CERT Polska

Raport 2005

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2005

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.

Zespół CERT Polska podejmuje różne inicjatywy na rzecz poprawy stanu bezpieczeństwa Internetu w Polsce. W październiku 2005 roku zaprosiliśmy „do wspólnego stołu" przedstawicieli zespołów bezpieczeństwa, zajmujących się reagowaniem na incydenty w sieci , funkcjonujących w ramach polskich firm teleinformatycznych i telekomunikacyjnych. W spotkaniu brali udział specjaliści reprezentujący firmy: ASTER, Exatel, Poznańskie Centrum Superkomputerowo-Sieciowe (Pionier-CERT), PKP Informatyka, Polkomtel, PSE, Telekomunikacja Polska, Telekomunikacja Kolejowa, UPC i VECTRA. Uczestnicy wyrazili wolę współpracy, której celem będzie synchronizacja działań oraz inicjatywy w postaci wspólnych projektów bądź akcji na rzecz poprawy bezpieczeństwa polskiego Internetu.

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 trzeci 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 2005 odnotowaliśmy 2516 incydentów. W następnych rozdziałach znajduje się szczegółowa klasyfikacja zgłoszonych do nas incydentów.

3.2 Typy odnotowanych incydentów

Rok 2005 był rokiem szczególnym z punktu widzenia obsługi incydentów przez zespół CERT Polska, ze względu na uruchomienie nowego narzędzia do raportowania incydentów, jakim stał się system ARAKIS po dodaniu nowych funkcjonalności. W związku z tym tegoroczne statystyki są jakościowo inne od statystyk z lat poprzednich.

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

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 precyzyjny opis incydentu, z jakim mieliśmy do czynienia.

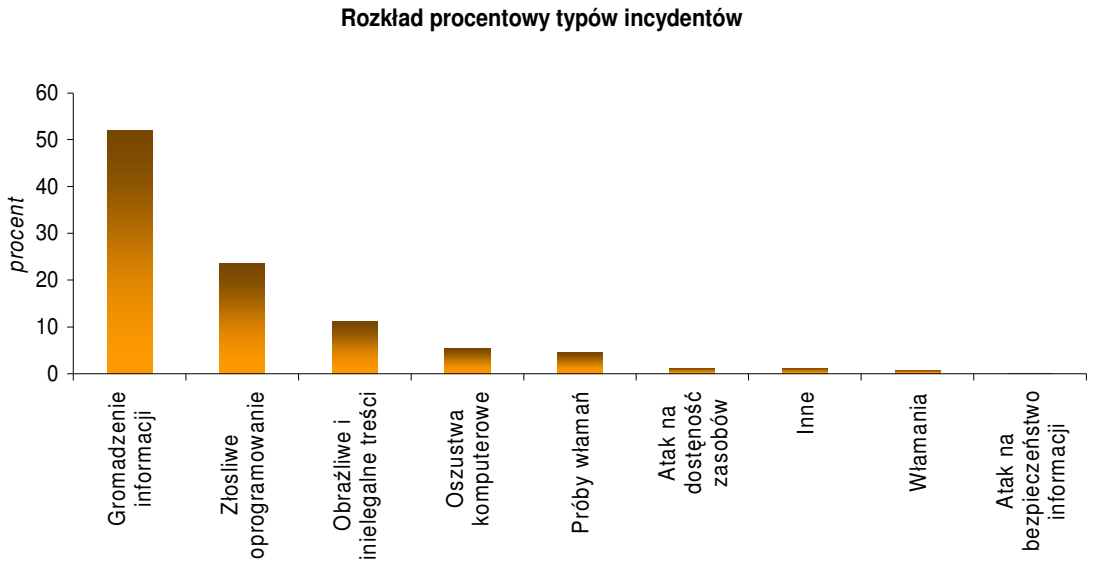
Typ/Podtyp incydentu	Liczba	Suma-typ	Procent-typ
Obraźliwe i nielegalne treści	0	283	11,2
Spam	275		
Dyskredytacja, obrażanie	8		
Pornografia dziecięca, przemoc[3]	0		
Złośliwe oprogramowanie	1	594	23,6
Wirus	11		
Robak sieciowy	462		
Koń trojański	117		
Oprogramowanie szpiegowskie	0		
Dialer	3		
Gromadzenie informacji	0	1305	51,9
Skanowanie	1292		
Podsłuch	6		
Inżynieria społeczna	7		
Próby włamań	0	117	4,6
Wykorzystanie znanych luk systemowych	18		
Próby nieuprawnionego logowania	99		
Wykorzystanie nieznanych luk systemowych	0		
Włamania	0	18	0,7
Włamanie na konto uprzywilejowane	9		
Włamanie na konto zwykłe	7		
Włamanie do aplikacji	2		
Atak na dostępność zasobów	0	28	1,2
Atak blokujący serwis (DoS)	13		
Rozproszony atak blokujący serwis (DDoS)	14		
Sabotaż komputerowy	1		
Atak na bezpieczeństwo informacji	0	3	0,1
Nieuprawniony dostęp do informacji	2		

