CERT POLSKA

Raport 2001

Przypadki naruszające bezpieczeństwo teleinformatyczne

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), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). Od roku 2000 członkiem europejskiej inicjatywy zrzeszającej zespoły reagujące – Trusted Introducer[1]. 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 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

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 szóstym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.pl/ -> Opracowania CERT Polska -> Raporty)

[1] 22 listopada 2001 zespół uzyskał najwyższy poziom zaufania Trusted Introducer Level 2.

3 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[2]

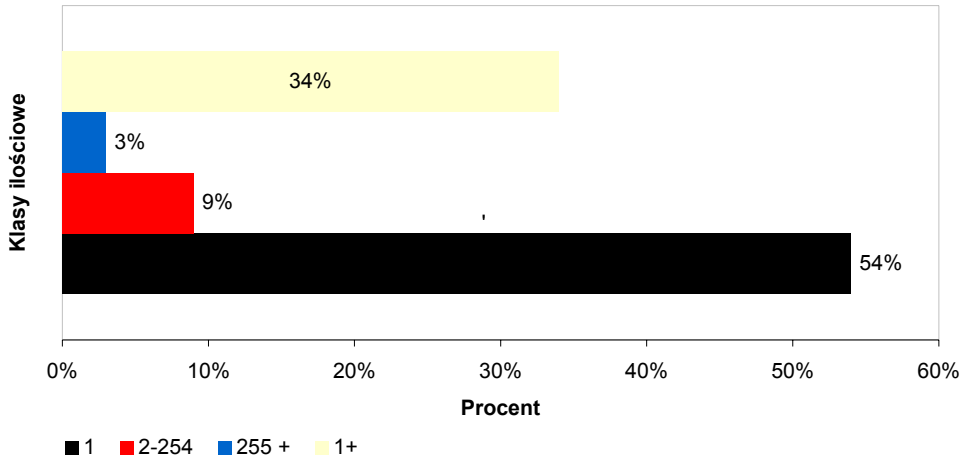
3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2001 odnotowano 741PNBT.

3.2 Liczba zaatakowanych komputerów

Wśród stwierdzonych PNBT odnotowaliśmy wiele takich, w trakcie których przeprowadzono atak na więcej niż jeden komputer czy inny obiekt sieciowy. W statystyce rodzajem „1+" określono te wszystkie przypadki kiedy wiadomo było, że liczba zaatakowanych komputerów była większa niż jeden, jednak nie było możliwe ustalenie konkretnej wartości.

Mimo tego w ponad 50% przypadków mieliśmy do czynienia z atakiem na jeden komputer.



Rysunek 1 **- Liczba zaatakowanych komputerów w trakcie jednego ataku**

3.3 Typy odnotowanych ataków

Począwszy od 2001 roku CERT Polska rozpoczął klasyfikację incydentów zgodnie z propozycją John'a D.Howard'a i Thomas'a A.Longstaff'a, znaną pod nazwą „Common Language"[3] .

Dodatkowo, aby dobrze scharakteryzować rozkład rodzajów ataków w kontekście najbardziej popularnych ataków, przygotowaliśmy skróconą statystykę najczęściej odnotowywanych ataków szczegółowych, takich jak chociażby najbardziej znane wirusy (3.3.2).

---

[2] W dalszej części raportu przypadki naruszenia bezpieczeństwa teleinformatycznego określane będą skrótem PNBT

[3] Wszystkich zainteresowanych szczegółami tej klasyfikacji odsyłamy do publikacji *Common Language (http://www.cert.org/research/taxonomy_988667.pdf)*

