CERT POLSKA

Raport 2002

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 jest także 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 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

2 Statystyki CERT POLSKA

Zgodnie z powyższymi założeniami programowymi CERT POLSKA co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich

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

zasobach internetowych. Niniejszy raport jest siódmym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.pl/raporty)

3 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[2]

3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

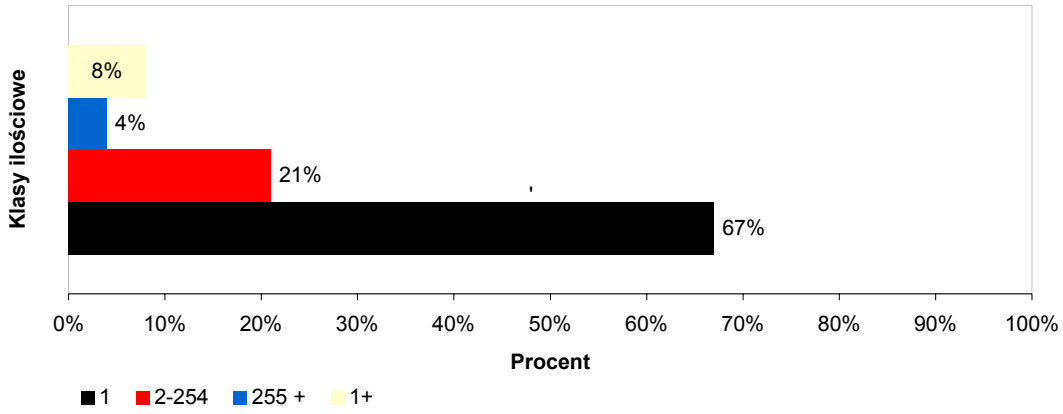
W roku 2002 odnotowano 3531 PNBT. Jednak 2518 przypadków było przypadkami tzw. spam'u (stanowi to 71,3% wszystkich przypadków). Przypadki te zostały potraktowane oddzielnie. Statystyki przedstawione poniżej odnoszą się więc do pozostałych 1013 przypadków.

3.2 Liczba zaatakowanych komputerów

Wśród stwierdzonych przypadków odnotowaliśmy takie, 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 67% przypadków mieliśmy do czynienia z atakiem na jeden komputer.

W sumie nasze statystyki uwzględniły ataki na 107553 obiekty sieciowe[3].



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

[2] W dalszej części raportu przypadki naruszenia bezpieczeństwa teleinformatycznego określane będą skrótem PNBT lub terminem „przypadeki"
[3] liczba ta uwzględnia jeden przypadek ataku na 65535 obiektów sieciowych.

3.3 Typy odnotowanych ataków[4]

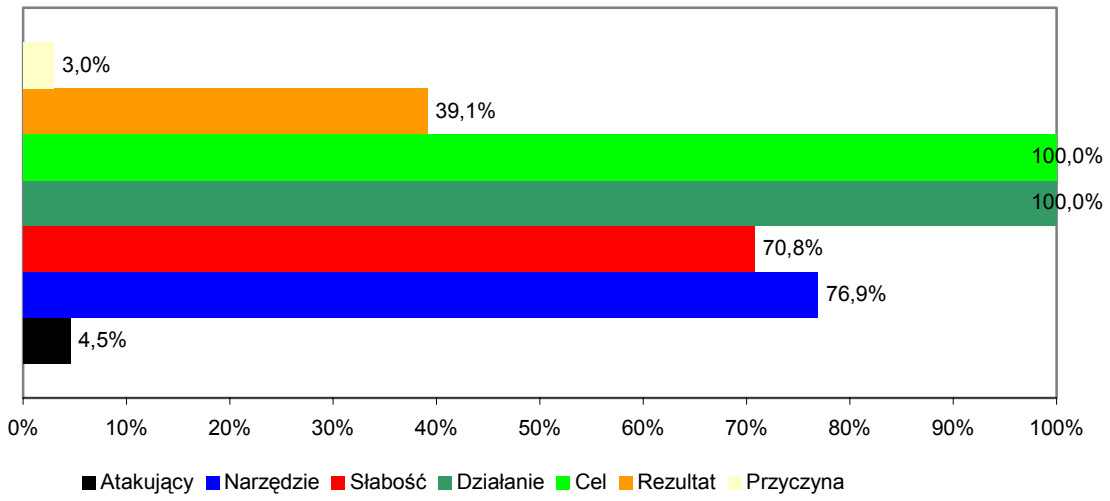
3.3.1 Klasyfikacja incydentów wg *Common Language*

Przypadki, w czasie obsługi których można było zgromadzić dane pozwalające na wypełnienie wszystkich cech przypadków, stanowią zaledwie 1,5% wszystkich przypadków.