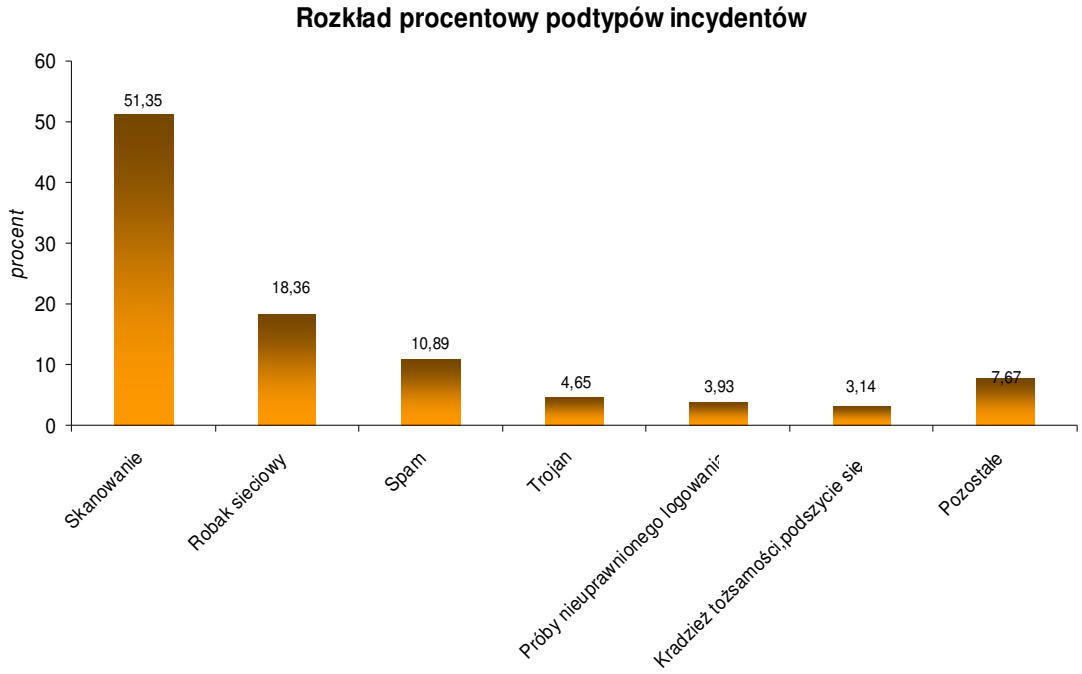
[3] Wszelkie zgłoszenia dotyczące nielegalnych treści, w rozumieniu polskiego prawa, przekierowywane są do zespołu Dyżurnet.pl, również działającego w ramach NASK (http://www.dyzurnet.pl/)

Nieuprawniona zmiana informacji	1		
Oszustwa komputerowe	1	137	5,5
Nieuprawnione wykorzystanie zasobów	26		
Naruszenie praw autorskich	31		
Kradzież tożsamości, podszycie się (w tym Phishing)	79		
Inne	31	31	1,2
SUMA	2516	2516	100,0

3.3 Typy odnotowanych ataków

Poniższe wykresy przedstawiają rozkład procentowy typów i podtypów incydentów.





