Raport CERT NASK w zakresie naruszeń bezpieczeństwa w sieci Internet w roku 1996

W roku 1996 kiedy formalnie zaczął swą działalność zespół CERT NASK zanotowano na całym świecie - Polska nie była tu wyjątkiem dużą liczbą zdarzeń zagrażających i naruszających bezpieczeństwo sieci Internet i jej użytkowników. Zespół CERT NASK reagujący na zdarzenia naruszające bezpieczeństwo w sieci polskiego Internetu począwszy od marca roku 1996 rejestruje zdarzenia naruszające bezpieczeństwo oraz reaguje m.in. poprzez :

- oferowanie pomocy poszkodowanym
- alarmowanie i ostrzeganie użytkowników i administratorów sieci wobec występujących zagrożeń i incydentów
- szerzenie informacji podnoszącej wiedzę z zakresu problematyki bezpieczeństwa i ochrony
- prezentowanie statystyk zanotowanych incydentów

CERT NASK w okresie marzec -grudzień 1996 zaprezentował dwukrotnie dane statystyczne W tym czasie zespół zanotował kilkadziesiąt incydentów o charakterze krajowym i międzynarodowym. Wśród tych zdarzeń były próby włamań do komputerów w Polsce z poza kraju, włamania z Polski do komputerów poza Polską, sygnały z innych krajów o próbach włamań z Polski, próby i udane przypadki włamań zgłaszane przez administratorów sieci w kraju.

Ilość i zagrożenie dla Internetu (nie tylko polskiego) jakie wynikają z tych statystyk stanowią poważny sygnał , że bez skoordynowanej akcji w celu zapobiegania włamaniom i właściwej reakcji na pojawiające się zdarzenia naruszające bezpieczeństwo polski Internet będzie traktowany jako

wygodne miejsce do działań sieciowych włamywaczy. Aby przeciwdziałać takiej sytuacji należy propagować ideę współpracy wszystkich administratorów sieci i osób odpowiedzialnych za ich bezpieczeństwo , zespołów reagujących na zdarzenia (w Polsce takim zespołem jest CERT NASK) a także przedstawicieli prawa - gdyż pewna część incydentów graniczy lub przekracza granicę poza którą sprawcy powinni być ścigani przez wymiar sprawiedliwości. Odrębnym problemem jest właściwe naświetlenie problematyki włamań w Internecie przez media - co w Polsce pozostawia wiele do życzenia.

Statystyka

Na podstawie danych zgromadzonych w czasie obsługi zgłoszonych do CERT NASK incydentów (obsługa polega na pomocy poszkodowanym lub narażonym na zagrożenia) opracowano podsumowanie typologiczne i statystyczne dotyczące charakteru incydentów, stosowanych przez intruzów technik oraz "obszaru rażenia" w podziale na domeny internetowe.

Wykorzystanie przez intruzów oprogramowania dostępnego w sieci na przykładzie danych w zakresie lokalizowania komputerów do zaatakowania.

Z danych CERT NASK wynika, iż w zakresie technik lokalizowania komputerów do zaatakowania intruzi wykorzystują rozmaite metody tzw. "skanowania" sieci i "próbkowania" komputerów w sieci. Metody te, wg. zanotowanych przypadków w Polsce, opierają się na wykorzystaniu istniejących w sieci programów i skryptów Są to skrypty wykonujące automatycznie setki a nawet tysiące prób "połączeń" z określoną grupą adresów w sieci w celu wykrycia i wykorzystania luk w systemach tych komputerów a także wykorzystywane są typowe pakiety skanujące, które są używane zarówno przez administratorów sieci w celu zbadania realnego poziomu bezpieczeństwa zarządzanego komputera czy sieci jak też używają ich intruzi. Wykryte przypadki sniffingu (podsłuchiwanie cudzych pakietów w sieci) zdecydowanie dominowały w działalności hackerskiej w drugiej połowie 1996 roku.

