CERT Polska

Raport 2004

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2004

1 Wstęp

1.1 Informacje dotyczące zespołu CERT Polska

CERT Polska (Computer Emergency Response Team) 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 organizacji inicjatywie Trusted Introducer[1] (http://www.ti.terena.nl/). W ramach tych organizacji CERT Polska 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 i 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] W 2001 r. 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 zgłoszonych do zespołu przypadków naruszenia bezpieczeństwa teleinformatycznego, w polskich zasobach internetowych[2], jak również prowadzi prace w dziedzinie tworzenia wzorców obsługi i rejestracji przypadków naruszenia bezpieczeństwa teleinformatycznego (zwanych dalej incydentami), a także klasyfikacji i tworzenia statystyk.

Jednym z najważniejszych celów tych działań jest wypracowanie stałej, możliwie najbardziej upowszechnionej klasyfikacji, której stosowanie umożliwi porównywanie danych, zarówno w kolejnych latach, jak i pozwoli analizować różnice pomiędzy naszymi obserwacjami a obserwacjami innych zespołów reagujących. W tym roku po raz drugi 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 2004 odnotowaliśmy 1222 incydenty. 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 są opisane przez precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	0	140	11,5
Spam	130		
Dyskredytacja, obrażanie	3		
Pornografia dziecięca, przemoc	7		
Złośliwe oprogramowanie	3[3]	165	13,5
Wirus	57		

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

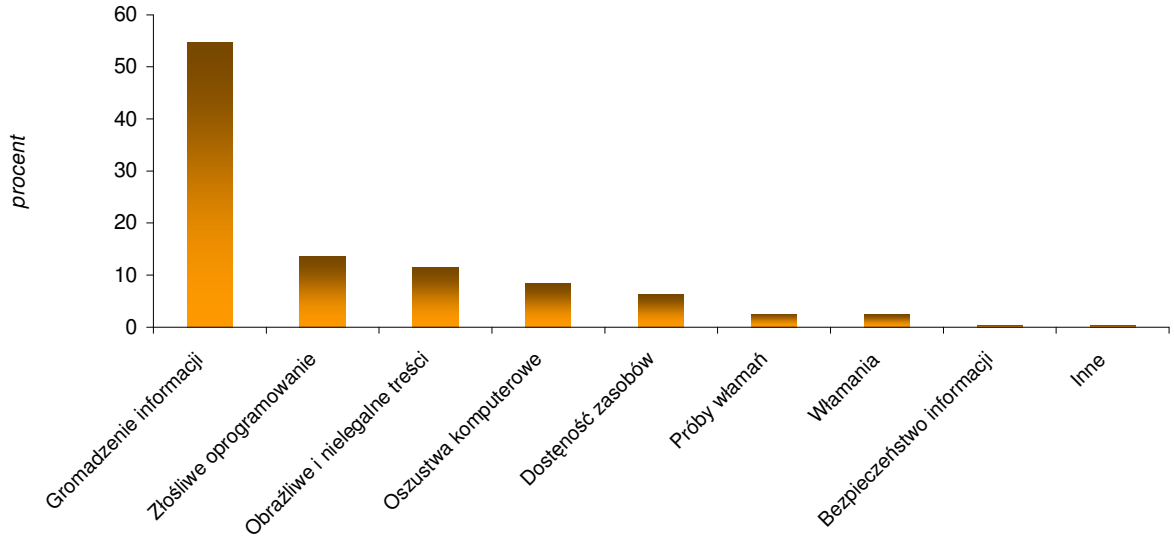
[3] Liczba pokazująca ile jest przypadków w typie głównym zawiera wszystkie te przypadki, które zaliczają się do tego typu, ale nie pasują do żadnego z podtypów.