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 (np.: ataki fizyczne). Niemniej jednak dla porządku i pełnego obrazu, w naszych statystykach nie pomijamy tych kategorii.

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.

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



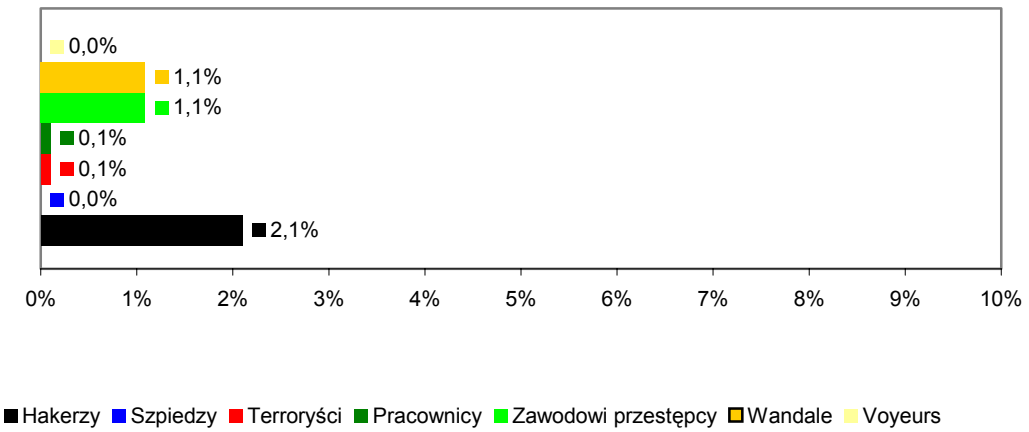
Rysunek 2 – Procent ustalenia poszczególnych cech PNBT.

Poniższe podpunkty pokazują rozkład procentowy w poszczególnych cechach opisujących przypadki.

[4] Począwszy od 2001 roku CERT Polska rozpoczął klasyfikację incydentów zgodnie z propozycją John'a D.Howard'a i Thomasa A.Longstaffa, znaną pod nazwą „Common Language" (*http://www.cert.org/research/taxonomy_988667.pdf*)

3.3.1.1 Atakujący[5]

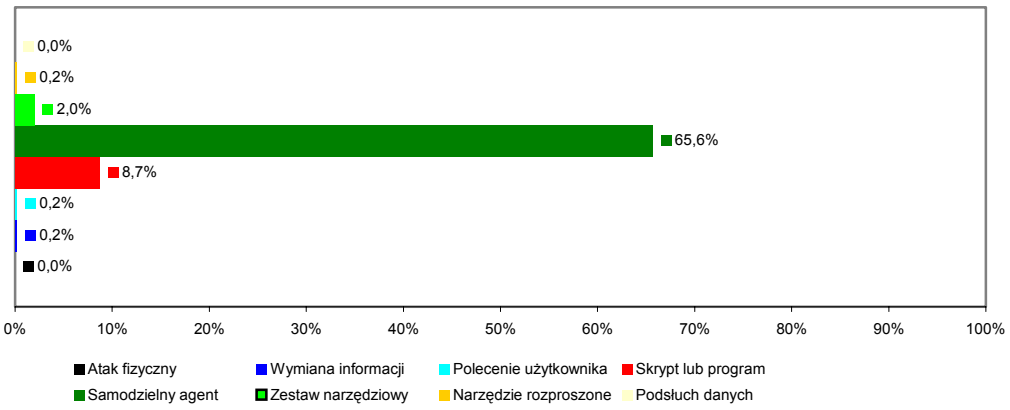
Na poniższym wykresie widzimy rozkład procentowy związany z kategorią „atakujący". Zgodnie z nim najczęściej do czynienia mieliśmy z hakerami, a w dalszej kolejności z wandalami i zawodowymi przestępcami. Należy jednak jeszcze raz zwrócić uwagę na niewielki procent ustalenia tej kategorii. Wyniki pochodzą z zaledwie 46 przypadków.