W roku 2005 najczęściej występującym typem incydentu było *gromadzenie informacji* (51,9%), a w szczególności *skanowanie* (aż 51,35%). Niebagatelny wpływ na taki wynik miało dodanie do zbudowanego przez zespół CERT Polska systemu ARAKIS <http://arakis.cert.pl/> funkcjonalności pozwalającej wykrywać, i raportować do systemu obsługi zgłoszeń, próby zauważonych przez niego ataków. Coraz rzadziej napotyka się skanowania „ręcznie sterowane" przez intruza. Ogromna większość to skanowania powodowane przez robaki lub botnety. Dzięki korelacji zgłoszeń z danymi udostępnionymi przez system ARAKIS udało się zauważyć bardzo ciekawe zjawisko „skanowania rozproszonego" powodowane przez botnety. Polega ono na tym, że w celu ukrycia prób gromadzenia informacji, sieci są skanowane przez „armię" np. 1000 zombies (czyli komputerów kontrolowanych przez atakującego), przy czym każdy z nich skanuje tylko niewielki fragment atakowanej sieci (rzędu kilku hostów). Ten typ skanowania jest także rozłożony w czasie. Przy stosowaniu „standardowych" metod wykrywania ataków ten typ (podtyp) jest zazwyczaj niezauważony (lub bagatelizowany) przez atakowanego.

Drugim, co do liczebności typem incydentów były przypadki działania *złośliwego oprogramowania* (23,6%) przy czym najczęściej mieliśmy do czynienia z *robakami sieciowymi* (18,36%). Zauważalna jest tendencja do zacierania się granic pomiędzy robakiem, wirusem, koniem trojańskim a oprogramowaniem szpiegowskim. Robaki sieciowe coraz częściej posiadają funkcjonalności typowe dla pozostałych rodzajów złośliwego oprogramowania.

Do grona najliczniejszych kategorii należy również zaliczyć *Obraźliwe i nielegalne treści* (11,2%) ze szczególnym uwzględnieniem *spamu* (10,89%). Najczęściej jest to spam rozsyłany za pośrednictwem skompromitowanej maszyny, bez wiedzy jej właściciela. Równie często intruz wykorzystuje fakt błędnej konfiguracji usług udostępnianych przez serwery (np. spam rozsyłany z wykorzystaniem „open proxy").

Spamerzy używają coraz bardziej wyrafinowanych technik, aby utrudnić rozpoznanie prawdziwego źródła rozsyłania niechcianej korespondencji. Przypadki zarejestrowane przez CERT Polska dotyczą wyłącznie wyjątkowo uciążliwego spamu, zgłaszanego bezpośrednio przez poszkodowanego. W rzeczywistości skala zjawiska jest o wiele większa.

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	368	**14,6**	368	**14,6**	148	**5,9**
CERT[4]	1808	**71,9**	0	**0**	0	**0**
ISP Abuse	8	**0,3**	0	**0**	0	**0**
Inna instytucja ds. Bezpieczeństwa	130	**5,2**	0	**0**	0	**0**
Firma komercyjna	113	**4,5**	1336	**53,1**	676	**26,9**
Ośrodek badawczy lub edukacyjny	27	**1,1**	145	**5,8**	347	**13,8**
Instytucja niekomercyjna	13	**0,5**	91	**3,6**	59	**2,3**
Jednostka rządowa	8	**0,3**	197	**7,8**	17	**0,7**
Nieznany	41	**1,6**	379	**15,1**	1269	**50,4**
Kraj	2140	**85**	2124	**84,4**	1702	**67,6**
Zagranica	347	**13,8**	203	**8**	144	**5,7**
Nieznany	29	**1,2**	189	**7,6**	670	**26,7**

Najaktywniej zgłaszającym incydenty były *zespoły reagujące* (71,9%). Innymi istotnymi źródłami zgłaszania incydentów były O*soby Prywatne* (14,6%), *Inne Instytucje ds. Bezpieczeństwa* (5,2%) oraz *Firmy Komercyjne* (4,5%). W celu usprawnienia obsługi incydentów, zespół CERT Polska udostępnił formularz