Robak sieciowy	89		
Koń trojański	16		
Oprogramowanie szpiegowskie	0		
Dialer	0		
Gromadzenie informacji	1	669	54,7
Skanowanie	659		
Podsłuch	0		
Inżynieria społeczna	9		
Próby włamań	3	31	2,5
Wykorzystanie znanych luk systemowych	6		
Próby nieuprawnionego logowania	21		
Wykorzystanie nieznanych luk systemowych	1		
Włamania	7	29	2,4
Włamanie na konto uprzywilejowane	16		
Włamanie na konto zwykłe	3		
Włamanie do aplikacji	3		
Dostępność zasobów	0	77	6,3
Atak blokujący serwis (DoS)	15		
Rozproszony atak blokujący serwis (DDoS)	62		
Sabotaż komputerowy	0		
Bezpieczeństwo informacji	0	4	0,3
Nieuprawniony dostęp do informacji	2		
Nieuprawniona zmiana informacji	2		
Oszustwa komputerowe	0	103	8,4
Nieuprawnione wykorzystanie zasobów	44		
Naruszenie praw autorskich	29		
Kradzież tożsamości, podszycie się	30		
Inne	4	4	0,3
SUMA	1222	1222	100,0

3.3 Typy odnotowanych ataków

Poniższy wykres przedstawia rozkład procentowy incydentów.

Rozkład procentowy typów incydentów



Ponad połowa wszystkich obsłużonych przez CERT Polska incydentów to przypadki dotyczące *gromadzenia informacji* (54,7%), a w szczególności *skanowania*. Powyżej 10% odnotowaliśmy jeszcze dwie kategorie: *złośliwe oprogramowanie* (13,5%) oraz *obraźliwe i nielegalne treści* (11,5%). Najmniej przypadków zgłoszono w kategoriach: *bezpieczeństwo informacji* (0,3%) oraz *włamania* (2,4%).

Zdecydowana przewaga skanowania nad innymi kategoriami wynika głównie z faktu otrzymywania automatycznych zgłoszeń z rozpoznanych i godnych zaufania źródeł, takich jak:

- australijski zespół reagujący – AusCERT;
- japoński zespół Incident Management Team of SECOM-J;
- koreański serwis SecurityMap.Net;
- brazylijski Security Incident Response Team National Education and Research Network – CAIS RNP;
- francuski zespół reagujący – CERT Renater;
- amerykański serwis bezpieczeństwa MyNetWatchMan.com;

Złośliwe oprogramowanie to przede wszystkim zgłoszone do nas przypadki wirusów i robaków sieciowych, zaś *obraźliwe treści* to, jak łatwo się domyślić spoglądając na podtypy tej kategorii, najczęściej przypadki spamu. Warto zwrócić uwagę, że często zgłoszenia spamu okazują się być związane z rozsyłaniem niechcianej korespondencji za pośrednictwem przejętego komputera lub całej ich sieci (botnetu). W takim przypadku incydent taki klasyfikowany był jako *nieautoryzowane wykorzystanie zasobów*. Odnotowane w zestawieniu przypadki spamu oczywiście nie oddają rzeczywistej skali tego

zjawiska; są to tylko takie przypadki, które dla poszkodowanych były wyjątkowo uciążliwe np.: powtarzające się i dlatego zdecydowali się oni je zgłosić.

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	201	**16,4**	169	**13,8**	55	**4,5**
CERT	651	**53,3**	0	**0**	0	**0**
ISP Abuse	56	**4,6**	0	**0**	0	**0**
Inna instytucja ds. Bezpieczeństwa	120	**9,8**	0	**0**	0	**0**
Firma komercyjna	116	**9,5**	150	**12,3**	105	**8,6**
Ośrodek badawczy lub edukacyjny	56	**4,6**	125	**10,2**	86	**7**
Instytucja niekomercyjna	10	**0,8**	19	**1,6**	15	**1,2**
Jednostka rządowa	9	**0,7**	22	**1,8**	15	**1,2**
Nieznany	3	**0,2**	737	**60,3**	946	**77,4**
Kraj	296	**24,2**	384	**31,4**	897	**73,4**
Zagranica	883	**72,3**	739	**60,5**	68	**5,6**
Nieznany	43	**3,5**	99	**8,1**	257	**21**

Jak wynika z przedstawionych danych, ponad połowa zgłoszeń pochodzi od innych *zespołów reagujących* (53,3%). Innymi istotnymi źródłami zgłoszeń incydentów są *indywidualni użytkownicy Internetu* (16,4%), *inne instytucje ds. bezpieczeństwa* (9,8%) oraz *firmy komercyjne* (9,5%).

