CERT POLSKA

Raport 2000

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). W ramach tej 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

1.2 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 piątym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.net.pl/statystyki.html)

2 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[1]

Poniżej przedstawione zostały statystki dotyczące PNBT. W statystykach odrębnie potraktowano przypadki przesyłania (otrzymywania) nie zamawianej poczty elektronicznej, zwanej popularnie tzw. spamem. Decyzję taką podjęto ze względu na niewspółmiernie dużą liczbę tych przypadków w stosunku do przypadków pozostałych. Przypadki spamu zostały odnotowane oddzielnie, w rozdziale specjalnie temu poświęconym.

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

2.1 Ilość przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2000 odnotowano 126 PNBT.

2.2 Ilość zaatakowanych komputerów

W 126 PNBT zaatakowano 292 komputery (hosty). Znacząca ich część – 206, co stanowi ponad 70% powiązana była z przypadkami włamania do systemu (182 przypadki) i próbami włamania do systemu (24 przypadki), czyli z najgroźniejszymi PNBT.

2.3 Typy odnotowanych ataków

Dokonano analizy rozkładu procentowego typów ataków zarówno w ujęciu ilości PNBT, jak też ilości zaatakowanych komputerów. Jak wynika z poniższych danych rozkłady te zasadniczo się różnią.

2.3.1 Typy odnotowanych ataków w ujęciu PNBT

Największy procent typów PNBT stanowiły próby włamania do systemów – 19% (24 przypadki). Następnie odnotowano taki sam udział procentowy włamań i skanowania hostów (15%, 19). Poniżej zestawienie wszystkich typów PNBT:

- Próba włamania do systemu – 19% (24)
- Włamanie do systemu – 15% (19)
- Skanowanie hosta – 15% (19)
- Skanowanie sieci – 13% (17)
- Ataki DoS (*ang. Denial of Service*) – 13% (16)
- Ataki na WWW serwer (podmiana strony) – 6% (8)
- Mail bombing – 5% (6)
- Skanowanie firewall – 3% (4)
- Inne (nielegalne oprogramowanie, social engeenering) – 10% (13)

Wszystkie przypadki skanowania (host, firewall, sieć) stanowią łącznie blisko 32% wszystkich PNBT i zdecydowanie jako łączna kategoria wysuwają się na czoło klasyfikacji.

2.3.2 Typy odnotowanych ataków w ujęciu zaatakowanych komputerów

W sytuacji rozważania rozkładu typów ataków w ujęciu zaatakowanych komputerów sytuacja zmienia się dosyć znacząco. Tu zdecydowanie na pierwszy plan wybijają się przypadki włamania – 62% (182). Łączny procent różnego rodzaju skanowania (firewall, host, sieć) wynosi 14% (40). Poniżej zestawienie wszystkich typów:

- Włamanie do systemu – 62% (182)
- Próby włamania – 8% (24)
- Ataki DoS (*ang. Denial of Service*) – 7% (19)
- Skanowanie hosta – 7% (19)

- Skanowanie sieci – 6% (17)
- Ataki na WWW serwer (podmiana strony) – 3% (8)
- Mail bombing – 2% (6)
- Skanowanie firewall – 1% (4)
- Inne (nielegalne oprogramowanie, social engeenering) – 4% (13)

2.3.3 Spam

Zdecydowanie największą ilość PNBT stanowiły przypadki spamu, dlatego z pewnych względów (wyjaśnienie powyżej na początku rozdziału) zostały one potraktowane oddzielnie.

Odnotowywane przypadki spamu wiązały się z pewnością z używaniem narzędzi automatycznych do generacji spamu. Przypadki jakie zostały zgłoszone do CERT POLSKA pochodziły głównie z sieci da.uu.net.

W ciągu roku do CERT POLSKA zgłoszono ponad 1 200 przypadków spamu.

2.4 Źródła odnotowanych ataków

Głównym źródłem odnotowanych ataków były sieci nadzorowane przez ośrodki edukacyjne, takie jak wyższe uczelnie, szkoły (głównie szkoły średnie) oraz instytuty naukowe. Łącznie wszystkie te ośrodki stanowiły 42% (53) źródeł odnotowanych PNBT.

Źródłem 29% (36) PNBT był intruz korzystający z zasobów dostarczyciela usługi internetowej (*ang. Internet Service Provider)*, z czego około 9% powiązanych było z adersami IP ogólnie dostępnej sieci publicznej.

