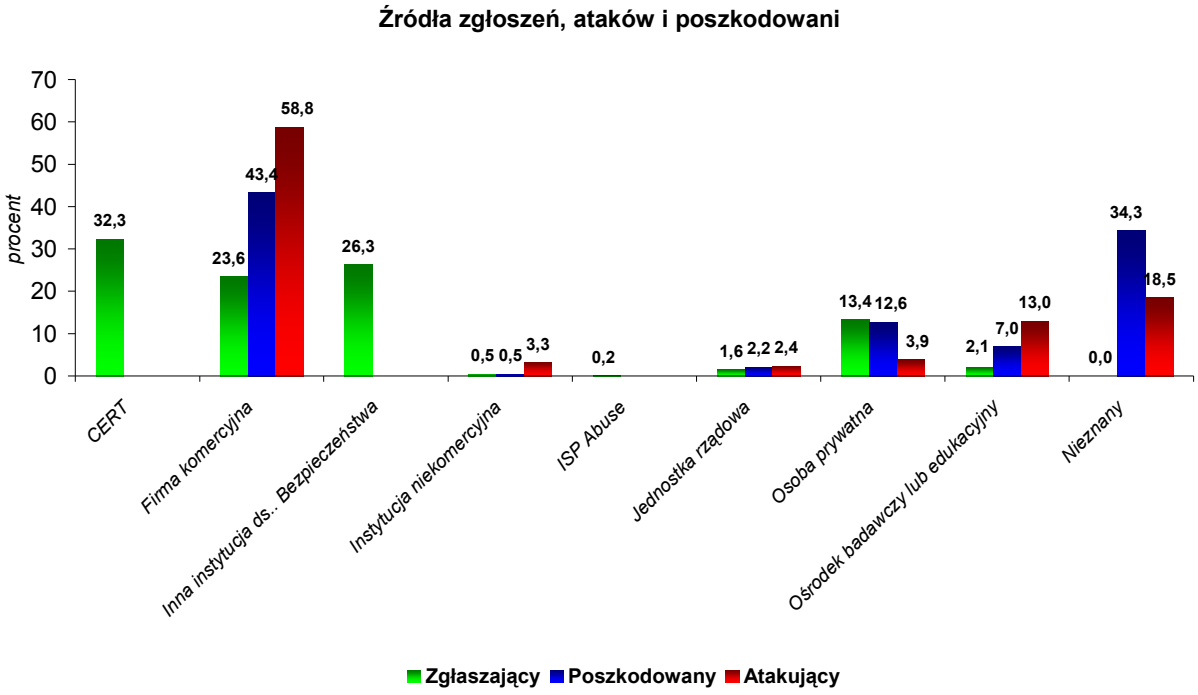
Nieznany	0	**0,00**	723	**34,30**	391	**18,55**
Kraj	966	**45,83**	955	**45,30**	1800	**85,39**
Zagranica	1142	**54,17**	540	**25,62**	162	**7,69**
Nieznany	0	**0,00**	613	**29,08**	146	**6,92**