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". Jest to wyraźna kontynuacja trendu zapoczątkowanego w zeszłym roku, związanego z używaniem automatycznych narzędzi do ataków oraz działania na dużą skalę tzw. robaków internetowych. Oprócz znanych z roku 2001 robaków Code Red i Nimda w roku ubiegłym odnotowaliśmy bardzo wiele przypadków zainfekowania wirusem Klez.



[5] 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.*

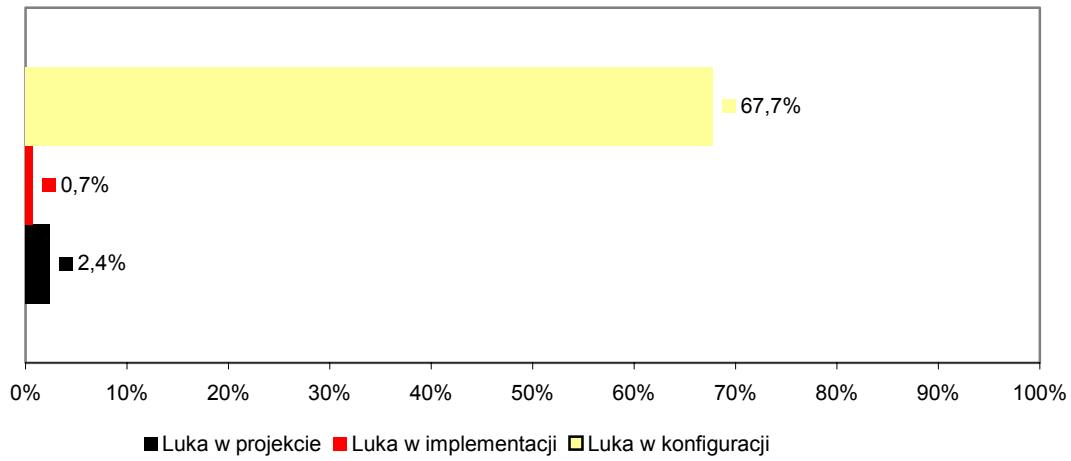
Rysunek 4 - Klasyfikacja używanych narzędzi ataku

3.3.1.3 Atakowana słabość systemu

Klasyfikacja *Common Language* wyróżnia trzy rodzaje słabości, które mogą zostać wykorzystane przez atakującego. Są to luka w projekcie, luka w implementacji oraz luka w konfiguracji. Poniekąd wszystkie słabości systemowe wywodzą się z błędów w zaprojektowaniu systemu, niemniej jednak trzeba pamiętać, że często dochodzi do skutecznego ataku w wyniku błędnej implementacji systemu, np: pozostawieniu działających niepotrzebnych usług, czy nie dograniu w czasie instalacji istniejących już łat systemowych. Natomiast błędy w konfiguracji wiążą się zazwyczaj ze złym zarządzaniem istniejącym systemem, np: nie instalowanie nowopojawiących się łat systemowych lub zmiana w systemie w celu rozwiązania chwilowego problemu w działaniu systemu. Często takie ”chwilowe” zmiany pozostają na zawsze i są przyczyną włamań do systemów.

Słabość związana z luka w konfiguracji systemów komputerowych jest zdecydowanie najczęstszą przyczyną ataków komputerowych.

Naszym zdaniem jest to wynikiem coraz większego wpływu zarządzania bezpieczeństwem istniejących systemów, które często pozostają nieuaktualniane po początkowej, często nawet poprawnej, implementacji. Wszystkie najbardziej znane robaki i wirusy internetowe wykorzystują słabości systemowe, które już wcześniej zostały rozpoznane i dla których zostały stworzone łaty systemowe. Na usprawiedliwienie administratorów systemów, którzy są głównymi odpowiedzialnymi za taki stan rzeczy, należy dodać, że ilość słabości systemowych wykrywanych dla poszczególnych systemów stale rośnie[6] i skuteczne ich śledzenie oraz reagowanie na nie stało się dla większości nie lada wyzwaniem.