W sieci Internet, a konkretnie na serwerach - głównie akademickich - znajduje się oprogramowanie, które może służyć do przygotowania lub przeprowadzenia zdalnego ataku na cudzy system komputerowy. Znaleźć można także opisy i instrukcje w jaki sposób można dokonać włamania czy też oszustwa przy pomocy Internetu i komputera (zanotowano np. przypadek upowszechnienia na serwerze akademickim instrukcji w języku polskim, jak dokonywać przy pomocy Internetu oszustw w dziedzinie kart płatniczych). Oprogramowanie ułatwiające przygotowywanie bądź atakowanie cudzych systemów można podzielić na kilka rodzajów:

- Pakiety służące do półautomatycznych testów stopnia zabezpieczenia komputerów (np. osławiony SATAN) lub monitorowania sieci i urządzeń (zgodnie ze swym przeznaczeniem mają służyć administratorom sieci do testowania zarządzanych przez siebie komputerów - powszechnie

jednak używają ich hackerzy aby zbadać zabezpieczenie cudzych sieci lub podsłuchiwać pakiety w celu ewentualnego późniejszego zaatakowania cudzych systemów)

Istnienie i dostępność tego typu programów nie musi być niczym nagannym. Potencjalne zagrożenie wynika z praktyki: paradoksalnie nie wszyscy administratorzy znają i wykorzystują to oprogramowanie w przeciwieństwie do sieciowych włamywaczy, którzy stosują je nagminnie.

- Programy i skrypty stworzone i opublikowane w sieci przez włamywaczy służące eksploatowaniu rozmaitych słabości systemów operacyjnych, sieciowych i oprogramowania użytkowego stosowanego w Internecie (w tej grupie znajdują się wirusy, bomby logiczne, konie trojańskie, sniffery i inne programy oraz
skrypty używane przez rozmaitych intruzów)

Programy takie często dostają się w ręce niedoświadczonych osób, które zaczynają je wykorzystywać do włamywania się do cudzych systemów. Obecnie zauważa się coraz większą liczbę przypadków poważnych włamań powodowanych przez mało doświadczonych włamywaczy używających groźnych ("profesjonalnych") narzędzi dostępnych w Internecie. Na niektórych serwerach w Polsce (głównie akademickich znajdują się prawdziwe "skarbnice" oprogramowania, które może być wykorzystane do włamań na cudze systemy. Rozpowszechnianie tego typu oprogramowania poprzez umieszczanie go na serwerach jest czynnością ze wszech miar naganną i nie powinno pozostawać bez reakcji - przynajmniej w trybie administracyjnym.

Typologia ataków

Ataki na systemy komputerowe w Internecie związane z Polską poprzez lokalizację źródła bądź celu mają różną wagę i zasięg. Jeśli weźmiemy pod uwagę tylko zdarzenia poważnie zagrażające lub naruszające bezpieczeństwo to w roku 1996 obok incydentów, w których zaangażowanych było kilka komputerów CERT NASK zanotował i obsłużyć np. incydent, w którym próbkowano kilkanaście tysięcy komputerów w Polsce, z czego - zgodnie z posiadanymi informacjami tylko w kilku z nich zostały skutecznie przełamane zabezpieczenia przez intruza.

W owych masowych atakach intruzi posługują się wcześniej wspomnianymi skryptami i programami, które automatycznie wyszukują w sieci swoje potencjalne ofiary a następnie probują wykorzystać określoną slabość danego systemu (np. popularnego acz niebezpiecznego systemu rozproszonego NIS) w celuprzechwycenia informacji przydatnych do włamania a następnie wykorzystania jej do samego włamania.

Jeżeli chodzi o typy ataków to najczęściej spotykano w okresie III - IX 96 (pierwszy okres sprawozdawczy CERT NASK) ataki poprzez:

- słabości systemów rozproszonych takich jak NIS,
- słabe hasła
- słabości HTTP (WWW)
- luki w oprogramowaniu (najczęściej sendmail)

W okresie X-XII 96 ataki najczęściej odbywały się poprzez:

- sniffing
- słabe hasła, (do tego celu używano często narzędzi skanujących)
- coraz częściej wykorzystywano niski poziom bezpieczeństwa stron World Wide Web

Tradycyjne systemy haseł, które są pierwszym i często ostatnim elementem zabezpieczenia każdego współczesnego systemu komputerowego wielodostępnego nie stanowią już w tej chwili dostatecznego zabezpieczenia w obliczu rozpowszechnionej przez intruzów techniki sniffingu czyli podsłuchiwania haseł. Odgadnięcie (złamanie) zbyt prostego hasła lub też podsłuchanie statycznego hasła (które jest zbyt żadko zmieniane) jest w dalszym ciągu jedną z podstawowych technik wykorzystywanych przez włamywaczy. Praktycznie atak na hasła jest elementem prawie 100% ataków zarejestrowanych przez CERT NASK. Czasem jest to podstawowy element scenariusza włamania, czasem tylko jeden z kroków nieuprawnionych działań intruza - jednakże prawie zawsze jest to chętnie wykorzystywana słabość systemów.

