Raport CERT NASK za rok 1999

W stosunku do roku 1998 CERT NASK w roku 1999 odnotował wzrost liczby zarejestrowanych incydentów naruszających bezpieczeństwo. Nie był to jednak tak duży wzrost jak w latach poprzednich. W roku 1999 liczba zarejestrowanych incydentów niewiele przekroczyła 100. Trzeba podkreślić, że rejestrowane są tylko oficjalne zgłoszenia (najczęściej pocztą elektroniczną), które dotyczą rzeczywistych przypadków związanych z naruszeniem bezpieczeństwa lub rażącym naruszeniem netykiety.

Typologia ataków

Wśród ataków największy procent dotyczy ataków wykorzystujących rozmaite metody skanowania poszczególnych komputerów w sieci Internet (hostów) a także skanowania całych podsieci. Łatwy dostęp do oprogramowania służącego do skanowania, często reklamowanego pod hasłem ,,sprawdź bezpieczeństwo swojego komputera" niewątpliwie poważnie przyczyniło się do popularności tego typu ataku. Wciąż popularne są też ataki na serwer z wykorzystaniem oprogramowania typu common gateway interface (CGI) wskazujących na chęć przejęcia istotnych informacji przez intruza z serwera WWW. Prawie 10% przypada w roku 1999 na ataki typu blokowanie usługi (DoS - Denial of Service) a światowe wydarzenia z początku roku 2000 potwierdzają coraz

większe zainteresowanie intruzów taką formą ataków. CERT NASK odnotowuje także przypadki tzw. uciążliwego spamu to jest spamu, wielokrotnym źródłem którego są ci sami użytkownicy, lub którego zakres negatywnego oddziaływania jest duży. Takich przypadków CERT NASK odnotował ponad 12 % z całej liczby incydentów. Z uwagi na wzrost ilości pojawiającego się w Internecie spamu CERT NASK nie jest jednak w stanie obsługiwać wszystkich przypadków związanych z tym zjawiskiem. Co warte podkreślenia spośród zarejestrowanych w 1999 roku incydentów 11% stanowiły typowe przypadki włamań.

Źródła ataków

Wśród prawdopodobnych źródeł ataków podobnie jak przed rokiem poważny procent zajmują adresy z umownie określanej sfery akademicko-naukowej. Nie jest to już jednak jak w poprzednich latach grupa dominująca. W roku 1999 największy procent ataków pochodził z kont w firmach komercyjnych. Drugą dużą grupę źródeł ataków stanowiły konta i dostawców internetu oraz publiczny dostęp do sieci poprzez TP S.A.

Efekt ataków

Podobnie jak rok wcześniej wśród zarejestrowanych ataków więcej jest tych, które wg zgłaszających zostały skutecznie odparte, niż tych które skończyły się przejęciem przez intruza praw administratora systemu. Potwierdza to fakt, że tylko nieliczne incydenty zgłaszane są do oficjalnych statystyk, i rzadko, kto chce się przyznawać do tego, że jego sieć została skutecznie zaatakowana. Jest to zjawisko ogólnoświatowe. Niestety największy procent odnosi się do sytuacji, w której poszkodowany nie jest w stanie ustalić poniesionych strat i często nie ma na to już szans gdyż system jest niezwłocznie reinstalowany.

Cel ataku i źródło zgłoszenia

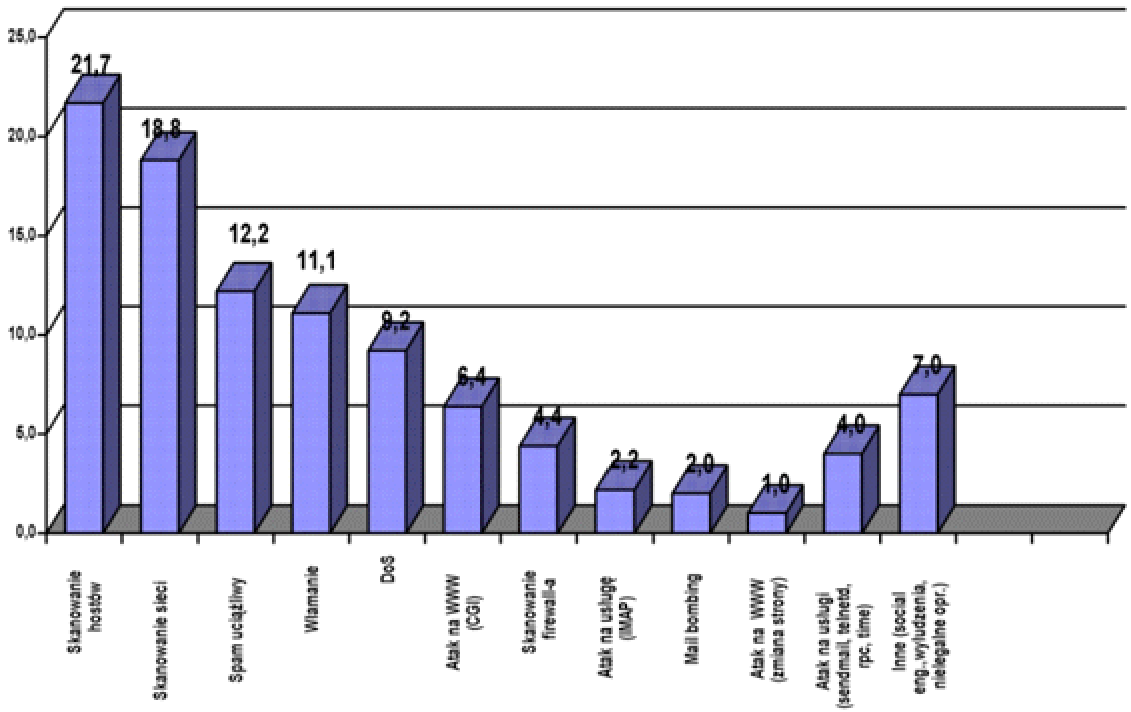
Większość, blisko 75%, zgłaszanych do CERT NASK incydentów pochodzi od użytkowników sieci - z czego około połowa to użytkownicy polscy a połowa to użytkownicy zagraniczni. Pozostałe 25% zgłoszeń pochodzi od instytucji, które w swojej działalności zajmują się walką z nadużyciami w sieci czyli innych zespołów reagujących (IRT) lub Policji, ze zdecydowanym wskazaniem na te pierwsze. Wśród poszkodowanych - podobnie ja w roku 1998 - dokładnie 50 % jest użytkowników zagranicznych i 50 % użytkowników polskiej sieci Internet. Wśród użytkowników polskich procentowo największą grupę docelową ataków stanowią jednostki naukowe bądź akademickie (20%) oraz firmy prywatne (ok.12%). Pokaźny procent ataków dotyczy także operatorów i dostawców usług telekomunikacyjnych. W roku 1999 zaobserwowano także utrzymywanie się trendu powstawania w ramach struktur firmowych zespołów lub osób odpowiedzialnych za sprawy bezpieczeństwa teleinformatycznego. CERT NASK częstokroć pełni rolę koordynacyjną w wymianie informacji między zainteresowanymi użytkownikami i zespołami bezpieczeństwa, ze szczególnym uwzględnieniem spraw międzynarodowych.