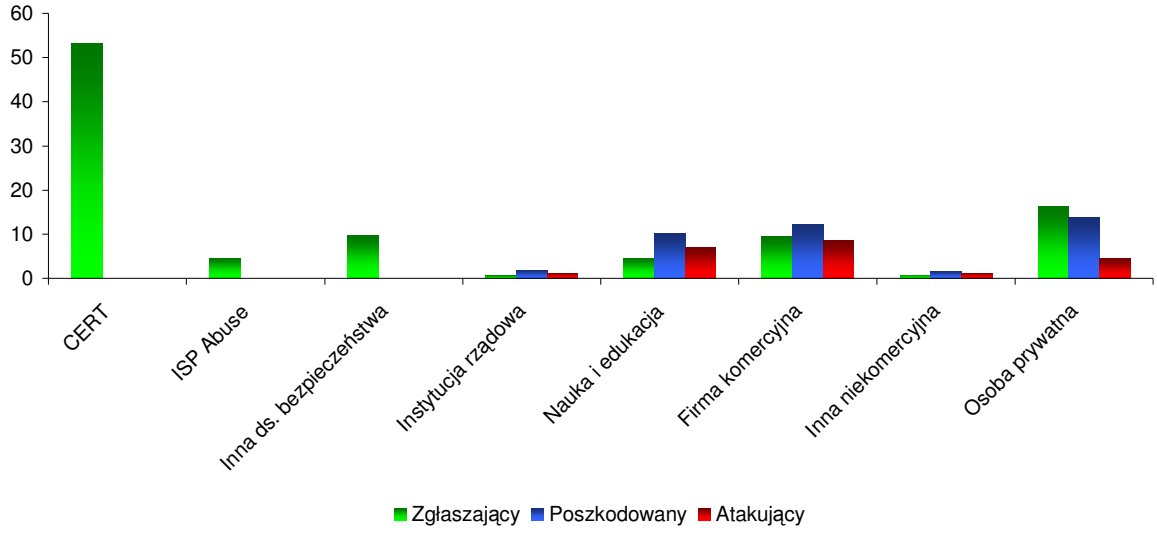
W dwóch pozostałych kategoriach: *poszkodowany* i *atakujący* w większości nie udało się ustalić rodzaju źródła w oparciu o przyjętą typologię. Spowodowane jest to faktem, że wiele zgłoszeń odbywa się w czyimś imieniu, np.: zespół reagujący występuje w imieniu poszkodowanego użytkownika sieci, który do nich

zgłosił incydent. Natomiast dane na temat *atakującego* są zazwyczaj trudne do uzyskania, gdyż najczęściej w poszukiwaniu źródła ataku natrafia się na dostarczyciela usług sieciowych, który oczywiście nie jest za niego odpowiedzialny.

W tych kategoriach, w których dało się to ustalić, najczęściej poszkodowanymi byli *użytkownicy indywidualni, firmy komercyjne* oraz *ośrodki badawcze lub edukacyjne.* Również *firmy komercyjne* i *osoby prywatne* były najczęściej źródłem ataku. Należy jednak jeszcze raz podkreślić, że odsetek zidentyfikowanych podmiotów kategorii *źródło ataku* jest niewielki (22,6%).