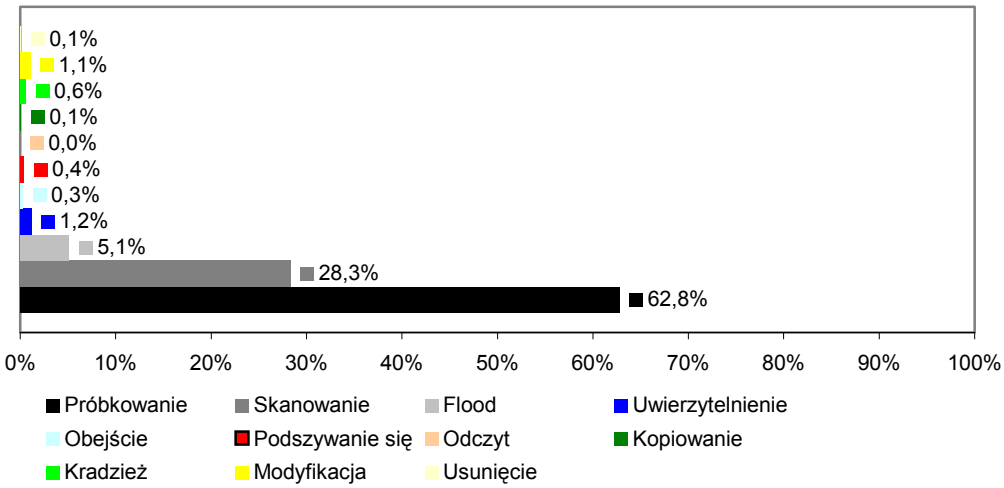


Rysunek 5 - Klasyfikacja wykorzystania poszczególnych luk w systemie

[6] patrz: http://www.cert.org/stats/cert_stats.html#vulnerabilities

3.3.1.4 Nieautoryzowane działanie

Podobnie jak w roku ubiegłym zdecydowanie największy procent nieautoryzowanego działania stanowią przypadki próbkowania i skanowania. Wynik ten jest potwierdzeniem trendu, z którym mamy do czynienia od kilku lat. Zarysowała się wyraźna granica pomiędzy tymi, którzy są świadomi niebezpieczeństw związanych z używania Internetu a tymi, którzy nie będąc tego świadomymi stali się ofiarami tych zagrożeń, a ich komputery bardzo często pośrednikami w dalszych atakach. To właśnie ci pierwsi zgłaszają do CERT Polska incydenty, natomiast tych drugich to my sami powiadamiamy o odnotowanych przypadków i prawdopodobnych włamaniach do ich systemów.