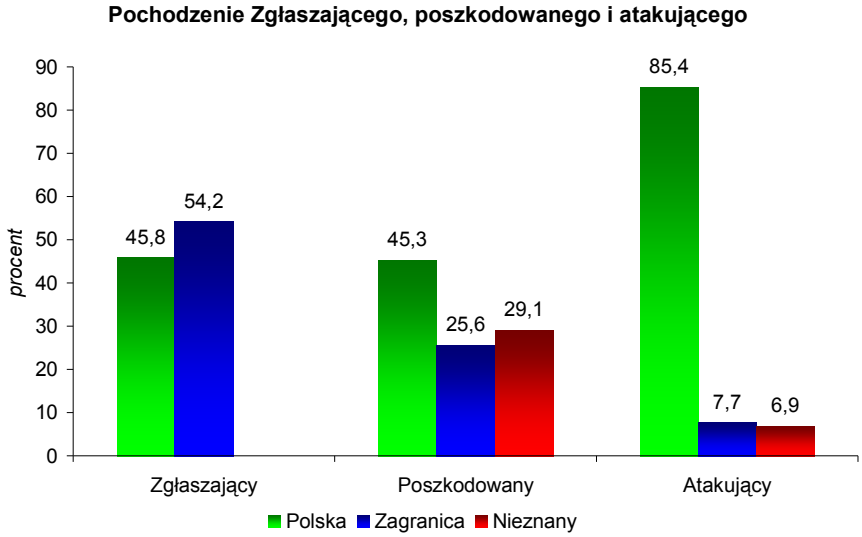
W roku 2007 najczęściej otrzymywaliśmy zgłoszenia od *Zespołów reagujących* (32,3 %) - Jest to sytuacja taka sama jak w poprzednim roku. Część z tych zgłoszeń pochodziła z systemu ARAKIS (http://www.arakis.pl/) i była wygenerowana automatycznie. Znaczącymi źródłami zgłaszania incydentów były również *Inne instytucje ds. Bezpieczeństwa* (26,3%) oraz *Firmy komercyjne* (23,6%). W pierwszym przypadku mieliśmy do czynienia głównie za zgłoszeniami ze SpamCopa., natomiast 13,4 % zgłoszeń otrzymaliśmy od *Osób prywatnych*.

Wśród *Poszkodowanych* najczęściej występowały *Firmy komercyjne* (43,4%). Sytuacja taka ma miejsce od kilku lat. Aż w 34,3% przypadków nie można było ustalić poszkodowanego, ponieważ były to w głównej mierze zgłoszenia przesyłane przez SpamCopa oraz zespoły reagujące w imieniu osób trzecich. 12,6% poszkodowanych to *Osoby prywatne*.

Spośród *Atakujących* ponad połowę stanowiły *Firmy komercyjne* (58,8%). Z roku na rok notujemy coraz więcej takich przypadków. W 18,5% *Atakujący* pozostawał *Nieznany*. Tak jak do tej pory, często nie jesteśmy w stanie zidentyfikować prawdziwego źródła ataku. *Atakujący* ukrywa się za serwerem Proxy, botnetem czy przejętą maszyną nieświadomej ofiary. Dodatkowo pojawiły i upowszechniły się działające na granicy prawa firmy udostępniające łącza, serwery fizyczne i wirtualne, na których umieszczane są nielegalne treści. Oczywiście firmy takie zapewniają pełną anonimowość swoim klientom (np. Russian Businnes Network).

Zmiana w porównaniu do lat ubiegłych nastąpiła w przypadku klasyfikacji dotyczącej źródła pochodzenia w rozumieniu geograficznym. Po raz pierwszy odsetek *Zgłaszających* pochodzących z zagranicy (54,2%) przewyższył *Zgłaszających* pochodzących z Polski (45,8%). Na taki stan rzeczy wpłynęła duża liczba zgłoszeń pochodzących ze SpamCopa, zagranicznych banków lub ich reprezentantów raportujących phishing oraz zagranicznych organizacji antypirackich. *Poszkodowany* i *Atakujący* pochodzili w głównej mierze z Polski (45,3% oraz 85,4%), a 25,6% *Poszkodowanych* oraz 7,7% *Atakujących* była z zagranicy. Niezmiennie na dość wysokim poziomie utrzymuje się odsetek *Poszkodowanych*, których pochodzenie nie jest znane (29,1%). Przyczyną są, podobnie jak jak w przypadku *Źródła poszkodowanych*, zgłoszenia składane w czyimś imieniu, bez wskazania poszkodowanego.