Znacznie lepiej jest, jeśli chodzi o ustalenie, skąd pochodzą zgłaszający, poszkodowany i atakujący. Blisko jedna czwarta (24,2%) nadesłanych do nas zgłoszeń incydentów pochodzi z Polski. Reszta, pominąwszy niewielki procent zgłoszeń nieustalonych, to zgłoszenia z zagranicy. Podobna relacja utrzymana jest w przypadku *poszkodowanych* – odpowiednio 31,4% i 60,5%. Nadal większość zgłoszeń to „skargi" na użytkowników polskich, ponieważ 73,4% źródeł ataków ustalonych zostało właśnie jako polskie.

Źródła zgłoszeń, ataków i poszkodowani



4 Wnioski i trendy

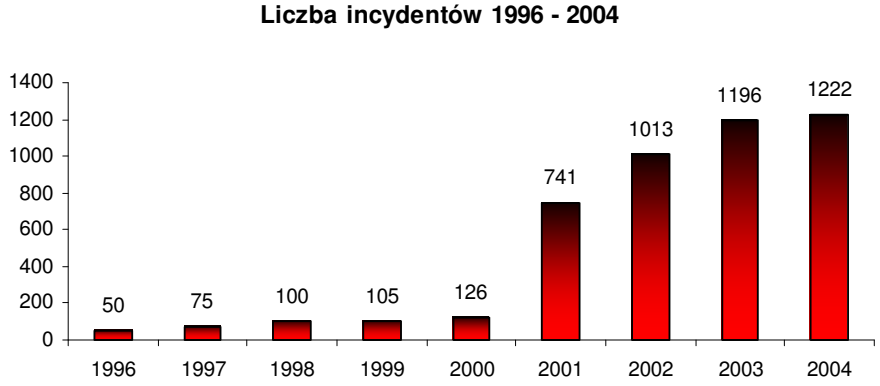
4.1 Najważniejsze zmiany w stosunku do roku ubiegłego

Rok 2004 jest drugim z kolei rokiem, w którym wykorzystaliśmy klasyfikację eCSIRT.net (patrz rozdział 2). Pozwala to na dokładne porównanie statystyk z dwóch ostatnich lat. W roku 2004 odnotowaliśmy kilka istotnych zmian w stosunku do roku 2003, a także utrzymanie się niektórych istotnych trendów. Poniżej przedstawiamy te, które są naszym zdaniem najważniejsze:

- Nastąpił ponad dwukrotny wzrost liczby incydentów dotyczących złośliwego kodu (a w szczególności robaków sieciowych) - z 6,7% do 13,5%;
- Prawie czterokrotnie wzrosła liczba ataków DoS i DDoS – z 1,7% do 6,3%;
- Niemalże pięciokrotnie wzrosła liczba *oszustw komputerowych* – z 1,8% do 8,4%, co wiąże się ze znacznym wzrostem zgłoszeń dotyczących *phishingu* oraz naruszania praw autorskich;
- Nadal decydującą rolę w zgłaszaniu incydentów odgrywają zespoły reagujące (CSIRT) – 53,3% w minionym roku i 51,5% w roku 2003;
- Coraz mniej zgłoszeń pochodzi z zespołów typu *Abuse*, coraz więcej od użytkowników indywidualnych i firm komercyjnych;
- Coraz więcej zgłoszeń incydentów pochodzi z Polski. Mimo to, nadal przeważają zgłoszenia z zagranicy – 72,3% w roku 2004, 89,6% w roku 2003.