Rosnąca popularność systemu WWW skutkuje także w pojawiających się coraz częściej atakach na serwery WWW poprzez wykorzystanie rozmaitych luk np. w programach CGI, języku Java i innych. Na serwerze WWW CERT NASK znajdują się kopie CERT /CC advisories oraz linki do zasobów udostępnianych przez inne zespoły.

Co robią intruzi w czasie udanych włamań?

Typowy scenariusz ataku na system komputerowy składa się z kilku etapów:

- lokalizowanie systemu do zaatakowania
- zdobycie dostępu do konta legalnego użytkownika systemu poprzez łamanie łatwych haseł bądź podsłuchanie hasła
- wykorzystanie dziur w konfiguracji i w oprogramowaniu systemowym w celu wejścia na konto uprzywilejowane
- zatarcie śladów działalności (usunięcie zapisów z pamiętników - audit log) przeprowadzenie nieuprawnionych działań
- zainstalowanie "konia trojańskiego" dla aktualnego i przyszłego wykorzystania
- ataki na inne komputery w sieci lokalnej

Intruzi atakujący systemy komputerowe znajdujące się w sieci częstokroć posługują się kilkoma złamanymi wcześniej kontami na różnych maszynach logując się kolejno z jednego na drugie. Utrudnia to śledzenie miejsca, z którego tak naprawdę przeprowadzony był atak.
W punkcie "przeprowadzenie nieuprawnionych działań" intruzi dokonują takich czynności jakie są

rzeczywistym celem ich ataków. Zgodnie ze statystyką CERT NASK w Polsce najczęściej spotykane działania to:

- wprowadzanie zmian w zaatakowanym systemie (modyfikacje ważnych plików np. /etc/passwd)
- podmienianie plików systemowych - (ang. deamons) - np. telnetd
- instalacja modułów "koni trojańskich"
- instalowanie snifferów
- ingerowanie w prywatność (np. przeglądanie cudzej poczty elektronicznej)
- powodowanie szkód moralnych i zaburzeń w komunikacji (nieuprawniona ingerencja w treść stron WWW)
- przechowywanie i kolportowanie pornografii - w tym dziecięcej

Działania wymienione w pierwszych dwóch punktach mają na celu uzyskanie pełnej kontroli nad zaatakowanym systemem. W dodatku często jest to przeprowadzane w taki sposób aby legalny administrator systemu nie zauważył faktu przejścia kontroli nad komputerem przez intruza. Intruz może wykorzystywać kontrolowany przez siebie komputer do ataków na inne systemy, składowania na nim niepożądanych plików (np. pirackiego oprogramowania), wykorzystywania jego mocy obliczeniowej do np. łamania plików z hasłami bądź też kradzieży informacji. Z kolei instalacja snifferów czy modułów zapewniających tzw. tylne drzwi do systemu ma na celu przygotowanie pola do ataku na inne komputery w danej sieci lokalnej oraz zapewnienie sobie łatwego dostępu do złamanego komputera w przyszłości.

Trzy ostatnie typy działań czyli ingerowanie w prywatność, powodowanie szkód moralnych oraz zaburzeń w komunikacji a także rozpowszechnianie nielegalnych czy niepożądanych treści są już typowymi czynnościami powodującymi określone szkody kwalifikującymi się wręcz do ścigania na drodze prawnej. Istnieją w Polsce precedensy, gdzie organa ścigania mogą powziąć z pozytywnym skutkiem określone czynności przeciwko sprawcom ww. czynów.