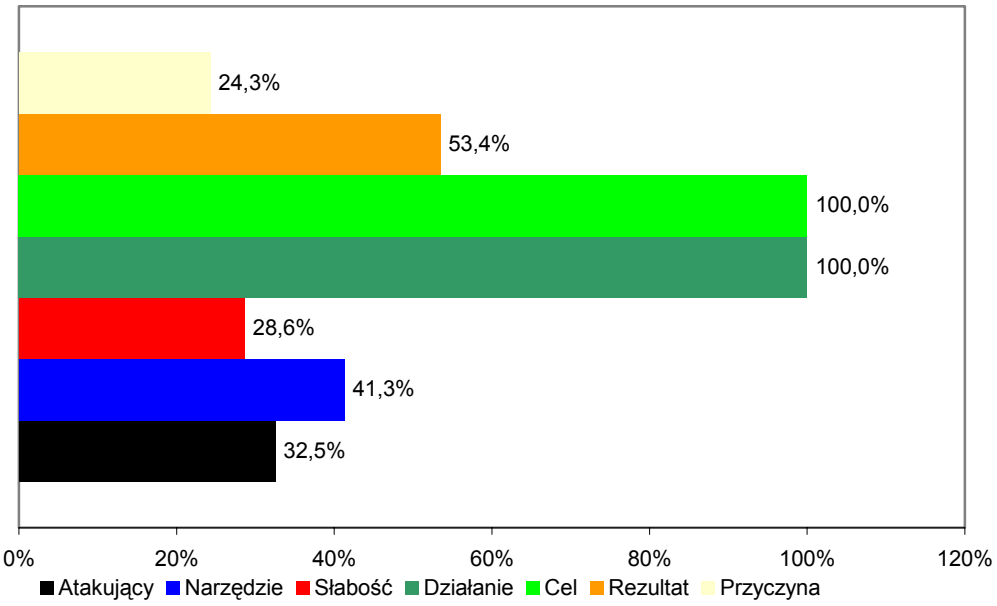
3.3.1 Klasyfikacja incydentów wg *Common Language*

Przypadki, w czasie obsługi których, można było zgromadzić dane pozwalające na wypełnienie wszystkich cech PNBT stanowią około 9%.

Należy zwrócić uwagę, że klasyfikacja *Common Language* z założenia jest klasyfikacją kompletną, dlatego zawiera również kategorie, które właściwie nie są zupełnie zgłaszane do zespołów reagujących podobnych do takiego jakim jest zespół CERT Polska (np.: ataki fizyczne). Niemniej jednak dla porządku i pełnego obrazu, w naszych statystykach nie pomijamy tych kategorii.

Poniższy wykres przedstawia w ilu przypadkach udało się ustalić daną cechę PNBT.

Najbardziej podstawową formą ataku komputerowego jest tzw. zdarzenie (*ang. event*). Cechami charakteryzującymi *zdarzenie* są *działanie (action)* jakie podjął intruz oraz *cel (target)* jaki zaatakował. W związku z tym wszystkie przypadki muszą i mają określone te dwie cechy.

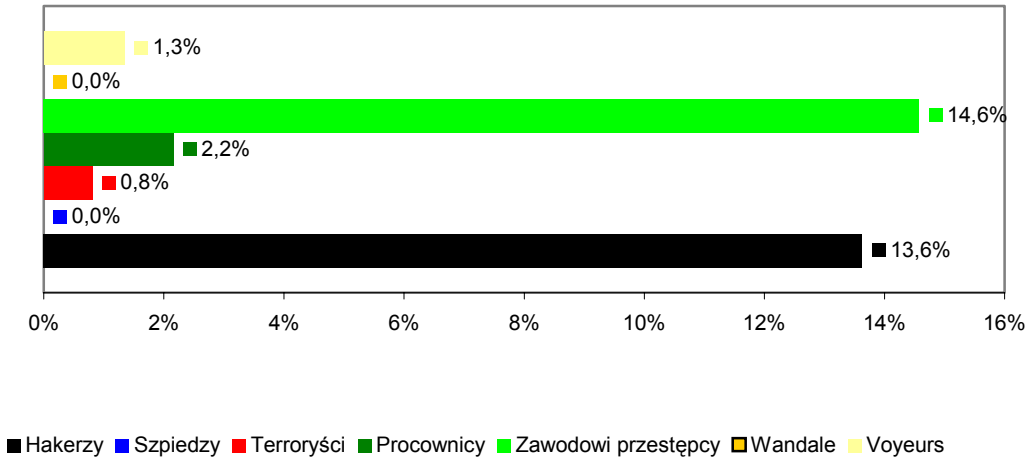


Rysunek 2 – Procent ustalenia poszczególnych cech PNBT.

Poniższe podpunkty pokazują rozkład procentowy w poszczególnych cechach opisujących PNBT