15% (19) PNBT powiązanych było z kontem firmowym jako źródłem ataku.

Najmniej znaczący procent - 7% (9) stanowiły źródła inne.

Również 7% (9) stanowiły przypadki, w których nie ustalono źródła ataku.

2.5 Źródła zgłoszenia incydentów

W przypadku źródła zgłoszenia incydentu wyróżniano 3 kategorie: CERT lub inna instytucja ds. bezpieczeństwa, użytkownik krajowy, użytkownik zagraniczny. W tej materii procent przypadków rozkłada się mniej więcej równo i wygląda następująco:

- Użytkownik krajowy – 35% (45)
- Użytkownik zagraniczny – 33% (41)
- CERT lub inna instytucja ds. bezpieczeństwa – 32% (40)

3 Wnioski

Biorąc pod uwagę niewielki procent zgłaszania incydentów (różne źródła podają wielkości rzędu kilku procent) szacowana liczba zgłoszonych incydentów a tym samym ilości incydentów w polskich zasobach Internetu nie jest mała. Nadal niestety jednak odnotowuje się dużą niechęć do zgłaszaniu incydentów. Powody są różne, ale z pewnością w największej mierze

decydują te, które dotyczą obawy przed utratą wizerunku firmy jako firmy bezpiecznej co na mocnym, konkurencyjnym rynku jest zadaniem niezwykle ważnym.

Z dużym prawdopodobieństwem, można zaryzykować stwierdzenie że odnotowany niewielki procent przypadków związanych z atakami blokującymi serwisy nie do końca odpowiada rzeczywistości. Ubiegły rok na całym świecie stał pod znakiem skomasowanych ataków DDoS i DoS, które dotknęły nie jedną, także te największe, firmę. Być może ataki tego typu stały się na tyle powszechne, że przestano je zgłaszać traktując jako normalną część związaną z obsługą urządzeń sieciowych dołączonych do Internetu. Jednak należy zastrzec, że są to tylko przypuszczenia i CERT Polska nie posiada szczegółowych danych na ten temat.

W trakcie obsługi zgłaszanych incydentów dosyć wyraźnie zarysował się fakt nie posiadania przez pokrzywdzonych odpowiednich procedur, które pozwalają na usystematyzowane działanie w przypadku wystąpienia zagrożenia. Często wynikiem braku tych procedur jest chaotyczne działanie, które w pierwszej kolejności przekłada się na reinstalację zaatakowanego systemu, co oczywiście jest skuteczne z punktu widzenia działania serwisu (choć czasami niestety nie na długo), ale uniemożliwia skuteczne pozyskanie informacji zmierzających do ustalenia sprawcy przestępstwa komputerowego.

Choć niewątpliwe stan świadomości dotyczącej bezpieczeństwa teleinformatycznego jak i sam poziom tego bezpieczeństwa poprawił się w ciągu kilku ostatnich lat to nadal napotykamy na przypadki elementarnych błędów związanych z wdrożeniem i obsługą systemów informatycznych.

4 Trendy

CERT Polska prowadzi swoje statystyki od 1996 roku. Począwszy od tego czasu liczba odnotowywanych incydentów stale rośnie.

W swoich obserwacjach odnotowaliśmy coraz więcej zgłaszanych incydentów, które nie kończą się sukcesem intruza ale naruszają w pewien sposób bezpieczeństwo zaatakowanych systemów, chociażby poprzez obciążenie osób odpowiedzialnych za ich bezpieczeństwo dodatkowymi obowiązkami kontroli i audytu zaatakowanego systemu. Świadczy to niewątpliwie o wzroście świadomości wśród polskich internautów. Coraz mniej jest tych którzy nie potrafią odpowiedzieć jednoznacznie na pytanie czy ich sieć była atakowana czy też nie.

Typy odnotowywanych ataków w drastyczny sposób się nie zmieniają na przestrzeni lat. Od lat najbardziej popularne są ataki na system poczty elektronicznej, ataki polegające na skanowaniu poszczególnych komputerów czy też całych sieci, ataki na serwery WWW, ataki zmierzające do blokady serwisu. Pewne ataki całkowicie lub częściowo zniknęły z naszej mapy typologicznej. Rzadziej odnotowujemy ataki bezpośrednio na konta użytkowników czy też na serwery *news*. Częściej występują bezpośrednie ataki na aplikacje i procesy. Na początku działalności naszej organizacji ataki te były znacznie bardziej popularne. Popularność tę w dniu dzisiejszym przejęły głównie ataki związane ze skanowaniem.