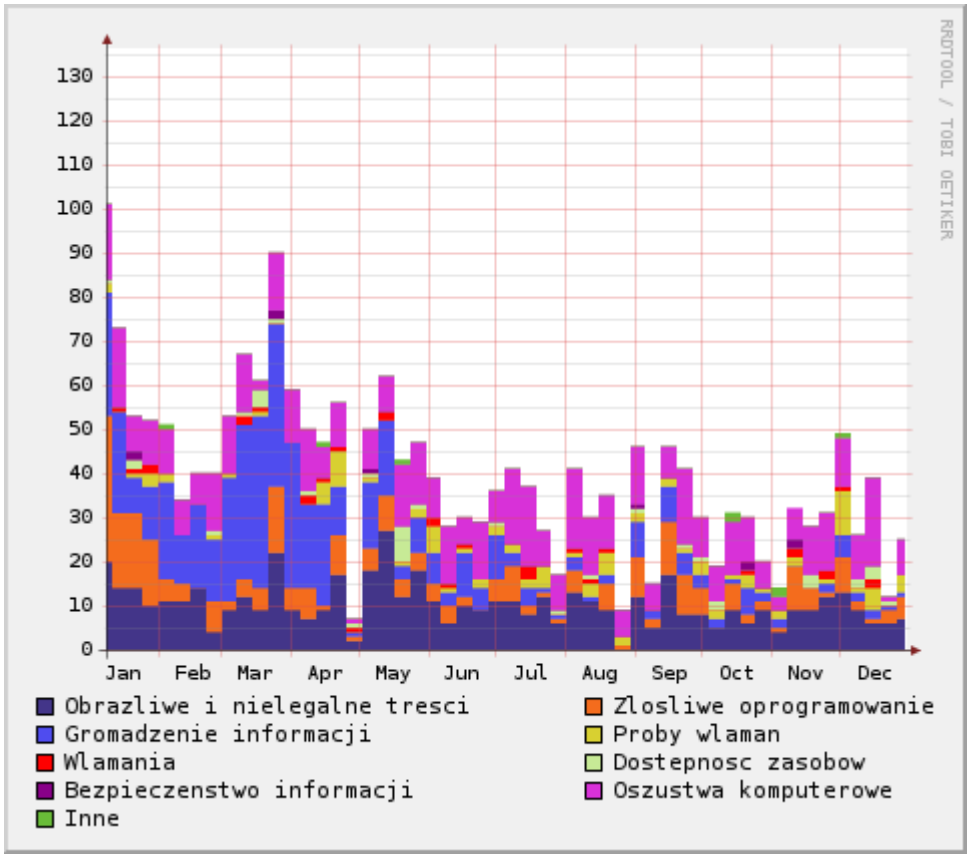




4 Statystyki dodatkowe

4.1 Liczba incydentów zgłaszanych tygodniowo z podziałem na główne kategorie

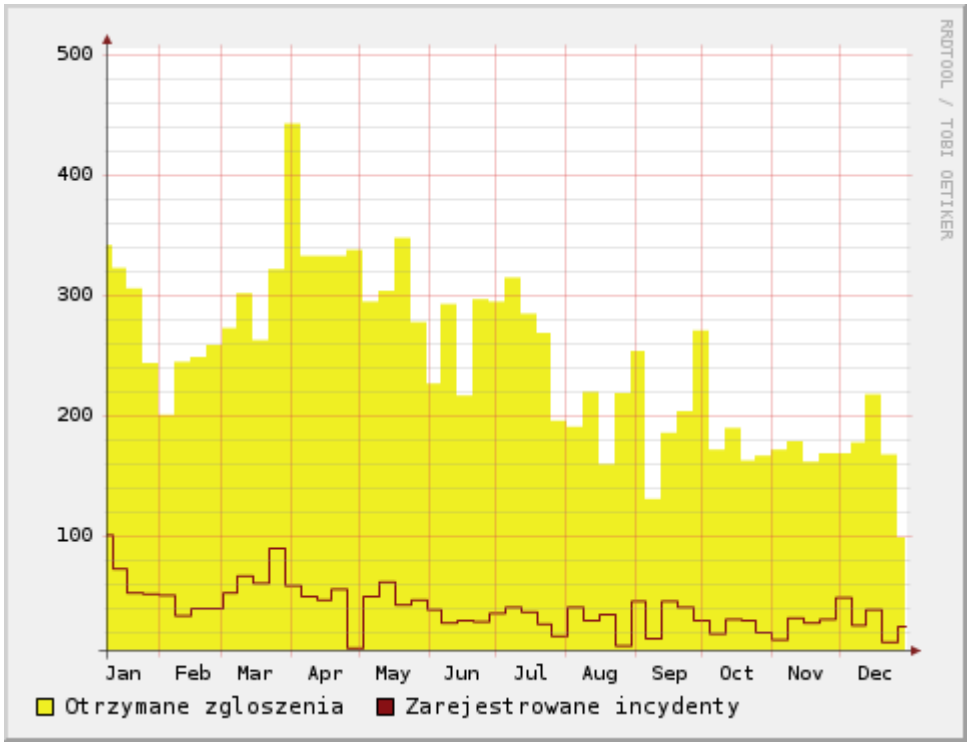
Poniższy wykres przedstawia liczbę incydentów zarejestrowanych w okresie tygodnia, z wyszczególnieniem głównych kategorii.