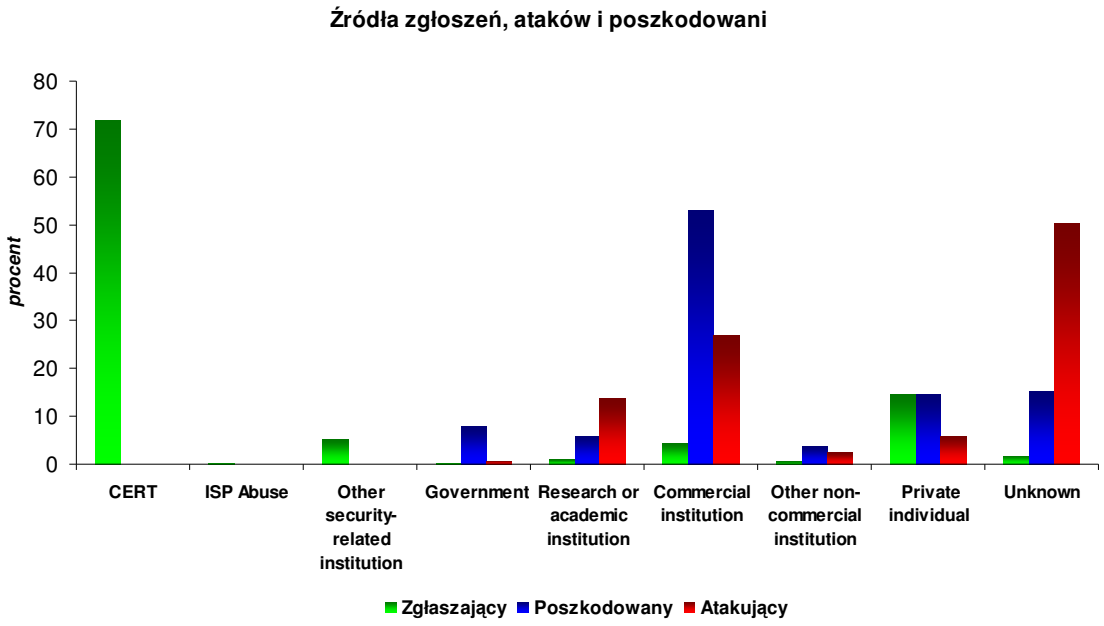
[4] Zawiera zgłoszenia pochodzące z systemów automatycznych, w tym także z systemu ARAKIS

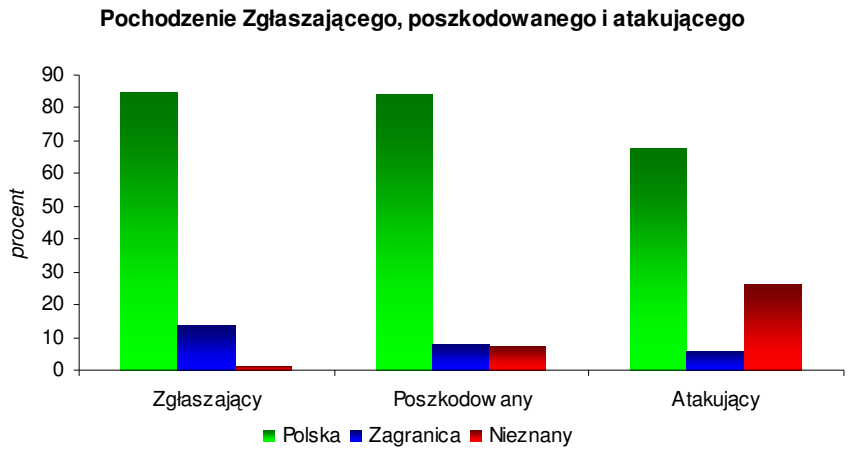
online do ich zgłaszania <https://www.cert.pl/formularz/formularz.php>. Zauważyliśmy, że intuicyjny interfejs oraz ograniczenie do minimum niezbędnych operacji do wysłania zgłoszenia, wpływa na zwiększenie aktywności *Osób Prywatnych* jako zgłaszających.