Oddzielną grupą stanowią działania związane z naruszeniem etykiety sieciowej (zwanej netykietą). Przykładami tego jest spamming i mail bombing. Można ten typ działalności podzielić na dwa rodzaje. Pierwszy to rozsyłanie materiałów reklamowych lub innych, które nie są zamawiane przez odbiorcę, drugi zaś to przesyłanie dużej ilości listów, lub mniejszej ale o większej zawartości, pod jeden wybrany adres. Ten drugi sposób niejednokrotnie może zablokować skrzynkę pocztową poszkodowanego i skutecznie utrudnić mu pracę i korzystanie z sieci. Pierwszy zaś może powodować np. dezorganizację jednej lub wielu list dyskusyjnych. Zdarza się także , że oba sposoby są wykorzystywane wspólnie. Wśród przypadków zarejestrowanych przez CERT NASK były takie gdzie sprawca dokonywał spammingu w dużej mierze nieświadomie (nie wiedział do końca,że skutek jego działalności może być przykry dla wielu set użytkowników Internetu na całym świecie, którzy mogą dostać wiele niezamówionych przesyłek tej samej treści). Nie zawsze więc incydent mający swoje źródło w Polsce a odbijający się szerokim echem na całym świecie jest intencjonalnie zaplanowany co

do skutków przez sprawcę (z resztą nie jest to nic niezwykłego od czasu incydentu Internet Worm z 1988 roku). Mail bombing natomiast to już z reguły intencjonalne działanie intruza mające na celu utrudnienie pracy lub wręcz zablokowanie innemu użytkownikowi pracy w sieci. Spośród zarejestrowanych przez CERT NASK przypadków szczególnie uciążliwy był ten w czasie którego sprawca mail bombingu zarzucał skrzynki pocztowe pracowników firmy przeciwko której prowadził prywatną wojnę w Internecie dużą ilością przesyłek pokaźnej objętości. "Wojna" ta obfitowała także w przesyłanie i publikowanie przez sprawcę treści nieprzychylnych czy wręcz szkalujących daną firmę.

Proporcje geograficzne i typologiczne W całym 1996 roku (licząc od marca) zgłoszenia incydentów z Polski stanowiły około 64%, pozostałe 36% to zgłoszenia z zagranicy. Można uznać, że w zgłoszeniach z Polski dominują informacje na temat konkretnych włamań i poczynionych szkód Zgłoszenia z zagranicy natomiast w większości dotyczyły przypadków skanowania sieci, spammingu (zarzucanie odbiorców ogromna ilością przesyłek), nienależytego używania USENET News (tzw. junk mails, wysyłanie zdjęć pornograficznych). Tego typu działania powodują szkody o charakterze szkód moralnych i faktu utrudniania pracy użytkownikom Internetu przez polskich użytkowników sieci. Były jednak również przypadki konkretnych włamań do komputerów za granicą przeprowadzone z Polski.

Na podstawie zgromadzonych danych CERT NASK przeprowadził analizę grupującą atakowane komputery w odpowiednie kategorie ze względu na domenę, w której zostały zarejestrowane. W ten sposób atakowane komputery w domenie .edu.pl a także komputery zarejestrowanie w domenach regionalnych należące do placówek akademickich (np. uczelnie wyższe niezależnie od ich charakteru - także uczelnie niecywilne) zostały ostatecznie zliczone w jednej grupie (umownie nazwaną : edukacja). Komputery z domeny .com.pl. a także należące do firm komercyjnych zarejestrowanych w innych domenach także zgrupowano (grupa: komercyjni). Z grupy tej wyodrębnioną klasą tzw. prowiderów (dostawców usług Internetowych). Trzecią grupą atakowanych komputerów stanowią hosty zarejestrowane w domenie .gov.pl. oraz innych instytucji administracji publicznej, państwowej (grupa: rządowe).

Na uwagę zasługuje ogromna ilość a także rozkład domenowy próbkowanych hostów (czyli komputerów, które były obiektem prób do przeprowadzenia ataku). Dane zgromadzone przez CERT NASK świadczą, ze ponad 7% komputerów w polskim Internecie było próbkowanych Na szczęście tylko nikły procent (<1%) z próbkowanych komputerów uległ udanemu atakowi hackerów - jednak CERT NASK podkreśla, ze statystyka ta dotyczy zgłoszonych incydentów Nie wiadomo ile prób i udanych ataków nie jest w ogóle zgłaszanych i rejestrowanych.