3.3.1.1 Atakujący[4]

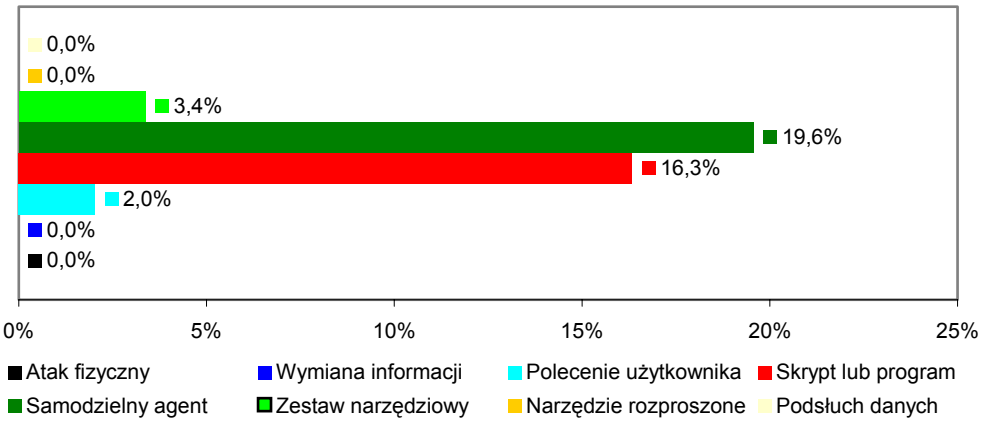
Na poniższym wykresie widzimy rozkład procentowy związany z kategorią „atakujący". Dwie najważniejsze grupy to hakerzy i zawodowi przestępcy. Termin „zawodowy przestępca" należy traktować umownie. W rzeczywistości w tej kategorii znaleźli się wszyscy, którzy rozsyłają niezamawianą korespondencję.



Rysunek 3 - Klasyfikacja atakujących

3.3.1.2 Narzędzia

Dla tej cechy związanej z PNBT zdecydowanie najwięcej jest przypadków, w których użyte zostały narzędzia określane jako „samodzielny agent" albo „skrypt lub program". Pierwsze z nich są związane z masowymi atakami wirusów (Code Red, Nimda), zaś drugie z przypadkami skanowania i rozsyłania niezamawianej poczty elektronicznej.

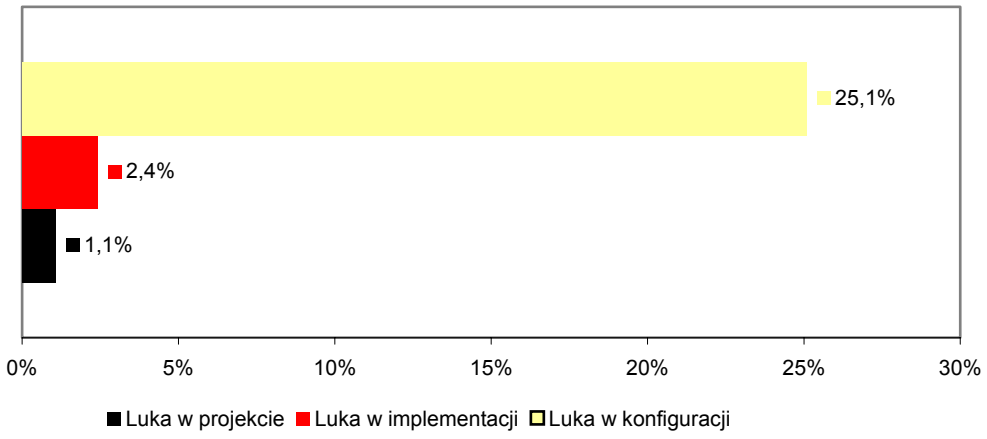


[4] W tej kategorii nie zostało przetłumaczone pojęcie *voyeur*s, ze względu na jego specyficzne znaczenie i brak jednoznacznego odpowiednika w języku polskim.
Voyeurs - *Atakujący, którzy atakują komputery dla podniecenia wywołanego uzyskaniem niejawnych informacji.*