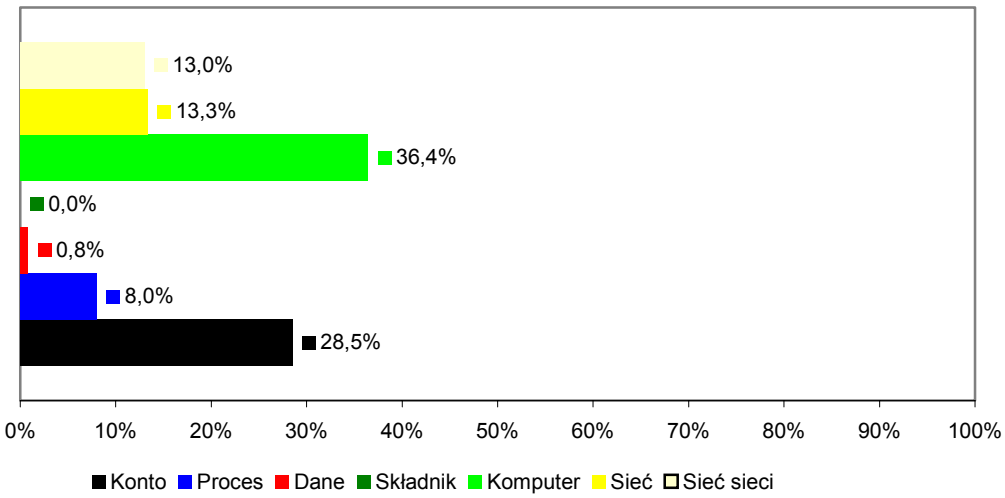


Rysunek 6 - Nieautoryzowane działanie podejmowane przez atakującego

3.3.1.5 Cel ataku

Cel ataku jest drugą podstawową cecha opisującą PNBT. Najczęściej, wśród przypadków w roku 2002, celem ataku były pojedyncze komputery, poddawane próbom włamań opartych o działanie wielokrotnie już wspominanych robaków internetowych. Przy tej okazji należy wspomnieć, że właściwie każdy przypadek skanowanie czy próbkowania jest de facto przypadkiem włamania do systemu, z którego to próbkowanie nastąpiło. Niezwykle rzadkie są sytuacje, w których intruz działa bezpośrednio ze swojego systemu. We wspomnianych sytuacjach CERT Polska ogranicza się do poinformowania właściciela źródła skanowania o prawdopodobnym włamaniu do jego systemu. W naszej działalności nadal obowiązuje zasada rejestracji przypadków tylko w przypadku zgłoszenia go przez poszkodowanego.

Atak na składnik jest w rzeczywistości atakiem fizyczny, np: kradzież tej części. Tego typu ataki jak dotąd nie są zgłaszane do CERT

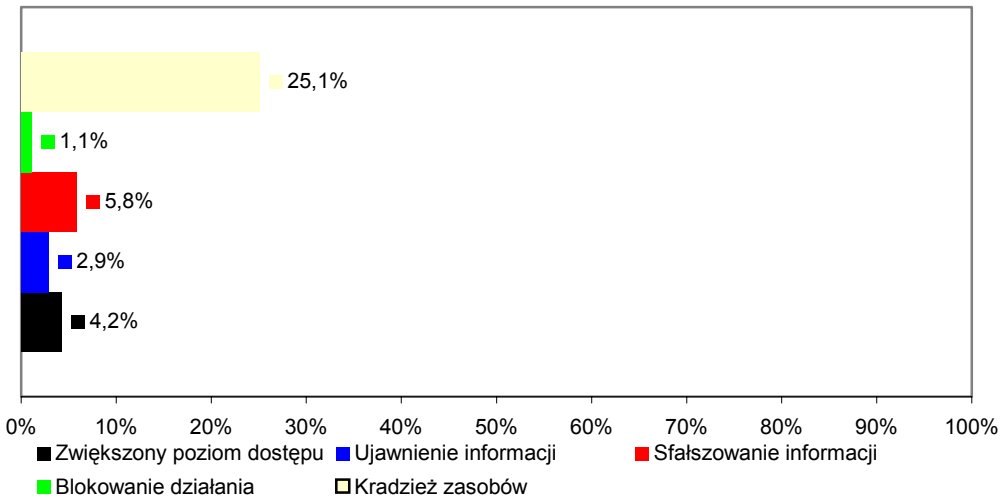


Polska.