Rejestrowaliśmy od 30 do 60 incydentów tygodniowo. W pierwszych dwóch miesiącach 2007 roku widoczny jest zwiększony udział incydentów dotyczących *Złośliwego oprogramowania*. Bezpośrednio po nim następuje wzrost incydentów dotyczących G*romadzenia informacji*. Możliwe, że jest to wynik budowania botnetu. W pierwszej fazie infekowano maszyny za pośrednictwem *Złośliwego oprogramowania* zaszytego w stronach WWW. Następnie zainfekowane w ten sposób maszyny, w poszukiwaniu nowych ofiar, zaczęły intensywnie skanować sieci. W odróżnieniu od roku 2006, w miarę równomiernie rozkłada się ilość incydentów dotyczących *Obraźliwych i nielegalnych treści*, czyli w głównej mierze spamu.

4.2 Liczba zgłoszeń a liczba incydentów

Poniższy wykres przedstawia liczbę zgłoszeń w stosunku do liczby incydentów.

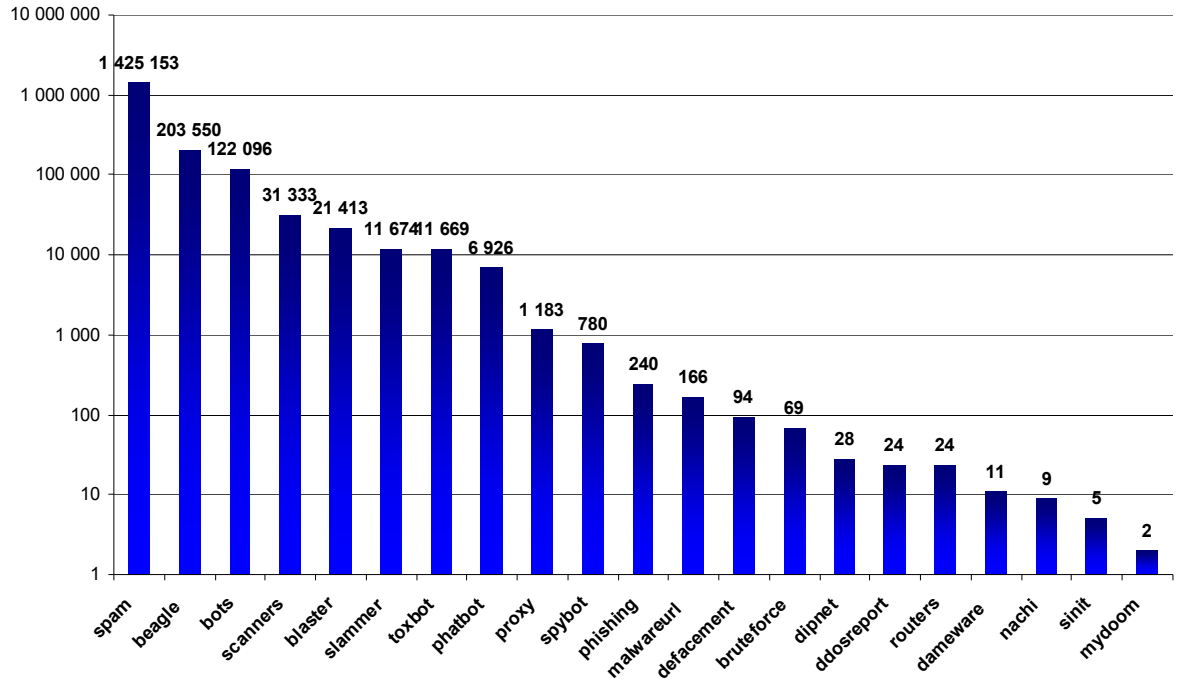


Jak można zauważyć, nie każda informacja trafiająca do naszego systemu obsługi jest w rzeczywistości incydentem. Większość odrzuconych przypadków to oczywiście spam. Bardzo często zdarza się, że informacja o incydencie trafia do naszego zespołu z wielu źródeł. Niejednokrotnie otrzymujemy niezależne zgłoszenia tego samego przypadku (np. zainfekowanego komputera będącego źródłem spamu) z automatycznych systemów detekcji oraz od użytkowników indywidualnych.