W kategorii *Poszkodowany* najwyższy odsetek stanowi grupa *Firm Komercyjnych* (53,1%). Drugą najczęściej poszkodowaną grupą użytkowników sieci były *Osoby Prywatne* (14,6%). Niestety aż 15,1% poszkodowanych nie zostało rozpoznanych. Istnieją dwie główne przyczyny takiego stanu rzeczy. Po pierwsze zgłoszenia są składane przez operatorów oraz zespoły reagujące w czyimś imieniu (bez podania poszkodowanego). Po drugie, grupa poszkodowanych w wyniku jednego incydentu może być bardzo duża, począwszy od *Osób Prywatnych* poprzez *Ośrodki badawcze i edukacyjne,* a kończąc na *Firmach Komercyjnych*.

Wśród *Atakujących* największą grupę stanowią *Nieznani* sprawcy (50,4%). Sytuacja taka wynika z faktu, że atakujący zazwyczaj korzysta z „pośrednika", jakim jest np. serwer proxy, botnet czy skompromitowany host nieświadomego użytkownika. Takiego sprawcę trudno jest zidentyfikować. Dość często *Atakującym* okazywała się *Firma Komercyjna* (26,9%). Coraz większa dostępność Internetu zachęca małe firmy komercyjne do jego wykorzystania. Nie zawsze jednak wiąże się to z zaimplementowaniem odpowiednich polityk bezpieczeństwa. Poza wymienionymi podmiotami zauważalna była również aktywność *Ośrodków Badawczych lub Edukacyjnych* (13,8%), czyli w praktyce szkół i uczelni wyższych, oraz w mniejszym stopniu *Osób prywatnych* (5,9%).

Jeśli chodzi o klasyfikację dotyczącą źródła pochodzenia w rozumieniu geograficznym, to znacznie wzrósł odsetek incydentów „polskich". W przeważającej większości zarówno *zgłaszający, poszkodowany i atakujący* pochodził z Polski (odpowiednio: 85%, 84,4%, 67,6%). Niestety nadal zdarzają się przypadki, w których nieznane jest pochodzenie *Poszkodowanego* (7,6%) oraz *Atakującego* (26,7%).





4 Wnioski i trendy

4.1 Najważniejsze zmiany w stosunku do roku ubiegłego

W roku 2005 system ARAKIS po dodaniu nowych funkcjonalności, stał się źródłem raportowania incydentów. Fakt ten miał niewątpliwie duży wpływ na kształt tegorocznych statystyk. Ponieważ system ARAKIS zgłasza de facto próby skanowania hostów, staraliśmy się zakwalifikować każdą z tych prób jako: skanowanie, działalność trojana lub robaka.

W roku 2005 powstał również nowy formularz zgłoszeniowy. Za główny cel postawiliśmy sobie uproszczenie i ułatwienie procesu zgłoszenia incydentu. Zmniejszyliśmy liczbę wymaganych danych oraz staraliśmy się stworzyć jak najbardziej intuicyjny i przejrzysty interfejs. Działania te spowodowały zwiększenie ilości zgłoszeń od osób prywatnych.

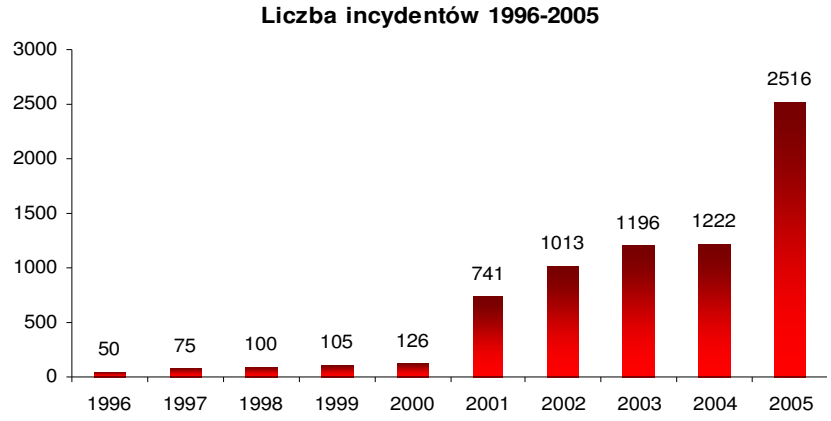
Odnotowaliśmy kilka istotnych zmian w stosunku do roku 2004, ale także utrzymanie się niektórych istotnych trendów. Poniżej przedstawiamy te obserwacje, które są naszym zdaniem najważniejsze:

- Nadal najczęściej występującym incydentem było skanowanie 51,35%
- Nastąpił prawie dwukrotny wzrost liczby incydentów dotyczących złośliwego oprogramowania (w szczególności robaków sieciowych i trojanów) – z 13,5% do 23,6%;
- Ponad pięciokrotnie zmalała liczba ataków DoS i DDoS – z 6,3% do 1,2%.
- Prawie dwukrotnie częściej dokonywano prób włamań – wzrost z 2,5% do 4,6%, ze wskazaniem na próby nieuprawnionego logowania.