Rysunek 7 - Cel ataku

3.3.1.6 Rezultat

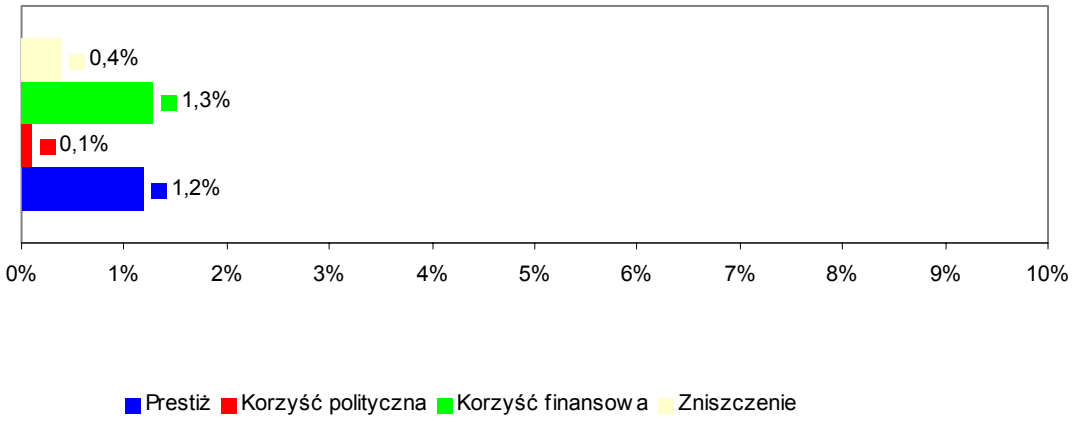
Wśród rozpoznanych skutków działania intruzów zdecydowanie na pierwszy plan wysuwa się *kradzież zasobów*. Dwa podstawowe przypadki wpływające na taki stan rzeczy to kradzież zasobów rozumianych jako moc obliczeniowa oraz rozumianych jak praca ludzka. Właśnie w przypadku skanowania mamy do czynienia z taką sytuacją. System poszkodowanego jest niepotrzebnie obciążony koniecznością „obsługi" nielegalnych pakietów a dodatkowo administrator musi poświęcić dużo pracy nad analizą logów ze swoich urządzeń filtrujących i systemów wykrywania zagrożeń.



Rysunek 8 - Rezultat przeprowadzonego ataku

3.3.1.7 Przyczyna

Przyczynę, która decydowała o wystąpieniu ataku jest bardzo trudno ustalić, dlatego procent odpowiedzi na pytanie *Co było przyczyną działalności intruza?* jest niewielki (zaledwie 4,5%). 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 niebudzącym wątpliwości, co do przyczyn, przypadkiem jest spam, który jak to wcześniej zaznaczyliśmy został potraktowany oddzielnie.



Rysunek 9 - Przyczyna ataku

3.3.1.8 Spam

Jak to zostało wspomniane wcześniej w roku 2002 zarejestrowaliśmy 2518 przypadków spam'u. Reakcja na te przypadki oprócz trudnych prób wyeliminowania źródła spam'u mają również za zadanie ustalenie jak największej liczby źle skonfigurowanych serwerów pocztowych, które są wykorzystywane przez sapm'erów. W przypadku ustalenia takiego serwera kontaktujemy się z jego właścicielem i przekazujemy wskazówki dotyczące poprawy konfiguracji.

Znakomita większość przypadków spam'u sklasyfikowana jest w następujący sposób:

- atakującym jest *Zawodowy przestępca;*

- używa on zazwyczaj *skryptu lub programu;*

- wykorzystuje najczęściej dziurę w *konfiguracji;*

- spam wiąże się z odnotowywaniem nielegalnego, przepełniającego łącza i inne zasoby, ruch czyli *flood* ;

- jest to atak na *sieć sieci;*

- jego rezlutatem jest *kradzież zasobów;*

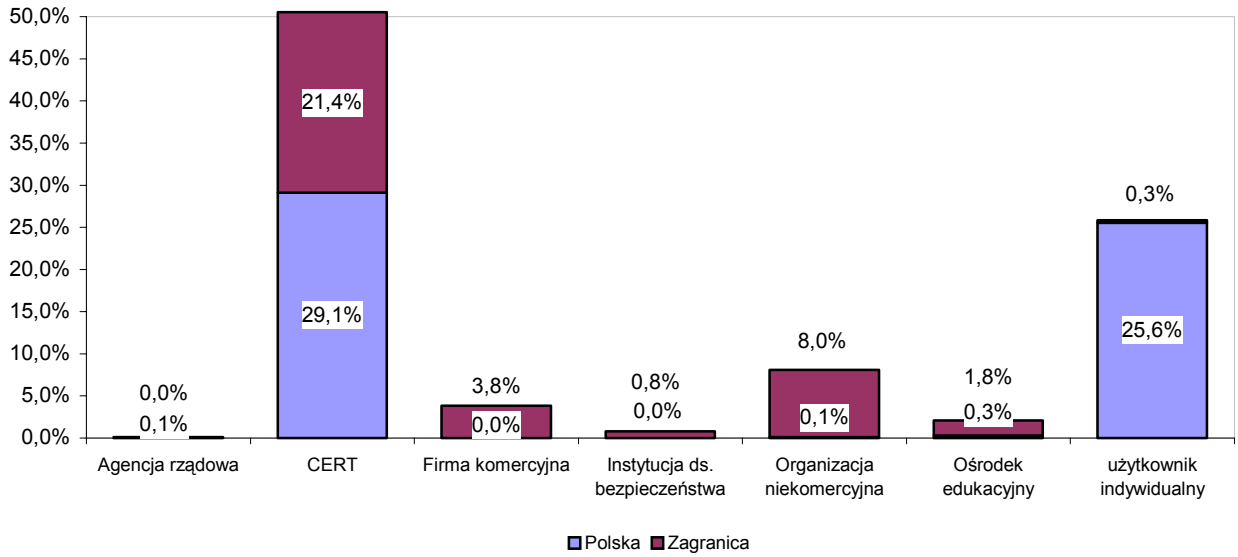
- a przyczyną zazwyczaj chęć uzyskania *korzyści finansowej*, znacznie rzadziej osiągnięcie korzyści politycznej.