4.3 Liczba przypadków nadużyć dotyczących największych polskich operatorów

Poniższe dane prezentują liczbę przypadków nadużyć oszacowaną na podstawie wszystkich danych zgłaszanych do CERT Polska.

Liczba przypadków nadużyć przekazanych do największych polskich operatorów



CERT Polska otrzymuje wiele informacji o poszczególnych wykrytych przypadkach infekcji, źródeł spamu, phishingu itp. znajdujących się w sieciach współpracujących z nami polskich operatorów internetowych[5]. Dane te nie są uwzględniane w liczbie incydentów, ponieważ zgłoszenia takie nie są przez nas obsługiwane i monitorowane. Większość operatorów otrzymuje natomiast dane dotyczące swojej sieci.

Zwraca uwagę olbrzymia liczba przypadków wykorzystania zainfekowanych komputerów do rozsyłania spamu. Zidentyfikowano łącznie 1 425 153 takich przypadków, co stanowi 77,6% wszystkich nadużyć. Należy tu podkreślić, iż jest to liczba infekcji, a nie wysłanych w ich wyniku wiadomości. Ta ostatnia byłaby o kilka rzędów wielkości większa.

[5] Współpraca ta realizowana jest w ramach powstałego z inicjatywy zespołu CERT Polska ABUSE-FORUM. Forum istnieje od listopada 2005 r.

5 Wnioski i trendy

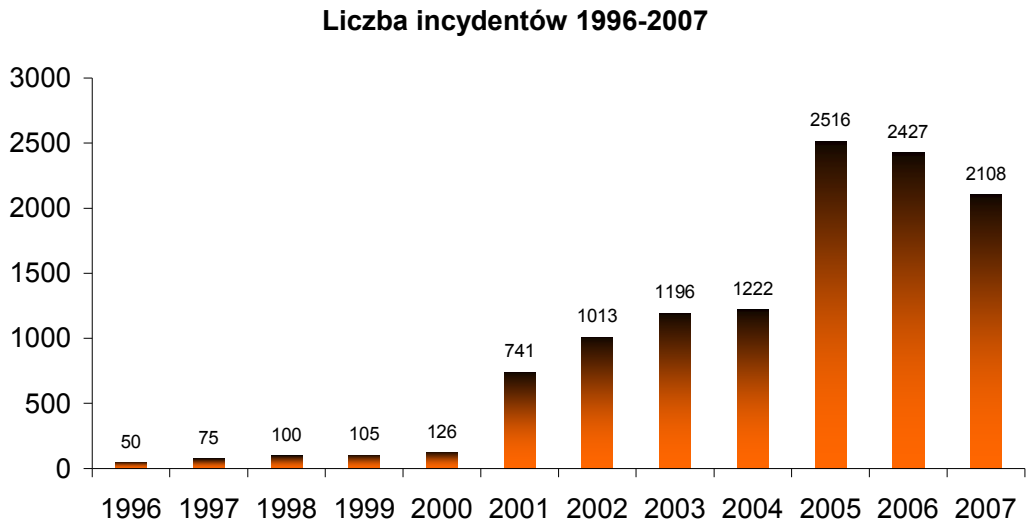
5.1 Najważniejsze zmiany w stosunku do roku ubiegłego

