CERT Polska

Raport 2003

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003

1 Wstęp

1.1 Informacje dotyczące zespołu CERT Polska

CERT (Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK). 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.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń
- współpraca z innymi zespołami IRT (Incidents Response Team) w ramach FIRST
- prowadzenie działań informacyjno edukacyjnych, zmierzających do wzrostu świadomości dotyczącej 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] 22 listopada 2001 zespół uzyskał najwyższy poziom zaufania Trusted Introducer Accredited Team.

2 Statystyki CERT Polska

Zgodnie z powyższymi założeniami programowymi CERT Polska co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych. Niniejszy raport jest ósmym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT Polska (http://www.cert.pl/raporty/)

3 Klasyfikacja incydentów naruszających bezpieczeństwo teleinformatyczne[2]

Jak wynika z przedstawionych powyżej zadań programowych, zespół CERT Polska prowadzi prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk.

Problematyka klasyfikacji incydentów komputerowych jest od lat dyskutowana wśród osób i instytucji zajmujących się tą tematyką. Co jakiś czas pojawiają się nowe propozycje klasyfikacji, które zyskują mniejszą lub większą popularność. Największą szansę upowszechnienia mają te propozycje, które zyskują aprobatę jak największej liczby ośrodków zajmujących się zbieraniem i publikowaniem statystyk. Dlatego naszym zdaniem na szczególną uwagę zasługuje propozycja klasyfikacji wypracowana w ramach projektu „The European CSIRT Network - eCSIRT.net" (http://www.ecsirt.net/), w którym to projekcie zespół CERT Polska również uczestniczył. Klasyfikacja ta jest podstawą opracowania niniejszego raportu.

4 Statystyka incydentów

4.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2003 odnotowaliśmy 1196 incydentów.

[2] Dalej zwanymi incydentami

4.2 Typy odnotowanych incydentów

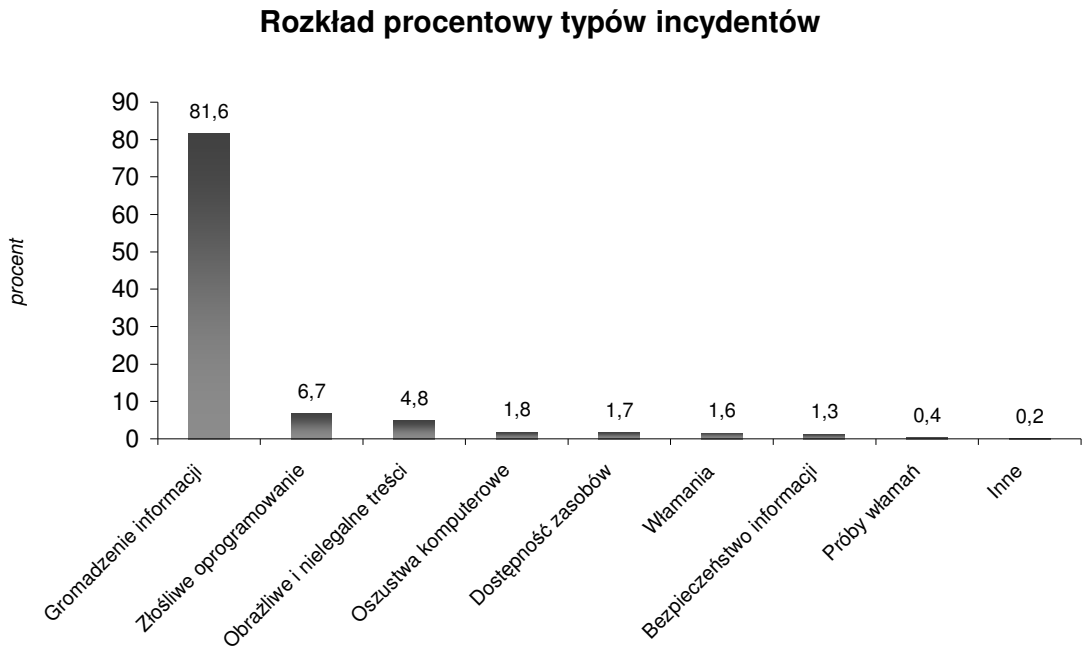
Poniża tabela przedstawia zbiorcze zestawienie statystyk odnotowanych incydentów. Nasza klasyfikacja zawiera 8 głównych typów incydentów oraz kategorię „inne". Każdy z głównych typów zawiera podtypy incydentów, które najczęściej stanowią precyzyjny opis incydentu, z jakim mieliśmy do czynienia[3].

Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	1	57	4,8%
Spam	48		
Dyskredytacja, obrażanie	2		
Pornografia dziecięca, przemoc	6		
Złośliwe oprogramowanie	0	80	6,7%
Wirus	32		
Robak sieciowy	41		
Koń trojański	7		
Oprogramowanie szpiegowskie	0		
Dialer	0		
Gromadzenie informacji	0	976	81,5%
Skanowanie	976		
Podsłuch	0		
Inżynieria społeczna	0		
Próby włamań	2	5	0,4%
Wykorzystanie znanych luk systemowych	1		
Próby nieuprawnionego logowania	1		
Wykorzystanie nieznanych luk systemowych	1		
Włamania	11	19	1,6%
Włamanie na konto uprzywilejowane	6		
Włamanie na konto zwykłe	2		
Włamanie do aplikacji	0		
Dostępność zasobów	0	20	1,7%
Atak blokujący serwis (DoS)	10		
Rozproszony atak blokujący serwis (DDoS)	10		
Sabotaż komputerowy	0		
Bezpieczeństwo informacji	0	16	1,3%
Nieuprawniony dostęp do informacji	16		
Nieuprawniona zmiana informacji	0		
Oszustwa komputerowe	0	21	1,8%
Nieuprawnione wykorzystanie zasobów	15		
Naruszenie praw autorskich	4		
Kradzież tożsamości, podszycie się	2		
Inne	2	2	0,2%
SUMA	1196		100%

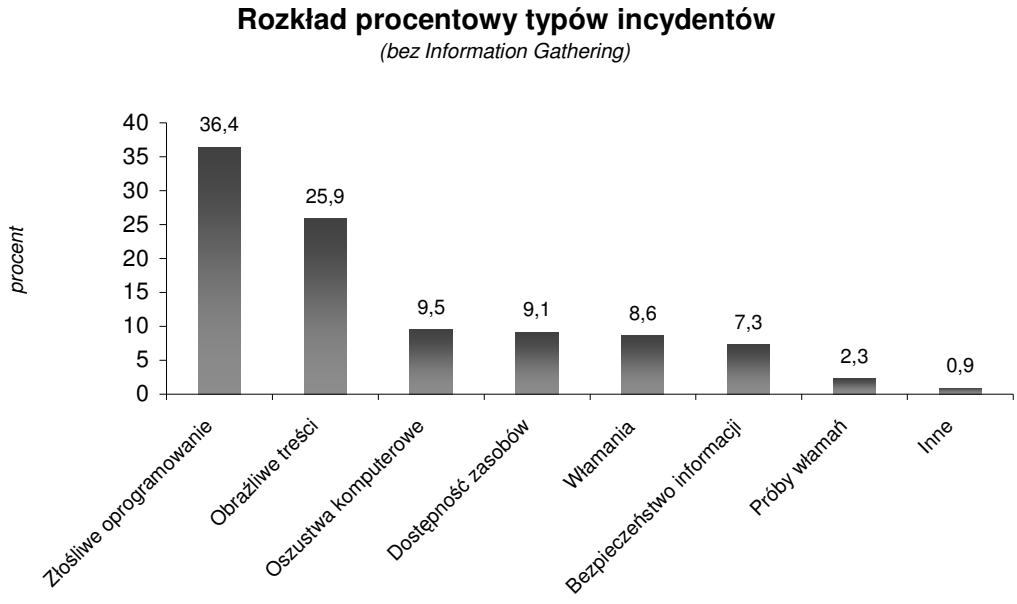
[3] Dokładny opis poszczególnych typów ataków można znaleźć na stronie projektu eCSIRT.net: http://www.ecsirt.net/service/documents/wp4-pub-userguide-v10.html#HEAD7