Diagram nr 1

Diagram nr1 pokazuje podział procentowy na główne domeny ilości próbkowanych hostów w obsłużonych przez CERT NASK incydentach. W kategorii "inne" umieszczono domeny typu np: miasto.pl lub nazwa.pl . W ramach grupy "inne" znalazły się podmioty o profilu edukacyjnym (81%)

bądź komercyjnym 19% (do tej ostatniej grupy zaliczono też dostawców internetu). Na podstawie diagramu nr 1 opracowano diagram nr 2.

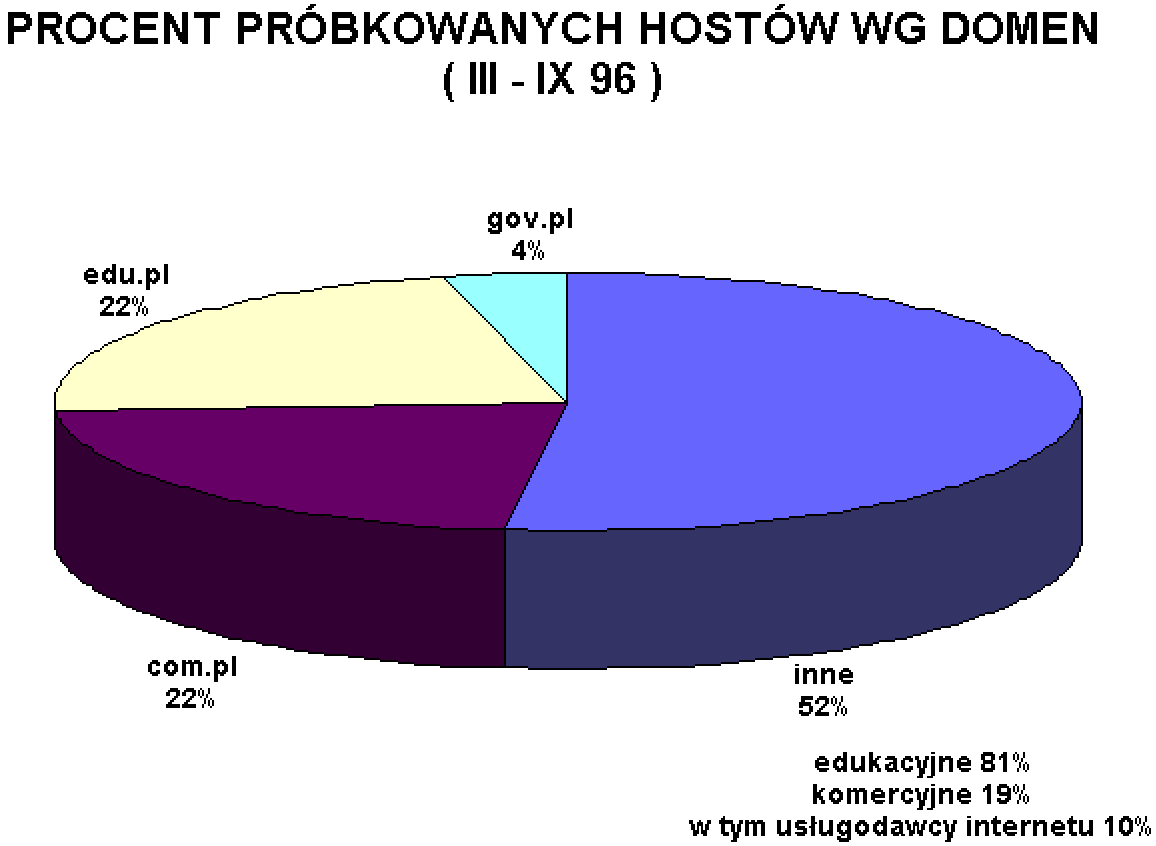


Diagram nr 2

Diagram ilustruje podział procentowy atakowanych komputerów wg. profilu działalności podmiotów do których te komputery należą.