3.4 Źródło zgłoszenia PNBT

Źródła zgłoszenia przypadków podzielono na 7 podstawowych kategorii[7]:

- Agencja rządowa;
- CERT;
- Firma komercyjna;
- Instytucja ds. bezpieczeństwa (inna niż CERT);
- Organizacja niekomercyjna;
- Ośrodek edukacyjny;
- Użytkownik indywidualny;

Każda z tych kategorii była podzielona na podmiot krajowy i zagraniczny. W ten sposób powstało 14 kategorii, które prezentowane są na poniższym wykresie.



Rysunek 10 - Źródła zgłaszania PNBT.

[7] W stosunku do roku 2001 nastąpił zwiększenie liczby kategorii o 3. Dotychczasowe kategorie to: użytkownik indywidualny, CERT, instytucja ds. bezpieczeństwa, firma-organizacja.

Z wykresu widać, że w tej kategorii prym wiodą instytucje typu CERT oraz użytkownicy indywidualni (głównie krajowi). Liczba zgłoszeń krajowych (55%) przewyższa liczbę zgłoszeń z zagranicy (37%).

3.5 Źródło ataku

W obsługiwanych przez nasz zespół przypadkach, w 94% 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.

Podstawowym, ustalonym dokładnie (kraj i kategoria) źródłem ataków[8] są zagraniczne firmy komercyjne oraz polskie ośrodki edukacyjne - odpowiednio 7 i 4 procent wszystkich ataków. Oczywiście chodzi tu o pojedynczych intruzów wykorzystujących do ataku sieci tych firm i jednostek edukacyjnych.