- Nadal decydującą rolę w zgłaszaniu incydentów odegrały zespoły typu CERT[5] – 71,9% zgłoszeń.
- Zmalał odsetek zgłoszeń od zespołów typu *Abuse* – z 4,6% do 0,3%.
- Użycie systemu automatycznego raportowania naruszeń bezpieczeństwa wpłynęło na zwiększenie liczby incydentów powiązanych z polskim użytkownikiem sieci jako poszkodowanym.
- Znacznie wzrosła liczba poszkodowanych wśród firm komercyjnych – *z 12,3% do 53,1%.*
- Wzrosła liczba incydentów, w których nie można ustalić pochodzenia atakującego – z 20% do 26,7%.

4.2 Liczba incydentów w latach 1996 – 2005

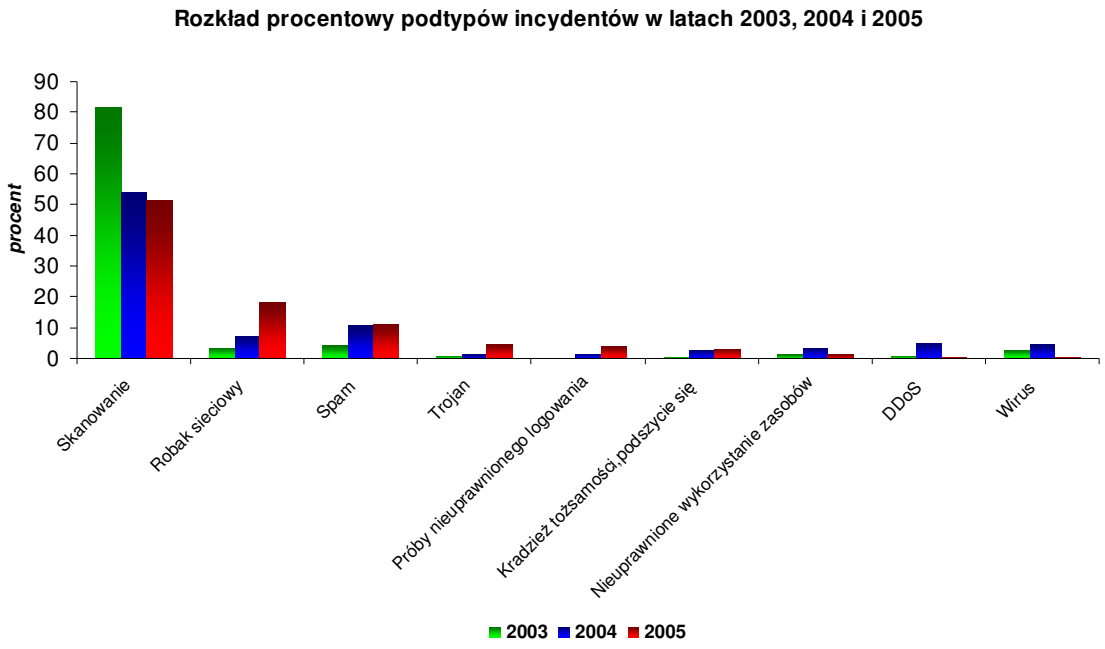
Poniższy wykres przedstawia liczbę incydentów w latach 1996 – 2005



Jak widać liczba incydentów wzrosła ponad dwukrotnie w stosunku do roku 2004. Jest to w głównej mierze wynik obsługi zgłoszeń generowanych przez system ARAKIS. Pomimo tego nie jest to jednak liczba w pełni odzwierciedlająca skalę zjawiska. Zdajemy sobie sprawę, że wiele incydentów jest bagatelizowanych lub niezauważonych przez potencjalną ofiarę. Wiele prób skanowania pozostaje niewykrytych w wyniku ich rozproszenia na wiele maszyn oraz w długim okresie czasu. Duża grupa osób rezygnuje ze zgłaszania incydentów ze względu na brak reakcji ze strony odpowiedzialnych za atakujące hosty czy sieci. Niemniej jednak, utrzymuje się tendencja wzrostowa notowanych incydentów i należy się spodziewać wzrostu zgłoszeń w latach następnych.