Rysunek 4 - Klasyfikacja używanych narzędzi ataku

3.3.1.3 Atakowana słabość systemu

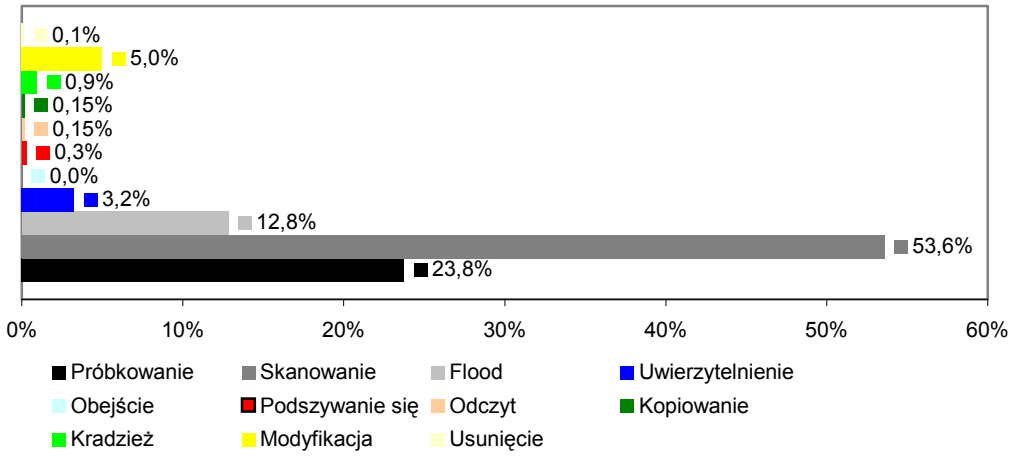
Luka w konfiguracji systemów komputerowych jest zdecydowanie najczęstszą przyczyną ataków komputerowych. Z doświadczeń CERT Polska wynika, że znacznie rzadszą przyczyną są luki w implementacji i zaprojektowaniu systemu. Zapewne przyczyną takiego a nie innego wyglądu tej statystyki jest stosowanie automatycznych narzędzi przez *script kiddies*, które to narzędzia (patrz również 5v) zazwyczaj są nastawiane na wykorzystanie luk w konfiguracji.



Rysunek 5 - Klasyfikacja wykorzystania poszczególnych luk w systemie

3.3.1.4 Nieautoryzowane działanie

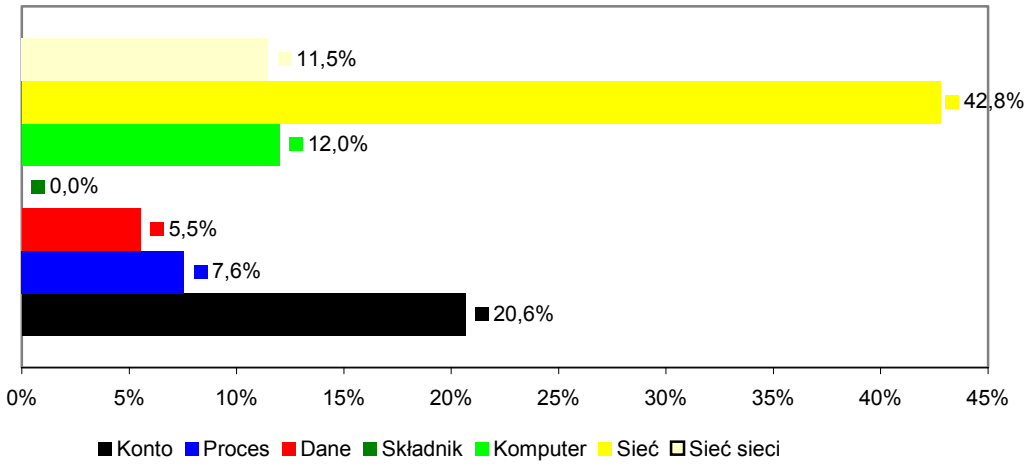
Zdecydowanie największy procent nieautoryzowanego działania stanowią przypadki próbkowania i skanowania. Wśród tych przypadków również znajdują się ataki powiązane z robakami internetowym (Code Red, Nimda). Odnotowane przypadki nieautoryzowanego *uwierzytelnienia i modyfikacji*, powiązane są zazwyczaj z przypadkami włamania, a czasami włamania połączonego z podmianą strony WWW.



Rysunek 6 - Nieautoryzowane działanie podejmowane przez atakującego

3.3.1.5 Cel ataku

Cel ataku jest drugą podstawową cecha opisującą PNBT. Najczęściej, wśród PNBT w roku 2001, celem ataku były całe sieci lub nawet sieci sieci (*internetworks*), co wynika z popularności przypadków skanowania. Naruszenie bezpieczeństwa *składnika* infrasruktury, jest w rzeczywistości atakiem fizycznym, tego typu ataki nie są zgłaszane do CERT Polska.