4.2 Liczba incydentów w latach 1996 – 2004

Poniższy wykres przedstawia liczbę incydentów w latach 1996 – 2004



Jak widać w ostatnich latach liczba ta nie rośnie gwałtownie. Niestety nie odpowiada to rzeczywistym trendom. Wzrost liczby incydentów naruszających bezpieczeństwo w sieci jest z pewnością większy niż przedstawiają to słupki na wykresie. Główną przyczyną rozbieżności pomiędzy danymi statystycznymi, a tym co obserwujemy w rzeczywistości jest fakt, że przeważająca większość obecnych ataków odbywa się w sposób automatyczny. Tego typu ataki przez wielu uznane zostały jako „szum sieciowy" - coś, z czym należy się pogodzić, a tym samym nie ma sensu zgłaszać do jednostek reagujących, zwłaszcza jeśli nie zostały poniesione istotne straty. Zdecydowana większość zgłoszeń dotyczących zautomatyzowanych ataków pochodzi od wyspecjalizowanych jednostek, które rozwinęły systemy ich detekcji i reagowania na nie (patrz zestaw instytucji w rozdziale 0). Również nasz zespół przystąpił do aktywnej obserwacji tego, co się dzieje w sieci. We wrześniu roku 2004 uruchomiony został serwis arakis.cert.pl, który prezentuje osiągnięcia systemu AgRegacji, Analizy i Klasyfikacji Incydentów

Sieciowych – ARAKIS (http://arakis.cert.pl/). Jednym z celów tego projektu jest identyfikacja źródeł najpoważniejszych ataków w sieci i próba ich wyeliminowania. System ten będzie najprawdopodobniej źródłem informacji, o konkretnych incydentach w roku 2005.

4.3 Najważniejsze trendy i zjawiska obserwowane w roku 2004

Poniższe zestawienie stanowi naszym zdaniem najbardziej istotne trendy i zjawiska zaobserwowane w roku 2004 w dziedzinie bezpieczeństwa TI:

- Szczególnej siły nabrały zagrożenia dystrybuowane w sposób automatyczny, czego najlepszym dowodem jest dramatyczny wręcz wzrost informacji dotyczących funkcjonowania rozproszonych sieci, poprzez które steruje się masowymi atakami (np.: atakami DDoS) – czyli tzw. Botnetów;

- Wzrosła aktywność wirusów (szczególnie niebezpiecznymi były MyDoom, Beagle czy Netsky). Wirusy te powodowały masowe ataki DDoS i wręcz "walczyły" ze sobą, np. przez deinstalację konkurenta po infekcji. Oprócz standardowego dołączania załącznika, do zarażania używały także metod socjotechnicznych;

- Nowości w świecie robaków sieciowych - m.in. robak Witty, który pojawił się w sieci po dwóch dniach od opublikowania informacji o luce, którą wykorzystywał – jest doskonałym reprezentantem zjawiska polegającego na wyraźnym skracaniu się czasu pomiędzy opublikowaniem informacji o luce systemowej, a jej wykorzystaniem. Innym robakiem, który spowodował wiele strat był Sasser, wykorzystujący słabość znalezioną w usłudze LSASS (Local Security Authority Subsystem Service), kolejny to Dabber, który wykorzystywał błąd popełniony w kodzie Sassera i był prawdopodobnie pierwszym w historii robakiem wykorzystującym lukę w innym robaku sieciowym;

- Intensywny rozwój zjawiska *phishingu -,* w przypadku tego zjawiska mieliśmy do czynienia z połączeniem technik znanych z dystrybucji spamu z socjotechniką. Wiele ofiar *phishingu* poniosło wymierne straty finansowe. Techniki użyte przy phishingu i spamie oparte są z kolei o sieci zbudowane często za pomocą robaków sieciowych i wirusów. Wszystkie te zjawiska łączą się ze sobą. Potwierdzają to ubiegłoroczne obserwacje, że zagrożenia w sieci są coraz bardziej skomplikowane i tworzą rozbudowaną sieć powiązań oraz połączeń technik ataków komputerowych. Za rozwojem tego typu zagrożeń stoją przestępstwa komputerowe na dużą skalę, z których czerpane są coraz większe nielegalne zyski;

- Wzrost problemu występowania w sieci nielegalnych treści, a w szczególności pornografii dziecięcej. Z racji specyfiki tego zjawiska w NASK powołano do istnienia zespół NIFC Hotline Polska http://www.hotline.org.pl.

5 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