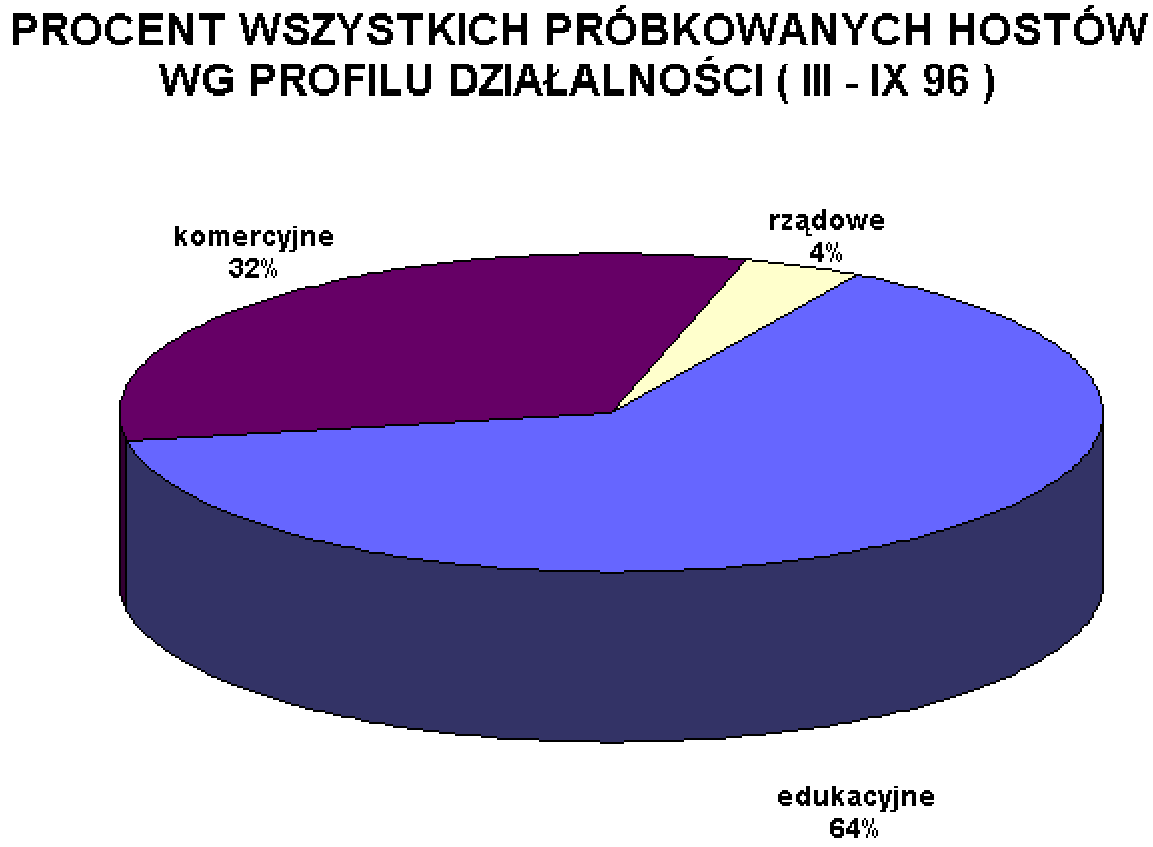
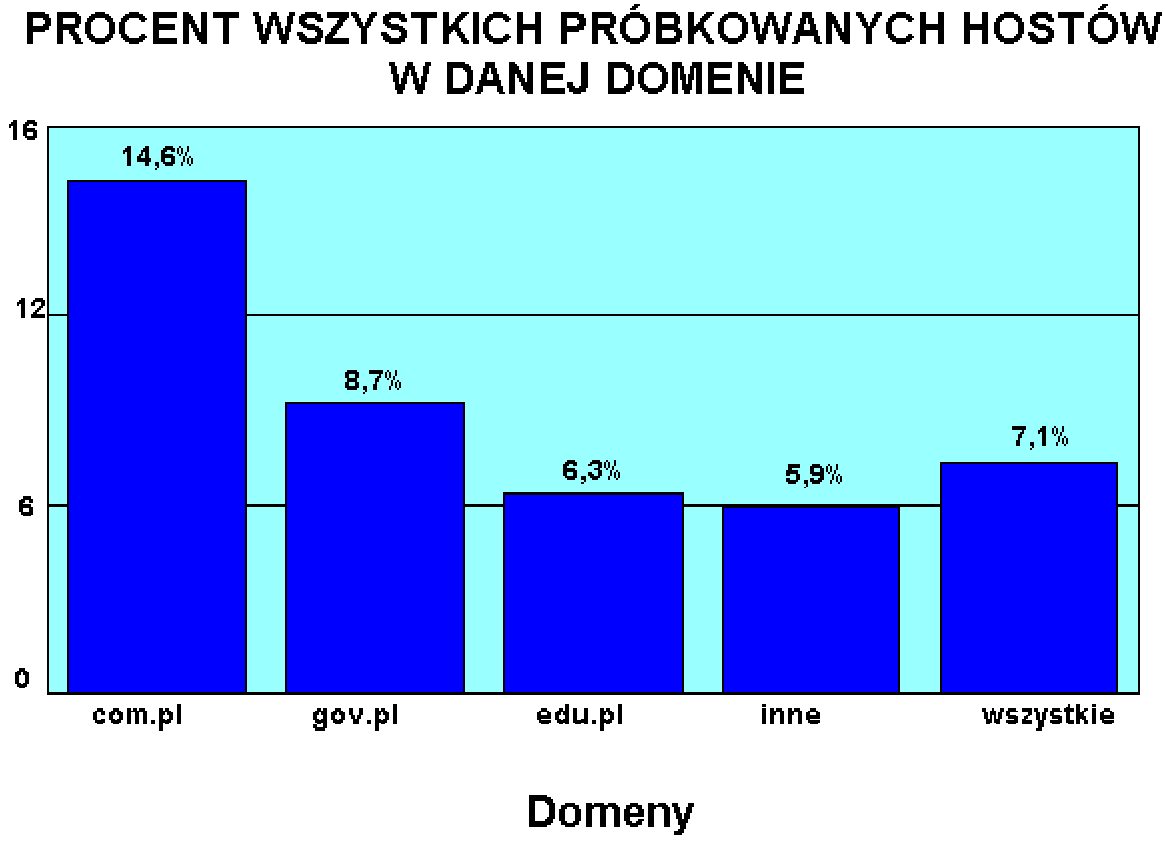