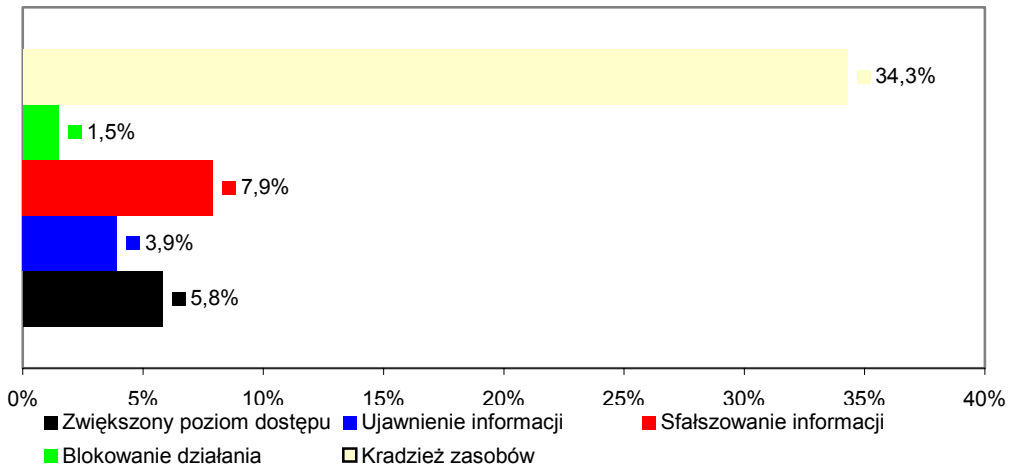


Rysunek 7 - Cel ataku

3.3.1.6 Rezultat

Wśród rozpoznanych skutków działania intruzów zdecydowanie na pierwszy plan wysuwa się *kradzież zasobów*. Dwa podstawowe przypadki wpływające na taki stan rzeczy to kradzież zasobów rozumianych jako moc obliczeniowa oraz rozumianych jak praca ludzka.

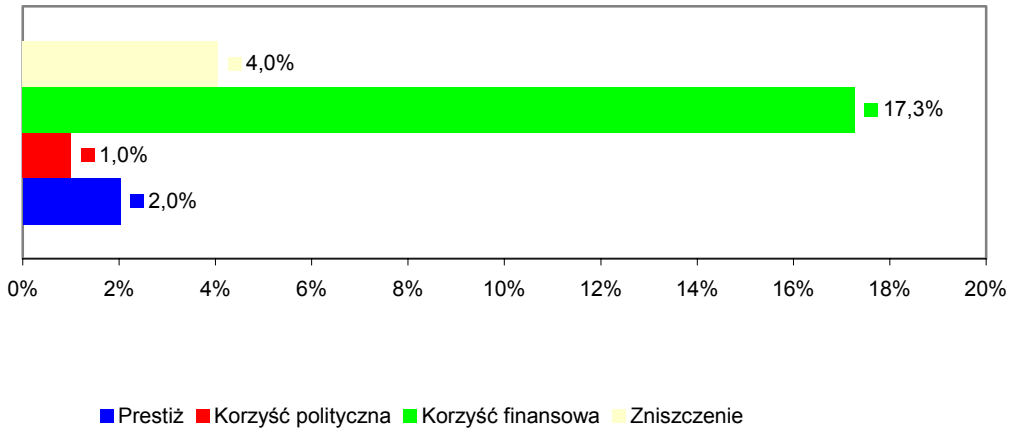
W pierwszym przypadku do nadużycia dochodzi w momencie wystąpienia ataków typu *Denial of Service* oraz co bardziej skomasowanych przypadków skanowania, zaś w drugim głównie w przypadku rozsyłania nie zamawianej korespondencji (*spam*), którego skutkiem działania jest swoista kradzież zasobów ludzkich poświęcanych na likwidację skutków spam'u.



Rysunek 8 - Rezultat przeprowadzonego ataku

3.3.1.7 Przyczyna

Przyczynę, która decydowała o wystąpieniu PNBT jest bardzo trudno ustalić, dlatego procent odpowiedzi na pytanie *Co było przyczyną działalności intruza?* jest niewielki. Właściwie możliwe jest to tylko w momencie rozpoznania całego incydentu i szczegółowego dochodzenia. Z takimi przypadkami w trakcie standardowych działań zespołu mamy do czynienia bardzo rzadko. Właściwie jedynym nie budzącym wątpliwości, co do przyczyn, przypadkiem jest spam. Rozsyłanie niezamawianej korespondencji niemalże w 100% powiązane jest z chęcią uzyskania korzyści finansowej, znacznie rzadziej z chęcią osiągnięcia celów politycznych (np.: propagandę)