Oprócz najważniejszych trendów i zjawisk, które opisane zostały w rozdziale 5.4, warto zwrócić uwagę na kilka innych istotnych zmian w stosunku do roku 2006, ale także na utrzymanie się niektórych znaczących trendów. Poniżej przedstawiamy te, które są naszym zdaniem najważniejsze:

- Nieznacznie spadł procent skanowań z 27,11% do 24,8%, ale nadal utrzymuje się na znaczącym poziomie
- Zmniejszył się udział zgłoszonego do nas spamu– z 35,31% do 25,34%
- Odnotowaliśmy zwiększenie udziału incydentów dotyczących Phishingu – z 12,5% do 18,93%, przy czym należy podkreślić, że zintensyfikowały się próby podszywania pod polskie banki.
- Nadal najczęściej zgłaszającym były zespoły typu CERT
- Odsetek zgłaszających pochodzących z zagranicy przewyższył odsetek zgłaszających z Polski. Poszkodowany i atakujący tak jak w roku poprzednim w większości pochodził z Polski
- Na dość wysokim poziomie utrzymał się odsetek incydentów, gdzie nieznany był poszkodowany (29,1%) . Zmalał za to procent incydentów, w których nieznany był atakujący (z 15% do 6,9%)
- Znacznie wzrósł udział incydentów dotyczących naruszenia praw autorskich z 0,78% do 6,16%
- Zanotowaliśmy mniejszą liczbę incydentów niż w roku poprzednim (wyjaśnienie tego faktu poniższym rozdziale)