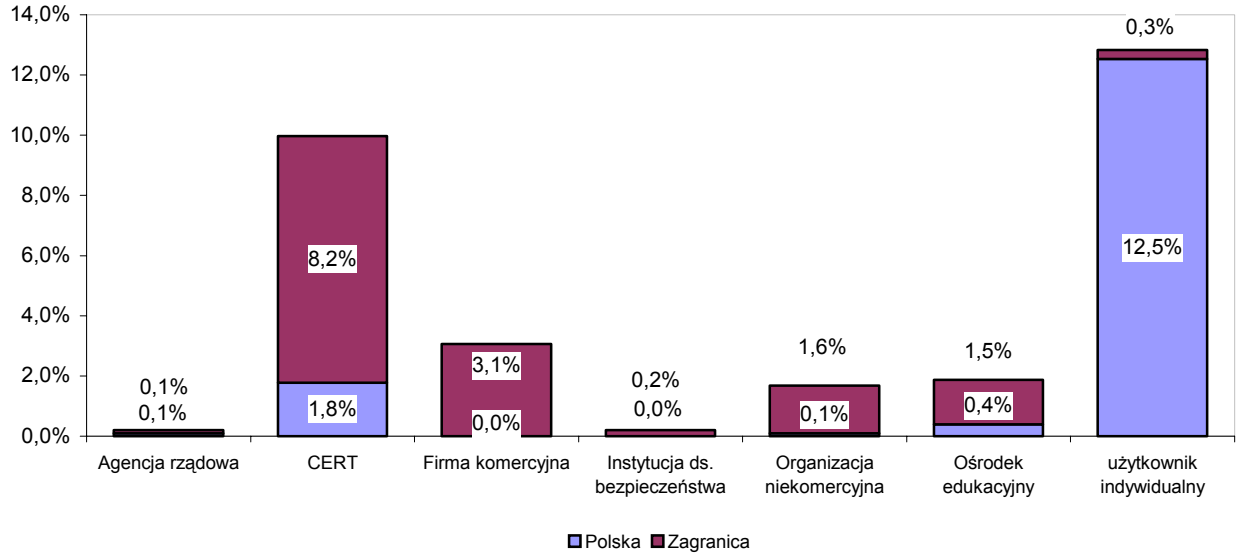
3.6 Poszkodowani

W tym roku po raz pierwszy wprowadziliśmy nową kategorię poszkodowanego. Do tej pory domyślnie poszkodowany wyszukiwany był wśród zgłaszających przypadki, jednak coraz większą rolę spełniają w obsłudze bezpieczeństwa zespoły reagujące na ataki komputerowe (CERT-y) oraz inne instytucje ds. bezpieczeństwa, które w całej sprawie są pośrednikami a nie poszkodowanymi. Dlatego statystyki coraz mniej odzwierciedlały rzeczywistość. Należy przy tym dodać, że sytuacja ta również wpływa na mniejszą szansę ustalenia dokładnych kategorii poszkodowanych[9].

Liczba dokładnie ustalonych poszkodowanych w Polsce jest dokładnie taka sama jak zagranicą (151 - co stanowi 15% wszystkich przypadków). Rozkład kategorii wygląda następująco:

[8] Ustalono to tylko w 12% przypadków

[9] Przy koordynacji PNBT pomiędzy CERT-ami przyjęte jest, że nie jest konieczna dokładna wiedza na temat poszkodowanego dla CERT-u którego zadaniem jest ustalenie sprawcy naruszenia bezpieczeństwa.



Rysunek 11 - Poszkodowani.

Warto zwrócić uwagę na stosunkowo duży procent CERT-ów wśród poszkodowanych. Głównym powodem znaczącej liczby tych zgłoszeń jest sam fakt istnienia wysokiego poziomu świadomości związanej z koniecznością zgłaszania przypadków, istniejącego wśród samych CERT-ów.

4 Wnioski i trendy

Poniżej zamieściliśmy głównie wnioski, jakie nasuwają się nam po analizie zebranych danych oraz wynikają z naszej codziennej pracy związanej z obsługą przypadków:

i) Polaryzacja wiedzy i świadomości dotyczącej zagrożeń teleinformatycznych. Rośnie zarówno procent posiadających dużą wiedzę i świadomość, jak i tych, którzy są bardzo słabo lub w ogóle nie zorientowani w tematyce bezpieczeństwa IT;

ii) Bezpieczeństwo w sieci zależy coraz bardziej od najsłabszego ogniwa, jakim staje się niski poziom dbania przez administratorów systemów o to, aby ich zasoby miały aktualne zabezpieczenia (tzw. łaty systemowe)

iii) Incydenty stają się coraz bardziej rozległe, coraz trudniej ustalić rzeczywistego atakującego i rzeczywistego poszkodowanego, który często nie jest bezpośrednio zaatakowany, ale w sposób istotny odczuwa skutki ataku na inne niż swoje zasoby;

iv) Coraz częściej to, co uważamy za źródło ataku, jest w rzeczywistości jedną z ofiar ataków. Źródła ataków w statystykach wskazują de facto na najgorzej zabezpieczone zasoby sieci;

v) Coraz więcej poszkodowanych jest wśród użytkowników indywidualnych, co zapewne jest skutkiem podłączenia stałymi, szybkimi łączami do internetu, domowych komputerów osobistych;

vi) Nadal nie ma zgłoszeń przypadków z najpoważniejszych ośrodków takich jak agencje rządowe i poważne firmy komercyjne. Wskazuje to na fakt istnienia w tych instytucjach wewnętrznej polityki nie informowania o tego typu przypadkach. Biorąc pod uwagę, że ataki na te podmioty są dokonywane przez najgroźniejszych intruzów, to w konsekwencji takie działanie prowadzi do znacznego osłabienia możliwości ich wyeliminowania.

5 Kontakt

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