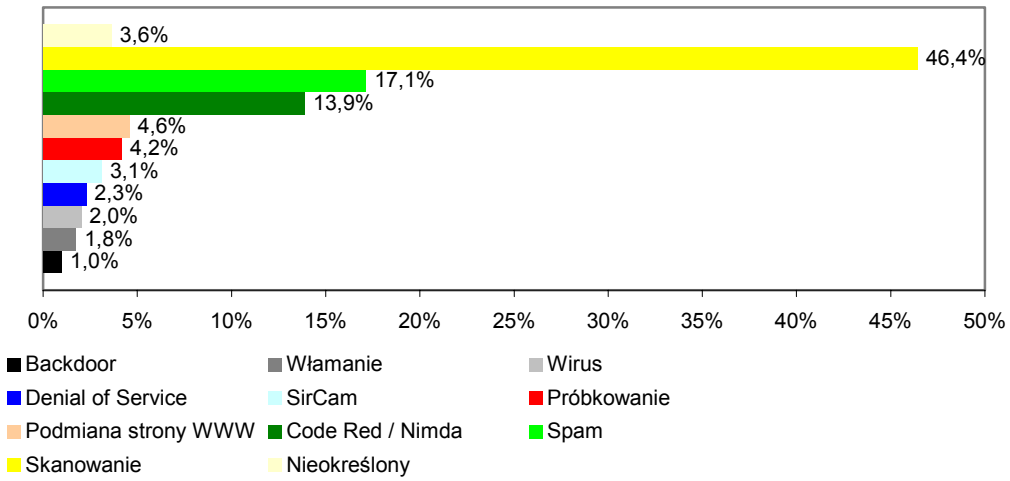


Rysunek 9 - Przyczyna ataku

3.3.2 Klasyfikacja wg charakterystycznych ataków

W celu uzupełnienia formalnej statystyki *Common Language* zamieszczamy również dodatkowe zestawienie, w którym można odnaleźć niektóre charakterystyczne kategorie, których nie ma w klasyfikacji *Common Language*

Poniższy wykres przedstawia charakterystyczne rodzaje ataków w roku 2001



Rysunek 10 - Charakterystyczne rodzaje ataków

Jak widać z powyższego wykresu obserwujemy wyraźną przewagę różnego rodzaju skanowania i próbkowania, które łącznie stanowiły ponad 50 % (50,6) obsługiwanych przypadków. Znaczącą rolę odgrywają również przypadki spam'u. Oczywiście przypadki, które są do nas zgłaszane wiążą się zazwyczaj z dużą uciążliwością lub z tzw. open relay'em, czyli takim skonfigurowaniem serwera pocztowego, które pozwala na wykorzystywanie go przez spamer'ów do rozsyłania niezamawianej korespondencji.

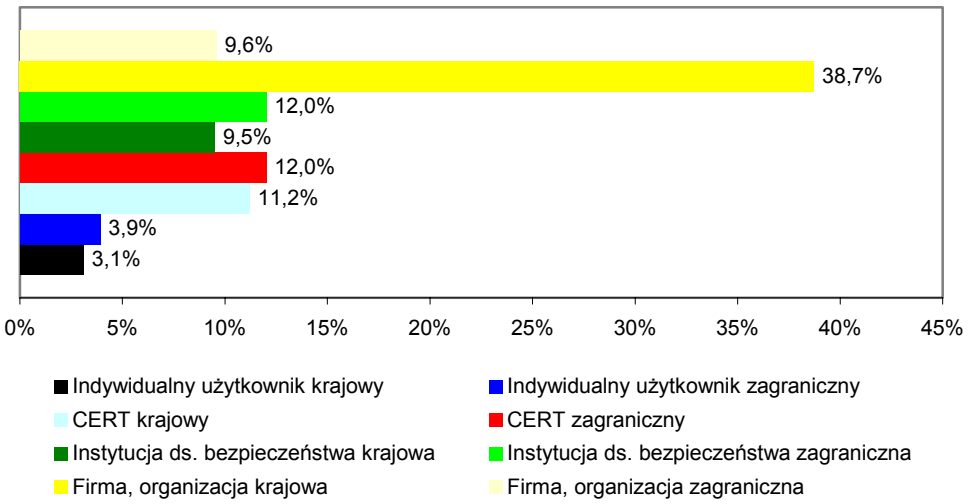
Trzecią pozycję (13,9%) na liście najbardziej popularnych rodzajów ataków zajmują łącznie potraktowane Code Red i Nimda, szczególnie aktywne w letnich miesiącach zeszłego roku. Code Red i Nimda zostały potraktowane razem jako wirusy sieciowe działające na podobnych zasadach, były one również przez nas obsługiwane w dużej mierze w sposób automatyczny.

3.4 Źródło zgłoszenia PNBT

Źródła zgłoszenia PNBT podzielono na 4 podstawowe kategorie:

- Użytkownik indywidualny;
- CERT;
- Instytucja ds. bezpieczeństwa;
- Firma, organizacja;

Każda z tych kategorii była podzielona na podmiot krajowy i zagraniczny. W ten sposób powstało 8 kategorii, które prezentowane są na poniższym wykresie.