5.2 Liczba incydentów w latach 1996 – 2007

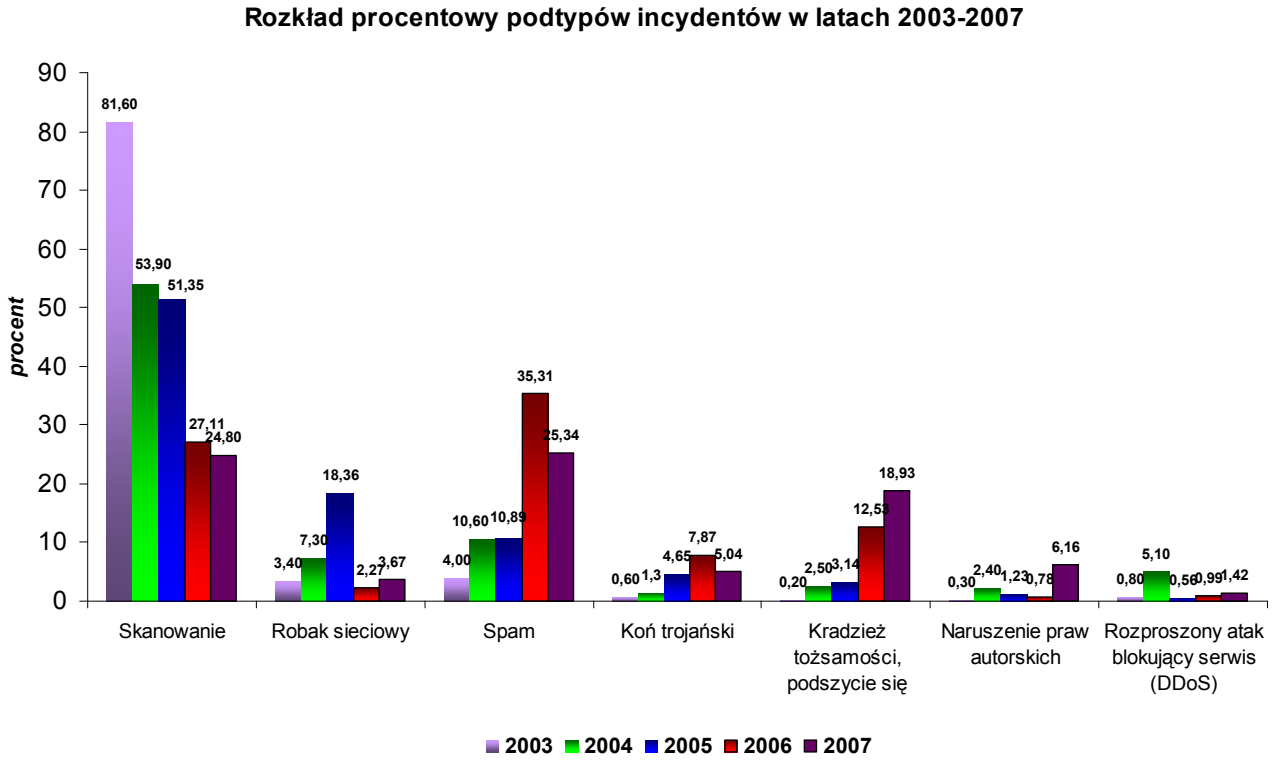
Poniższy wykres przedstawia liczbę incydentów w latach 1996 – 2007



Drugi rok z rzędu zanotowaliśmy mniejszą liczbę incydentów. Jedną z przyczyn takiej sytuacji jest zmniejszenie liczby zgłoszeń z systemów automatycznych. Przestaliśmy otrzymywać je z takich źródeł jak myNetWatchman.com, CERT RENATER czy DShield.org. Dodatkowo incydenty dotyczące największych operatorów są przekazywane bezpośrednio do nich w sposób automatyczny, bez rejestracji w naszym systemie (więcej na ten temat w p.4.3) . Warto zwrócić również uwagę, że w ostatnich 2 latach nie pojawiły się spektakularne przypadki masowych robaków czy wirusów, które w przeszłości systematycznie zgarniały żniwa w postaci olbrzymiej liczby przejętych komputerów. Ostatnie takie przypadki miały miejsce w 2004 i 2005 roku i związane były z robakami Sasser i Blaster (więcej na ten temat w 5.3).

5.3 Rozkład procentowy podtypów incydentów w latach 2003-2007.

Od roku 2003 statystyki są tworzone w oparciu o tę samą klasyfikacje. Umożliwia to nam porównanie rozkładu procentowego incydentów na przestrzeni ostatnich pięciu lat (patrz wykres poniżej).