[5] W tym zgłoszenia pochodzące z systemów automatycznych oraz systemu ARAKIS

4.3 Rozkład procentowy podtypów incydentów w latach 2003-2005.



Ponieważ od 2003 roku tworzymy statystyki opierając się o tę samą klasyfikację, możliwe jest porównanie rozkładu procentowego incydentów występujących na przestrzeni ostatnich trzech lat. Przez cały ten okres mieliśmy najczęściej do czynienia z przypadkami *skanowania sieci*. Tendencja spadkowa nie wynika bynajmniej z coraz mniejszej liczby prób *skanowania*, lecz z faktu zakwalifikowania ich jako działalność *robaka* lub *trojana* (bardziej precyzyjna klasyfikacja była możliwa dzięki danym z systemu ARAKIS). W związku z powyższym wzrósł procent incydentów powodowanych przez *robaki sieciowe* i *trojany*. Dostrzegalna jest tendencja wzrostowa liczby rozsyłanego spamu - w rzeczywistości jest ona jednak znacznie silniejsza.

Reasumując, przez cały okres stosowania klasyfikacji e_CSIRT.net , największy udział procentowy miały incydenty będące wynikiem *skanowania,* działalności *robaków* oraz rozsyłania *spamu*. Reszta podtypów jest reprezentowana w statystykach znacznie słabiej.

4.4 Najważniejsze trendy i zjawiska obserwowane w roku 2005

Poniżej przedstawiamy najbardziej istotne naszym zdaniem trendy i zjawiska, występujące w roku 2005, wynikające zarówno z obsługi incydentów, jak i z innych obserwacji poczynionych przez CERT Polska:

- Widoczna jest zmiana w wykorzystywaniu botnetów. Coraz rzadziej są one źródłem ataków DoS i DDoS, za to coraz częściej stają się narzędziem do czerpania nielegalnych zysków, rozsyłania spamu czy przejmowania numerów kart kredytowych i kont bankowych (np. *phishing*).

- Nadal na bardzo wysokim poziomie utrzymywała się aktywność robaków internetowych.

- Spamerzy stosują coraz wymyślniejsze techniki, aby ukryć pochodzenie prawdziwego nadawcy niechcianej korespondencji. Nierzadko powoduje to generowanie fałszywych alarmów (nawet przez doświadczone organizacje antyspamerskie).

- Ciągle bolesny jest brak zabezpieczeń oraz profesjonalnego zarządzania sieciami w wielu firmach, które często nie zdają sobie sprawy z niebezpieczeństw wynikających z dostępu do Internetu.

- Coraz większy problem stanowi brak reakcji wielu operatorów i dostawców usług, na np. uporczywe próby skanowania sieci, będące ewidentnym wynikiem działalności robaków sieciowych.

- Działania hakerów są coraz bardziej zaawansowane, a wykorzystywane mechanizmy coraz bardziej skomplikowane.

- Zauważalny jest nowy trend propagacji robaków poprzez luki w aplikacjach WWW. Jako metoda wyboru celu wykorzystywane są, poza klasycznym skanowaniem sieci, popularne wyszukiwarki Internetowe takie jak Google, które wyszukują strony WWW z potencjalnie dziurawym oprogramowaniem. Głównym celem są aplikacje open source bazujące na PHP i Perl.

- Pojawiło się dużo ataków „brute force" na SSH, powodowanych przez automaty oraz robaki.

- Komunikatory zaczynają być wykorzystywane do propagacji malware'u (z dużą skutecznością). Trudno kontrolować tego typu działania.

5 Kontakt

Zgłaszanie incydentów:	cert@cert.pl, spam: spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	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 3808 274
fax:	+48 22 3808 399