Rysunek 11 - Źródła zgłaszania PNBT.

W przypadku kategorii „CERT krajowy" zdecydowaną większość stanowią zgłoszenia wewnętrzne CERT Polska związane ze spam'em i wirusami, które zostały przesyłane na adres poczty elektronicznej przeznaczony do zgłaszania incydentów. Zgodnie z powyższymi statystykami 62,5% zgłoszeń pochodziło z Polski, pozostałe z zagranicy.

3.5 Źródło ataku

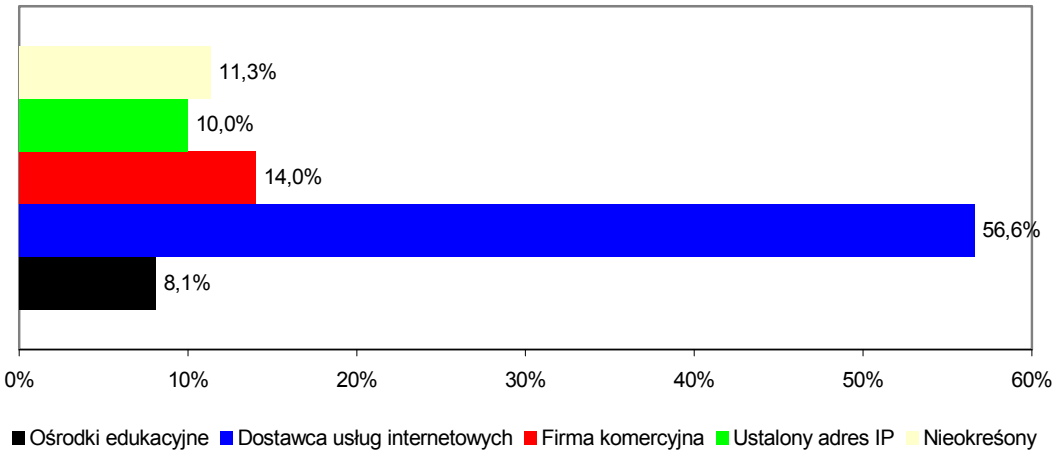
W obsługiwanych przez nasz zespół PNBT w blisko 90% udało się ustalić źródło ataku. Należy oczywiście wziąć pod uwagę, że wiele z tych adresów było tzw. adresami pośrednimi, które intruz wykorzystał w celu ukrycia rzeczywistego źródła ataku. Nie posiadamy informacji jak dużo było tego typu przypadków. W wielu przypadkach szczegóły dotyczące źródła ataku, CERT Polska pozostawiał do ustalenia poinformowanej osobie lub komórce, odpowiedzialnej w danej organizacji za bezpieczeństwo lub administrację sieci.

Kategorie na jakie podzieliliśmy źródła ataku są następujące:

- Ośrodki edukacyjne;
- Operatorzy telekomunikacyjni (ISP)[5];
- Firmy i organizacje;
- Ustalony Adres IP;

[5] kategoria ta w dużej mierze dotyczy również użytkowników indywidualnych, którzy są klientami ISPs

Jak widać wśród tych kategorii jest też pozycja „Ustalony adres IP". W tych przypadkach nie można było w prosty sposób zaklasyfikować źródła do innej kategorii dlatego zastosowano taką kategoryzację mówiącą o tym, że mimo braku dokładnych danych źródło ataku jest znane.



Rysunek 12 - Źródła ataków

Jak widać z powyższego wykresu podstawowe źródło ataków stanowią użytkownicy indywidualni, korzystający z połączeń oferowanych przez dostarczycieli usług internetowych.

4 Kooperacja przy obsłudze PNBT

W trakcie obsługi PNBT współpracowaliśmy z wieloma zespołami typu CERT z całego świata. Zdecydowana większość z nich jest członkami międzynarodowych organizacji FIRST (Forum of Incident Response and Security Teams) lub/i Terena TF-CSIRT (Task Forces Computer Security Incident Response Teams). O transgraniczności przestępstw komputerowych niech świadczy lista krajów, z których pochodziły zespoły reagujące współpracujące z nami przy wyjaśnianiu incydentów: Australia, Dania, Finlandia, Francja, Holandia, Korea Południowa, Meksyk, Niemcy, Rosja, Stany Zjednoczone, Szwajcaria, Wielka Brytania, Włochy.