Od lat stałym elementem rejestrowanego zestawu typologicznego jest również spam, który szczególnie w zeszłym roku przyjął gigantyczne rozmiary.

5 Tabela zbiorcza

Typy odnotowanych ataków

Typ	*Ujęcie – PNBT*		*Ujęcie – host*	
	Procent	*Ilość*	*Procent*	*Ilość*

Włamanie do systemu	15	19	62	182
Próba włamania do systemu	19	24	8	24
Skanowanie sieci	13	17	6	17
Skanowanie host'a	15	19	7	19
Skanowanie firewall'a	3	4	1	4
Ataki DoS	13	16	7	19
Ataki na WWW	6	8	3	8
Mail bombing	5	6	2	6
Inne	10	13	4	13
Ogółem	**100**	**126**	**100**	**292**

Źródła odnotowanych ataków

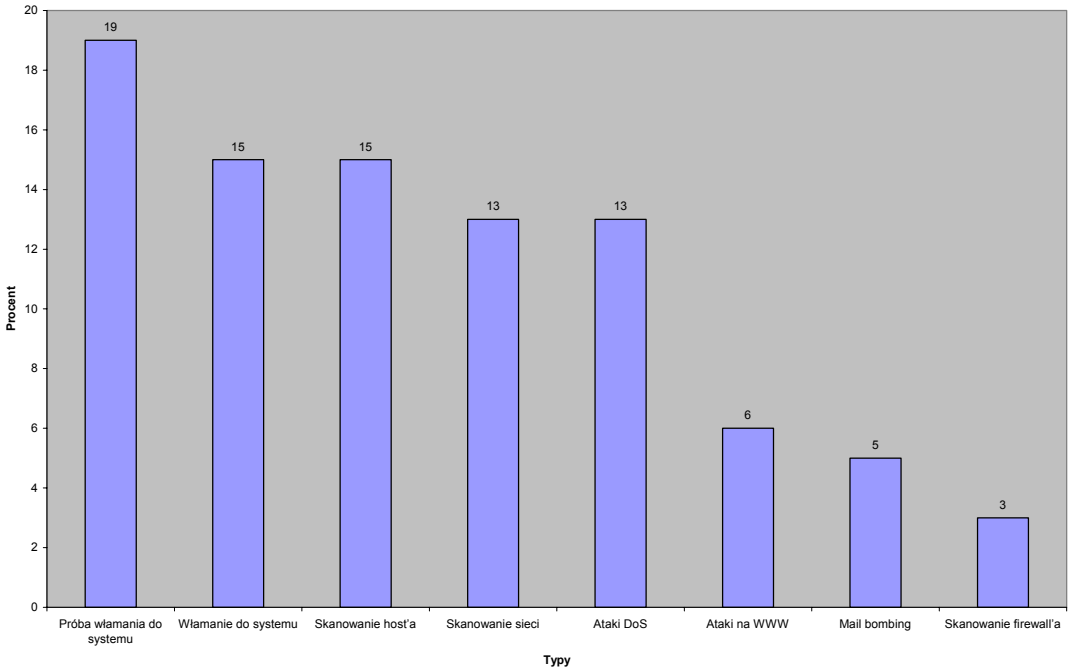
Źródło	*Procent*	*Typ*
Ośridki edukacyjne	42	53
ISP	29	36
Firma	15	19
Inne	7	9
Nieustalone	7	9
Ogółem	**100**	**126**

