Raport CERT NASK 1998

Podobnie jak w roku 1997, również w roku 1998 odnotowaliśmy poważny wzrost liczby zarejestrowanych incydentów naruszających bezpieczeństwo.

Rozkład czasowy

Ataki te odnotowywane były w przeciągu całego roku z nasileniem na takie miesiące jak marzec i październik, szczególne nasilenie tego procesu w październiku może być spowodowane aktywnością środowiska akademickiego, z którego jak wskazuje statystyka wywodzi się najwięcej ataków.

Typ ataku

Wśród ataków prym wodzą te, które jako cel obrały sobie system poczty elektronicznej. Poważna część z tych ataków związana jest z popularnością, i dużą ilością dziur w oprogramowaniu sendmail. Poważnym problemem okazało się też skanowanie sieci, czy też pojedynczych komputerów. Ogólnodostępność oprogramowania służącego do skanowania, często reklamowanego pod hasłem "sprawdź bezpieczeństwo swojego komputera" niewątpliwie poważnie przyczyniło się do popularności tego typu ataku. Również niezwykle łatwy atak na serwer z wykorzystaniem oprogramowania typu common gateway interface (CGI) sprawiło, że wśród zgłoszonych incydentów wiele było tych, które wskazywały na chęć przejęcia istotnych informacji przez intruza w ten właśnie sposób.

Źródło ataków

Tak jak było już wspomniane wcześniej prym w tej kategorii wiedzie środowisko akademickie. Nie jest to zjawiskiem nowym w odróżnieniu do tego co dotyczy sieci TPNET. "Darmowy" dostęp do sieci stał się w zeszłym roku doskonałym sposobem na ukrycie swojej tożsamości, przynajmniej

zdaniem intruzów. Aktywna działalność CERT NASK, poparta zdecydowanym głosem środowiska internautów, niewątpliwie przyczyniła się do ograniczenia tego zjawiska, czego efekty są już widoczne. W strukturach TP S.A. powstał dedykowany zespół odpowiedzialny za tego typu przypadki, uruchomiono procedury organizacyjne i techniczne, które prowadzą do zdecydowanego ograniczenia zjawiska. Także współpraca z firmami udostępniającymi na swych serwerach darmowe konta dla internautów niewątpliwie przyniosła efekty, które widać w niewielkiej ilości incydentów powiązanych właśnie z darmowymi kontami.

Efekt ataków

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.

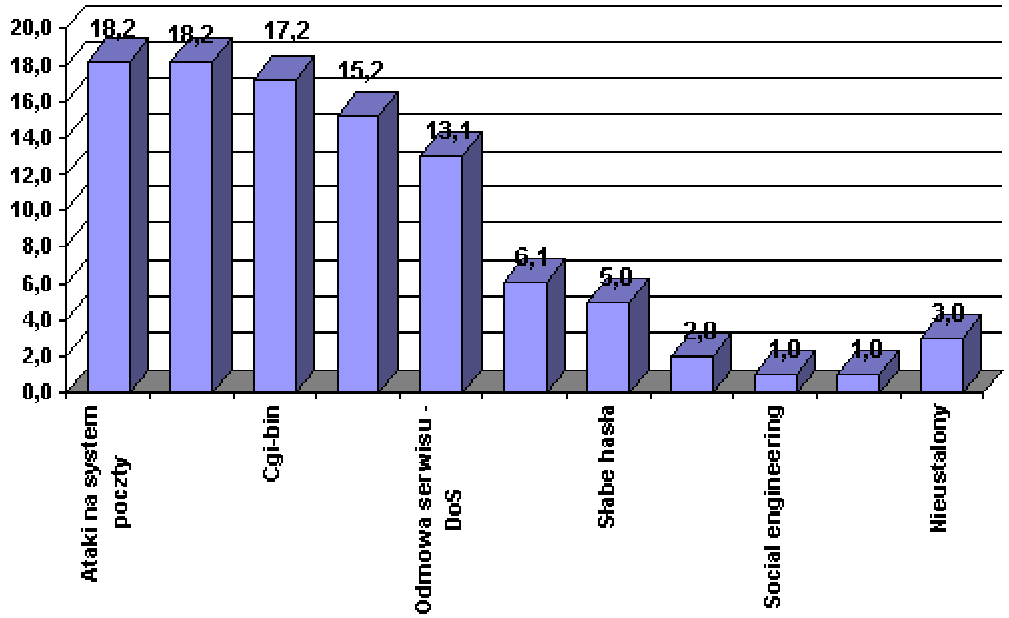
Niestety największy procent odnosi się do sytuacji, w której poszkodowany nie jest w stanie ustalić poniesionych strat i często nie ma na to już szans gdyż system, który musi działać w trybie natychmiastowymi jest reinstalowany.