W Polsce szczególną rolę odgrywała współpraca z zespołem TPSA Abuse Team, dodatkowo sporadycznie z zespołami bezpieczeństwa dostarczycieli usług internetowych.

5 Wnioski i trendy

i. **Wzrost PNBT.** Z roku na rok odnotowujemy coraz to większą liczbę PNBT. Mimo niepodważalnego trendu związanego z rzeczywistym przyrostem tego typu przypadków, należy zwrócić uwagę również na inne istotne czynniki, wpływające na ostateczne statystyki:

- Wzrost świadomości dotyczącej możliwości zgłoszenia PNBT i uzyskania pomocy od zespołu reagującego;
- Lepszy poziom obsługi zgłoszonego przypadku, co powoduje że poszkodowany zgłosi również następne tego typu przypadki (efektywność obsługi PNBT związana jest również z używaniem automatycznych narzędzi do obsługi standardowych przypadków);

ii. **Więcej przypadków skanowania.** W znaczący sposób został potwierdzony trend związany z przyrostem przypadków skanowania komputerów i sieci. Wskazuje to na większą świadomość dotyczącą istnienia zagrożeń w sieci Internet i monitorowanie tych zagrożeń oraz, jak należy przypuszczać, używanie w większym stopniu systemów detekcji zagrożeń (IDS), które pozwalają na zwiększoną wykrywalność i łatwiejszą dokumentację tych przypadków.

iii. **Po raz pierwszy *Common Language.*** W tym roku po raz pierwszy przedstawiliśmy statystyki oparte o klasyfikację *Common Language.* Wyniki tych statystyk pokazują jak trudno jest określić wszystkie dane dotyczące incydentu, okazuje się, że jest to możliwe tylko w przypadku bardzo szczegółowego rozpoznania przypadku. Najważniejszymi cechami tej klasyfikacji jest kompletność i jednoznaczność co w przyszłości pozwoli porównać statystyki z różnych lat. Dlatego też ta klasyfikacja będzie kontynuowana w latach następnych.

iv. **Automatyczne ataki.** Obserwowane przypadki skanowania i rozprzestrzeniania się wirusów sieciowych wskazują na fakt powszechnego wykorzystywania przez hakerów automatycznych narzędzi, zarówno w fazie ich przygotowywania (np.: tworzenie wirusów) jak i przeprowadzania (np.: skanowanie, włamania za pomocą tzw. rootkits, czy działanie robaków sieciowych). Zdecydowana większość tych przypadków związana jest działalnością tzw. s*cript kiddies*, którzy w swojej działalności wykorzystują gotowe narzędzia, nie znając w rzeczywistości sposobu ich działania.

v. **Słabość konfiguracji.** Działanie wspomnianych *script kiddies* powiązane jest zazwyczaj z wykorzystaniem znanych słabości, które nie zostały załatane przez administratorów. Potwierdzeniem tego faktu jest statystyka pokazująca, że największa liczba ataków związana była z wykorzystaniem luk w konfiguracji systemu. Dzięki temu jeszcze raz można się przekonać jak istotną rolę w zarządzaniu systemem informatycznym odgrywa sprawa odpowiedniego i systematycznego łatania istniejących w nim dziur.

vi. **Sprawcy ataków.** Jeśli chodzi o źródło ataków, to najpoważniejszym zagrożeniem dla bezpieczeństwa systemów komputerowych są klienci dostarczycieli usług internetowych. Najczęściej są to klienci działający na łączach dodzwanianych (*dial-up*). Niestety, wciąż istnieje błędne przekonanie o anonimowości tego typu połączenia,

chociaż należy przyznać, że w przypadku działania z zagranicy, ustalenie sprawcy jest trudniejsze, co nie znaczy że niemożliwe. Przy wyjaśnianiu tych spraw dochodzą po prostu trudności organizacyjne polegające na wymianie odpowiednich danych pomiędzy CERT'em a administratorami ISP. Wymaga to dobrej woli i potwierdzenia wiarygodności obydwu stron. Znaczący odsetek PNBT, w których źródłem ataku jest adres ISP sprawia, że kwestia dobrej współpracy z ISPs odgrywa i odgrywać będzie bardzo ważną rolę.

6 Kontakt

Zgłaszanie incydentów:	cert@cert.pl
Informacja:	info@cert.pl
Web site:	http://www.cert.pl/
Adres:	CERT POLSKA
	NASK
	ul. Wąwozowa18
	02-796 Warszawa
tel.:	+48 22 5231 274
fax:	+48 22 5231 399