Źródła zgłoszenia incydentów

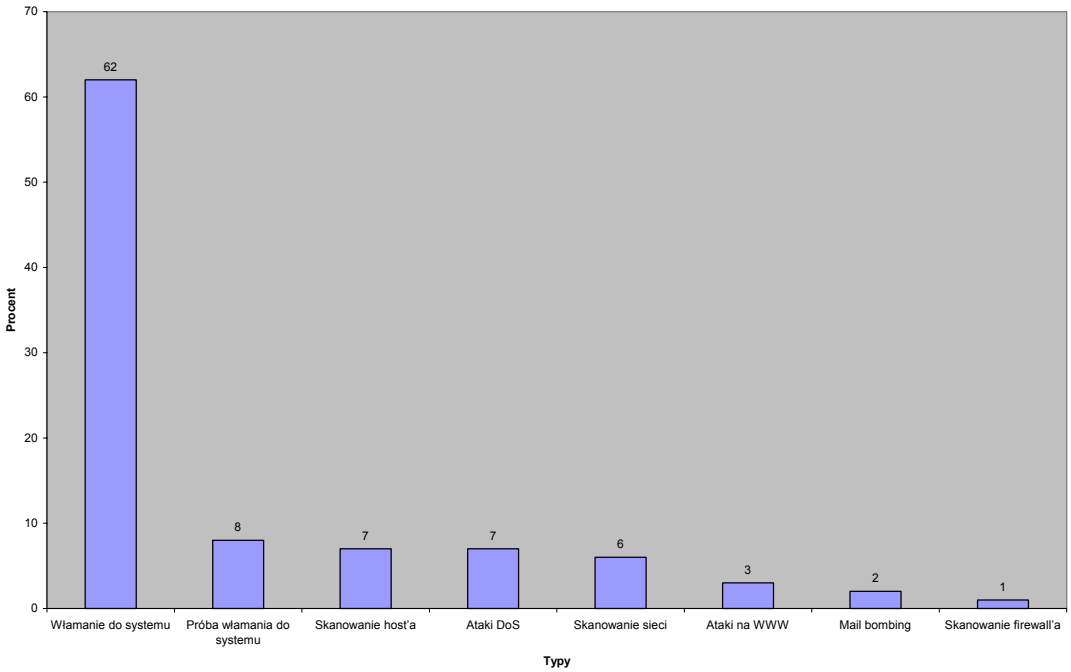
Źródło	*Procent*	*Typ*
Użytkownik krajowy	35	45
Użytkownik zagraniczny	33	41
CERT lub instytucja ds. Bezpieczeństwa	32	40
Ogółem	**100**	**126**

6 Wykresy

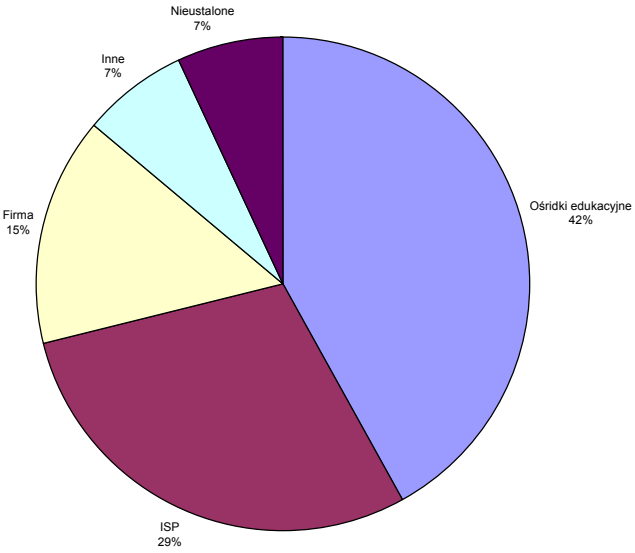
Typy ataków w ujęciu PNBT



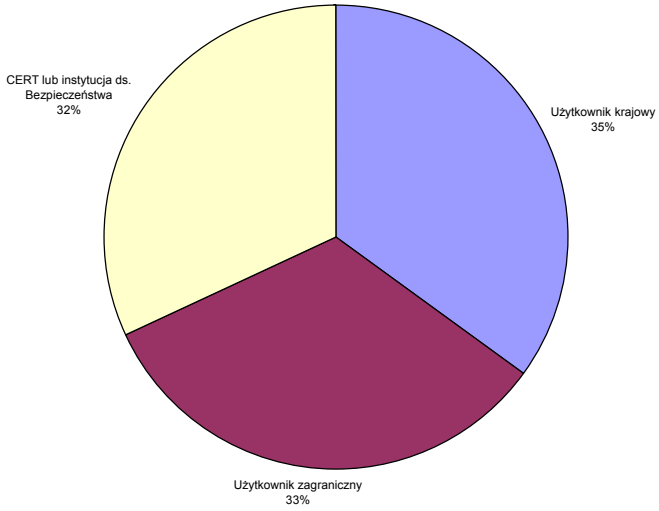
Typy ataków w ujęciu zaatakowanych hostów



Źródła ataków



Źródła zgłoszenia ataków



7 Kontakt

e-mail: cert@cert.pl

Web site: http://www.cert.pl/

Adres: CERT POLSKA

ul. Bartycka 18

00-716 Warszawa

tel./fax: 00 48 22 5231274