4.3 Typy odnotowanych ataków

Zgodnie z przedstawioną powyżej klasyfikacją odnotowano następujący rozkład procentowy incydentów.



Jak widać z wykresu zdecydowaną większość stanowi *gromadzenie informacji*, dlatego aby przedstawić wyraźniej różnice pomiędzy pozostałymi kategoriami, przedstawiamy poniżej wykres, z którego został usunięty ten typ ataku:



Należy zwrócić uwagę, że zdecydowana dominacja skanowania, które w całości „tworzy" kategorię *gromadzenie informacji* nie jest związana tylko i wyłącznie z próbą zbierania informacji przed ewentualnym atakiem sieciowym. Trzeba być świadomym, że praktycznie niemalże każdy przypadek skanowania w Internecie świadczy o tym, że gdzieś już nastąpiło włamanie do komputera, z którego odbywa się skanowanie, niezależnie od tego czy włamanie nastąpiło poprzez działanie robaka sieciowego, czy też był to inny atak specjalnie skierowany na dany komputer. Problemem oczywiście pozostaje w takim przypadku klasyfikowanie. Jeśli mamy do czynienia z przypadkiem skanowania z komputera, do którego wcześniej nastąpiło włamanie, to powstaje pytanie: Czy jest to w klasyfikacji *włamanie* czy *skanowanie*? Otóż przyjęliśmy zasadę, że incydent jest klasyfikowany zgodnie z tym jaki problem jest zgłaszany. Jeśli otrzymujemy informację od poszkodowanego, że jego sieć jest skanowana to incydent jest klasyfikowany jako *skanowanie*, niezależnie od tego, że w toku wyjaśniania sprawy może się okazać, że do komputera z którego odbywało się skanowanie, wcześniej nastąpiło włamanie i teoretycznie jest to przypadek znacznie poważniejszy.

Warto również odnotować duży udział w zgłoszeniach przypadków związanych z obraźliwymi i nielegalnymi treściami. Oczywiście kilkadziesiąt przypadków spamu, jakich zostało do nas zgłoszonych, nie odzwierciedla rzeczywistego problemu związanego z przesyłaniem niezamawianej korespondencji. Przypadki te należy traktować jako wyjątkowo uciążliwe dla poszkodowanego. W rzeczywistości w zeszłym roku nastąpił zdecydowany wzrost ilości spamu w sieci Internet. Problem został zidentyfikowany jako poważny i obecnie wiele działań technicznych i legislacyjnych skierowanych jest na opanowanie i ograniczenie tego zjawiska.

Zgłoszenia *obraźliwych i nielegalnych treści* dotyczą również przypadków wykorzystywania Internetu do dystrybucji i wymiany treści związanych z pornografią dziecięcą.