Problemy z typologią i klasyfikacją

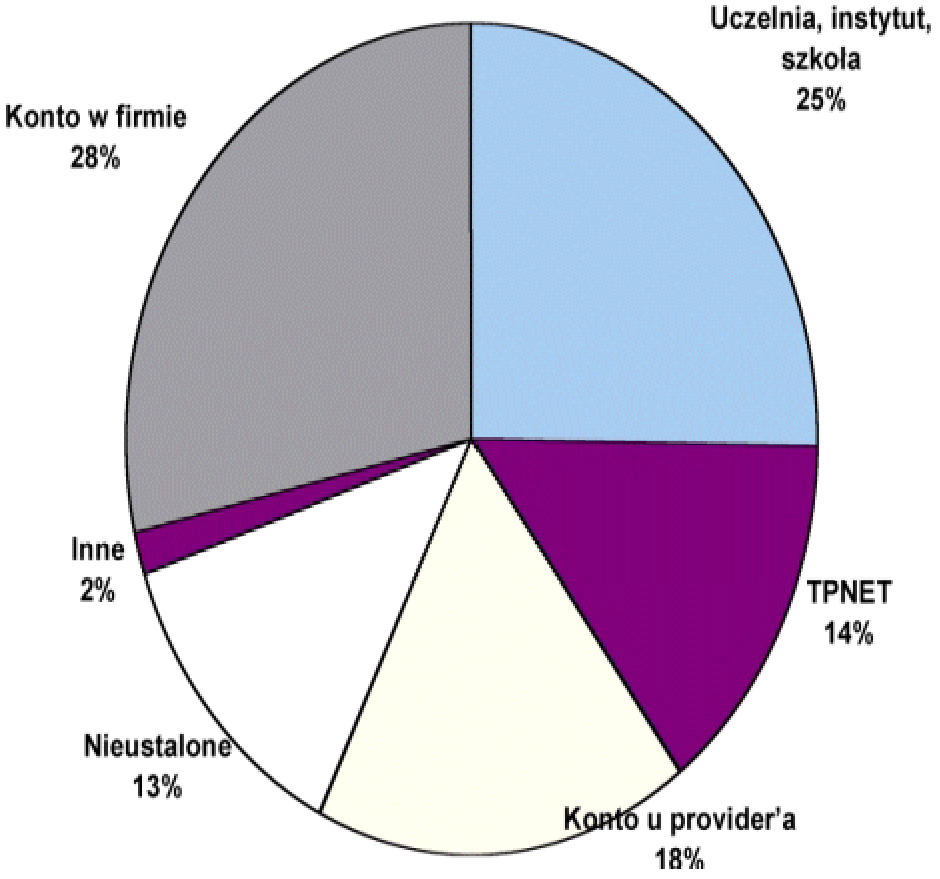
Przygotowując rokrocznie statystyki rejestrowanych incydentów CERT NASK napotyka na problem braku spójnej klasyfikacji i typologii ataków, którą można by się posłużyć w celu sklasyfikowania i zaprezentowania danych w taki sposób aby w możliwie standardowy sposób operować pojęciami związanymi z typami ataków. Niestety na świecie nie istnieje wspólny, obowiązujący wszystkich język pojęciowy w zakresie zdarzeń naruszających bezpieczeństwo sieci. Pewne próby stworzenia jednoznacznych klasyfikacji zostały podjęte w USA oraz w dwóch krajach europejskich - daleko jest jednak do stworzenia jakiegoś standardu. W ubiegłym roku CERT NASK podjął lokalnie pracę nad stworzeniem zrębów nowoczesnej klasyfikacji. Zespół chętnie udostępni wyniki swych prac w tym zakresie wszystkim zainteresowanym.

Poniżej przedstawiono kilka diagramów ilustrujących dane statystyczne zebrane w ramach pracy CERT NASK w roku 1999.

Wykres nr1. Procentowy rozkład typów ataków, 1999.



Wykres nr 2. Procentowy rozkład źródła ataków,1999.



Wykres nr 3. Procentowy rozkład źródła zgłoszenia ataków, 1999.