Cel ataku i źródło zgłoszenia

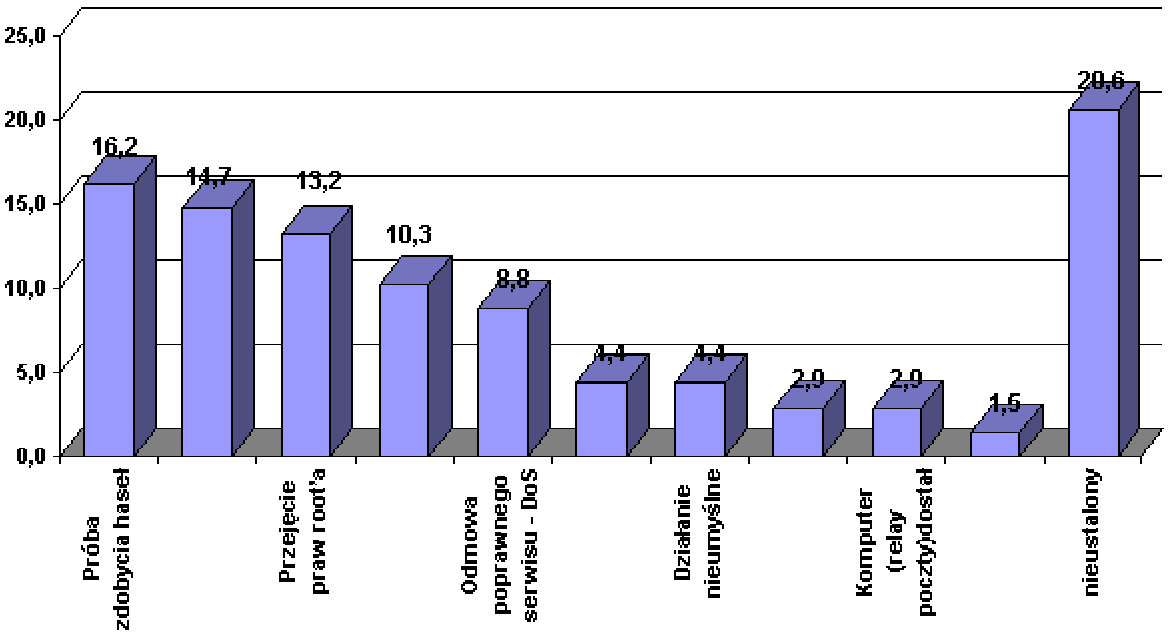
Większość, blisko 80%, zgłaszanych do CERT NASK incydentów pochodzi od niezależnych użytkowników sieci, głównie przedstawicieli firm i instytucji. Pozostałe, niewiele ponad 20% zgłoszeń pochodzi od instytucji, które w swojej działalności zajmują się walką z przestępczością komputerową, czyli innych zespołów reagujących (IRT) lub Policji, ze zdecydowanym wskazaniem na te pierwsze. Wśród poszkodowanych dokładnie 50 % jest użytkowników zagranicznych i 50 % użytkowników polskiej sieci Internet. Na negatywne oddziaływanie intruzów bardziej uczuleni wydają się być użytkownicy zagraniczni. Przyczyną takiego stanu rzeczy jest z jednej strony większa wrażliwość użytkownika zagranicznego na nieuprawnioną działalność intruzów, zaś z drugiej dotychczasowe przekonanie o bezkarności i często anonimowości intruza jakie panuje wśród polskich internautów. Na szczęście opinia ta się zmienia, na co wpływ ma bardziej szczegółowa kontrola dostępu (funkcja rozliczalności) wśród polskich provider'ów (w szczególności chodzi tu o TP S.A.) oraz wprowadzenie nowego kodeksu karnego, który w większym stopniu daje szansę dochodzenia krzywd na drodze prawnej.

Z pozytywnych zmian zaobserwowanych w ramach naszej działalności jest powstawanie w ramach struktur firmowych zespołów lub osób odpowiedzialnych za sprawy bezpieczeństwa teleinformatycznego. Wskazuje to poniekąd podstawową rolę dla zespołów reagujących, takich jak CERT NASK, wydaje się nim być koordynacja w wymianie informacji między zainteresowanymi, ze szczególnym uwzględnieniem spraw międzynarodowych.

Wykres nr1. Procentowy rozkład typów ataków, 1998.



Wykres nr 2. Procentowy rozkład efektów ataków, 1998.



Wykres nr 4. Procentowy rozkład źródła zgłoszenia ataków, 1998.