4.4 Zgłaszający, poszkodowani, atakujący

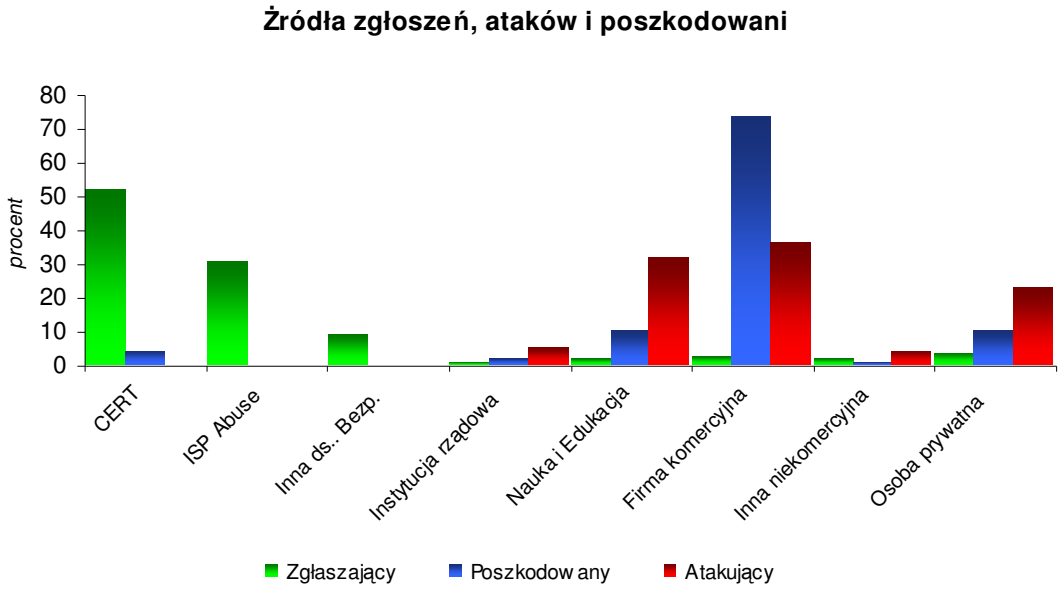
Na potrzeby statystyki odnotowywane są trzy kategorie podmiotów związanych z incydentami: zgłaszający incydent, poszkodowany w incydencie i odpowiedzialny za przeprowadzenie ataku, czyli atakujący. Dodatkowo kategorie te uwzględniane są w rozbiciu na podmiot krajowy i podmiot zagraniczny.

Poniższa tabela przedstawia zbiorcze zestawienie danych dotyczących podmiotów incydentu.

Podmiot	Zgłaszający	%	Poszkodowany	%	Atakujący	%
Osoba prywatna	38	**3,2**	49	**4,1**	44	**3,7**
CERT	616	**51,5**	20	**1,7**	0	**0**
ISP Abuse	359	**30**	0	**0**	23	**1,9**
Inna instytucja ds. Bezpieczeństwa	104	**8,7**	0	**0**	0	**0**
Firma komercyjna	25	**2,1**	356	**29,8**	47	**3,9**

Ośrodek badawczy lub edukacyjny	18	**1,5**	48	**4**	61	**5,1**
Instytucja niekomercyjna	18	**1,5**	3	**0,3**	8	**0,7**
Jednostka rządowa	8	**0,7**	8	**0,7**	10	**0,8**
Nieznany	10	**0,8**	712	**59,4**	1003	**83,9**
Kraj	109	**9,1**	133	**11,1**	1071	**89,6**
Zagranica	1072	**89,6**	993	**83**	23	**1,9**
Nieznany	15	**1,3**	70	**5,9**	102	**8,5**

Jak wynika z powyższej tabeli, najłatwiej można było ustalić i sklasyfikować dane dotyczące zgłaszających incydenty. Mniejsza możliwość ustalenia danych dotyczących poszkodowanych wynika głównie z tego, że wiele zgłoszeń jest dokonywanych tylko w imieniu poszkodowanego i konkretna informacja o nim nie dociera do CERT Polska. Najmniej wiemy o tym, kto jest odpowiedzialny atak. W tym wypadku głównym problemem jest ustalenie kategorii atakującego w przypadku, kiedy jego adres internetowy nie zdradza tego w sposób oczywisty. Tak np. jest w przypadku korzystania z szerokopasmowego dostępu do Internetu, zarówno przez osoby prywatne jak i firmy komercyjne czy inne instytucje.