Jak można zauważyć, w okresie tym znacznie spadła liczba S*kanowań* (z 81.6% do 24,8%). Na taki stan rzeczy, w głównej mierze, mają wpływ dwa czynniki. Po pierwsze, coraz częściej potrafimy rozpoznać przyczynę skanowania, przez co incydent kwalifikowany jest np. jako robak sieciowy. Po drugie, po 2004 roku nie pojawiły się luki w systemach z rodziny Microsoft Windows, które pozwalałyby na automatyczną dystrybucje robaka, tak jak miało to miejsce w przypadku Sassera czy Blastera. W związku z tym robaki nie skanują już tak intensywnie sieci w poszukiwaniu nowych ofiar. Z tego też powodu obserwujemy dużo mniejszą liczbę zgłoszeń dotyczących *Robaków sieciowych (*spadek z 18,4% w roku 2005 do 3,7% w roku 2007*)*. Szczyt przypadł na lata 2004 oraz 2005, kiedy to sieci były intensywnie penetrowane przez wspomniane już robaki. Podkreślić należy bardzo duży wzrost zgłoszeń dotyczących *Kradzieży tożsamości, podszycia się* , czyli w głównej mierze phishingu. Na przestrzeni czterech ostatnich lat udział procentowy tego typu incydentów wzrósł ponad siedmiokrotnie. Dość duży przyrost nastąpił również w ostatnim roku w przypadku zgłoszeń *Naruszenia praw autorskich.* Oscylowały one wokół poziomu 1% - 2%, zaś w roku 2007 osiągnęły ponad 6%. Jest to wynik aktywności dużych koncernów filmowych oraz reprezentujących je organizacji antypirackich. Nadal na wysokim poziomie utrzymuje się *Spam* (25,3%), który obok stron WWW jest obecnie głównym kanałem dystrybucji złośliwego oprogramowania.

5.4 Najważniejsze trendy i zjawiska obserwowane w roku 2007

Poniżej przedstawiamy najbardziej znaczące trendy i zjawiska, występujące w roku 2007, wynikające zarówno z obsługi incydentów, jak i z innych obserwacji poczynionych przez CERT Polska:

- Na niskim poziomie utrzymuje się liczba incydentów dotyczących *robaka sieciowego*. Wynika to z faktu, że nie pojawiły się w 2007 roku żadne nowe luki pozwalające na automatyczną propagację robaków.

- Częściej notowaliśmy incydenty związane z *phishingiem*. Większość spraw dotyczyła fałszywych stron zagranicznych banków, umieszczonych na polskich serwerach. Były to zazwyczaj maszyny przejęte przez hakera.

- Zdarzają się coraz poważniejsze incydenty związane z *phishingiem* ukierunkowanym na polskie banki. Spodziewamy się wzrostu tego zjawiska.

- Liczba *ataków DDoS* jest niewielka, ale są to zazwyczaj poważne ataki na duże instytucje, a nawet całe państwa. Przykładem jest Estonia, w której atak taki doprowadził do paraliżu ważnych serwerów rządowych oraz bankowych.

- Nastąpił wzrost liczby zgłoszeń dotyczących *praw autorskich*. Jest on spowodowany aktywnością dużych producentów filmowych i muzycznych oraz reprezentujących je organizacji. Zgłoszenia pochodziły głównie z automatów skanujących sieci P2P.

- Pojawiło się dużo incydentów związanych z Javascriptem. Zazwyczaj dotyczą one dystrybucji i ukrywania malware'u w kodzie Javasriptu. Dodatkowo kod taki pozwala atakującemu na identyfikację pochodzenia ofiary. Tego typu incydenty są dość trudne i nawet doświadczeni administratorzy mają problem z ich identyfikacją i analizą kodu.

- Po raz pierwszy mieliśmy do czynienia z wykorzystaniem metod *socjotechnicznych* na dużej grupie ofiar. W przypadku incydentu związanego z serwisem fotka.pl, atakujący rozsyłał maile, w których podszywał się pod użytkowników fotka.pl z propozycja obejrzenia ich zdjęć. W rzeczywistości po kliknięciu na link, ładował się złośliwy kod.

- Jak w zeszłych latach, działania hakerów są coraz bardziej zaawansowane, a wykorzystywane mechanizmy coraz bardziej skomplikowane.

6 Kontakt

Zgłaszanie incydentów:	cert@cert.pl, spam: spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	http://www.trusted-introducer.nl/teams/0x553FEB09.asc
Strona WWW:	http://www.cert.pl/
Feed RSS:	http:/www..cert.pl/rss
Adres:	NASK / CERT Polska
	ul. Wąwozowa 18

02-796 Warszawa

tel.: +48 22 3808 274

fax: +48 22 3808 399