Diagram nr 3

Na wykresie zilustrowano proporcje próbkowanych hostów do ogólnej ilości zarejestrowanych hostów w danej domenie. Kategoria "inne" odpowiada tej samej kategorii z diagramu nr. 1. Kategoria "wszystkie" dotyczy wszystkich hostów zarejestrowanych w domenie .pl. Dane jakie przedstawiają te wykresy, choć prezentują stan za okres marzec - październik, można odnieść do całego okresu działalności CERT NASK w 1996, gdyż próbkowanie polskich hostów na dużą skalę miało miejsce głównie we wspomnianym wcześniejszym okresie. Uważna analiza danych trzech zaprezentowanych diagramów pozwala wysnuć bardzo ciekawe wnioski. Niewątpliwie najwięcej próbkowanych komputerów należy do grupy: edukacja. Jest to poniekąd zrozumiałe ponieważ hostów należących do uczelni, instytutów badawczych i innych placówek akademickich jest w polskim Internecie zdecydowanie najwięcej. Na drugim miejscu są komputery z grupy komercyjnej a na trzecim z grupy rządowej. Jednak rzut oka na diagram trzeci wskazuje, że ilościach względnych (ilość atakowanych komputerów w stosunku do wszystkich zarejestrowanych w danej kategorii) "edukacja" wcale nie jest tą najchętniej atakowana kategorią komputerów (6,3%). Relatywnie większym zainteresowaniem cieszą się komputery z grupy "rządowe" , z których a? 8,7% było próbkowanych w tym samym okresie. Największym, w stosunku do ich ilości, zainteresowaniem włamywaczy cieszą się komputery z grupy: komercyjni (14,6% próbkowanych hostów).


PROCENT WSZYSTKICH PRÓBKOWANYCH HOSTÓW
W DANEJ DOMENIE
16
12
6
0
14,6%
8,7%
6,3%
5,9%
7,1%
com.pl
gov.pl
edu.pl
inne
wszystkie
Domeny