Jak widać wśród zgłaszających dominują CERT-y oraz komórki bezpieczeństwa ISPs (Internet Service Providers). Dodatkowo otrzymujemy wiele zgłoszeń od innych instytucji zajmujących się monitoringiem bezpieczeństwa w Internecie. W tym przypadku zgłoszenia te dotyczącą głównie skanowań o dużym nasileniu oraz odnotowanych w sieci komputerów umożliwiających anonimowe rozsyłanie spamu (tzw. *Open relay*). Wśród poszkodowanych najwięcej jest firm komercyjnych[4], dużo mniej natomiast instytucji badawczych i edukacyjnych oraz osób prywatnych. W każdym z tych przypadków warto zauważyć, że podmioty te stanowią również największe źródło ataków. Potwierdza to fakt wykorzystywania przez hakerów przejętych komputerów do dalszych ataków w sieci.

Zdecydowana większość zgłoszeń jak i poszkodowanych (ponad 80%) pochodzi z zagranicy, natomiast atakujący w blisko 90% to użytkownicy krajowi.

5 Wnioski i trendy

1) Obserwowane w sieci masowe skanowania nie świadczą tylko i wyłącznie o przygotowaniach przyszłych ataków. Są one skutkiem skutecznego przeprowadzenia wielu ataków, gdyż atakujący wykorzystują przejęte sieci i komputery do przyszłych ataków.

2) W naszych statystykach pojawiają się poważne przypadki dystrybucji w Internecie nielegalnych treści, w szczególności pornografii dziecięcej. Walka z tym zjawiskiem wymaga dobrej koordynacji zarówno krajowej jak i międzynarodowej. Zjawisko nielegalnych treści w Internecie nie jest typowym zjawiskiem, jakim zajmują się CERT-y. Dlatego w odpowiedzi na nie, zespół CERT Polska dąży do stworzenia wydzielonego *hotline'u*, który zjawiskiem tym będzie się zajmował.

3) Wśród źródeł ataku odnotowujemy coraz więcej ataków z firm komercyjnych, ale nadal jest ich też wiele z ośrodków badawczych i edukacyjnych (wyższe uczelnie, szkoły średnie). Należy pamiętać, że wielokrotnie atak z tych jednostek jest konsekwencją wcześniejszego skutecznego ataku na nie.

4) W roku ubiegłym działalność zespołu CERT Polska służyła przede wszystkim użytkownikom zagranicznym, gdyż to oni głównie zgłaszali incydenty[5] Należy jednak dodać, że najpoważniejsze przypadki dotyczyły zgłoszeń od użytkowników krajowych.

5) Coraz bardziej umacnia się pozycja CERT-ów jako jednostek koordynujących przypadki naruszenia bezpieczeństwa w sieci. Ponad 50% wszystkich zgłoszeń to zgłoszenia od innych CERT-ów.

6) Incydenty komputerowe są coraz bardziej skomplikowane i tworzą rozbudowaną sieć powiązań, której efektem są ataki typu DDoS, dystrybucja spamu, nielegalnych treści, próby oszustw na dużą skalę i naruszeń praw autorskich.

[4] z pewnością wynika to również z lepszego monitoringu zagrożeń prowadzonego przez firmy komercyjne
[5] głównie ze względu na fakt, że mają oni zautomatyzowaną detekcję skanowań.

7) W chwili obecnej nie obserwujemy dużego przyrostu ilościowego incydentów. Obserwujemy natomiast coraz więcej poważnych incydentów. W odróżnieniu do lat ubiegłych do zespołu CERT Polska zaczęły trafiać zgłoszenia pochodzące z poważnych instytucji komercyjnych i publicznych.

6 Kontakt

Zgłaszanie incydentów:	cert@cert.pl, spam: spam@cert.pl
Informacja:	info@cert.pl
PGP key:	ftp://ftp.nask.pl/pub/CERT_POLSKA/cert_polska_pgp_keys/CERT_POLSKA.pgp
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 5231 274
fax:	+48 22 5231 399