Cyber-zagrożenia

Zagrożenia współczesnych technologii teleinformatycznych z punku widzenia organów ścigania w globalnej sieci Internet

Wydział dw. z Cyberprzestępczością

Komenda Wojewódzka Policji

w Bydgoszczy

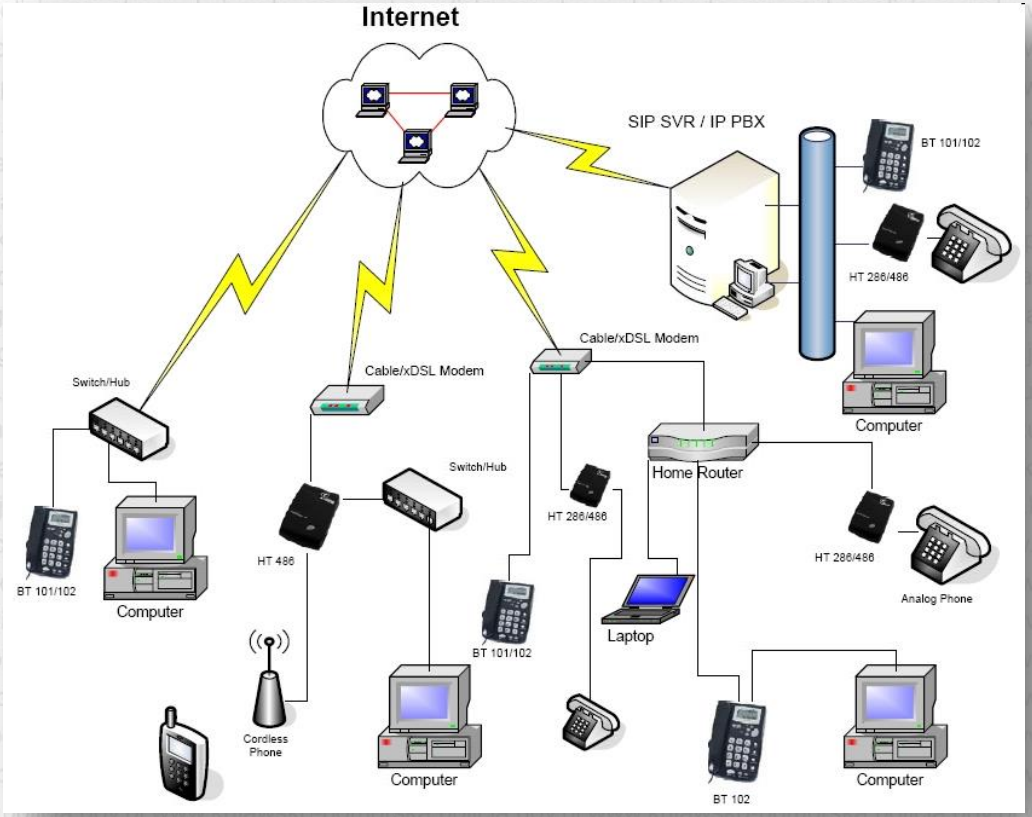
STRUKTURA WYDZIAŁU

NACZELNIK

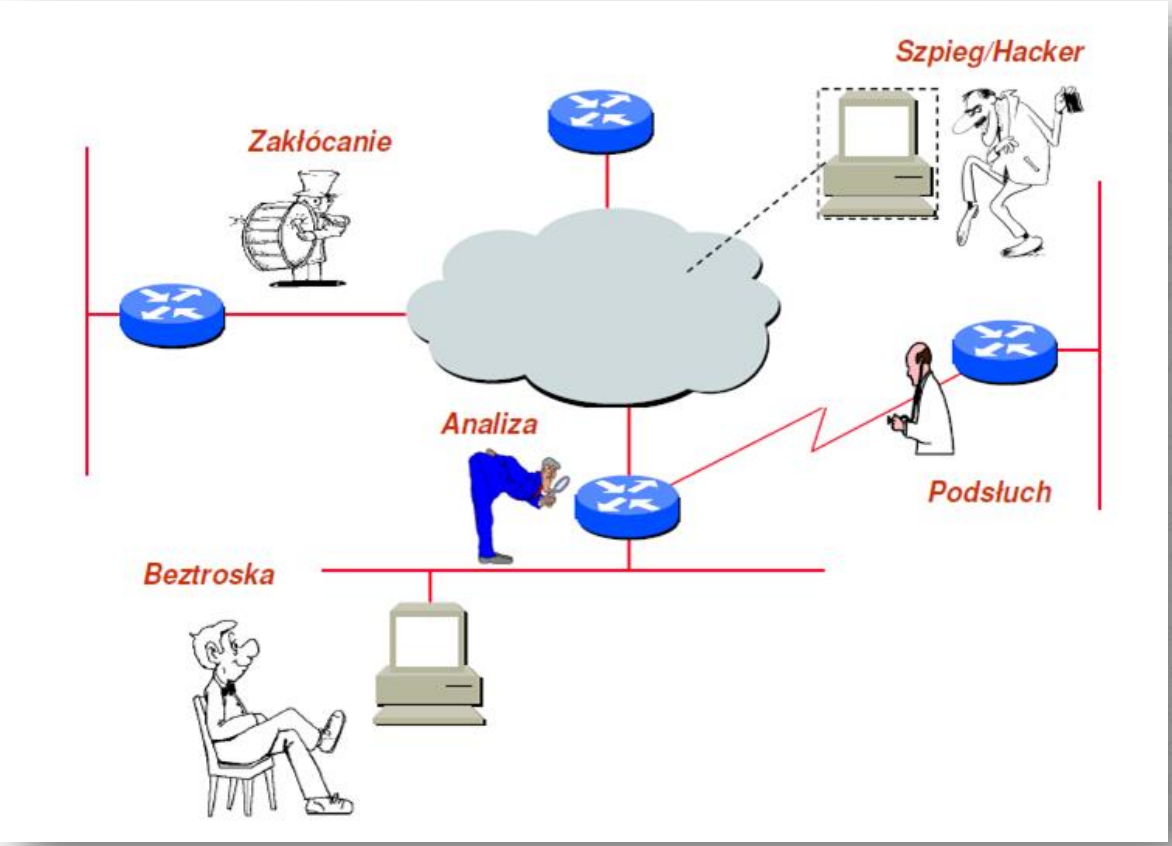
- Zespół Dochodzeniowo-Śledczy
- Zespół Operacyjno-Rozpoznawczy
- "Informatyka śledcza"

INTERNET

- Globalna sieć



ZAGROŻENIA



NADUŻYCIA

- Nadużycia finansowe/Defraudacja środków finansowych,
- Nadużycia dotyczące etyki,
- Wyciek/Kradzież danych,
- Kradzież projektów,
- Celowe niszczenie danych,
- Szpiegostwo przemysłowe,
- Łamanie praw autorskich,
- Ujawnienie tajemnicy handlowej,
- Kradzież i użycie danych osobowych,
- Sprawy kryminalne (handel narkotykami, terroryzm, morderstwa, samobójstwa, zorganizowana przestępczość, pedofilia).

UKRYWANIE TOŻSAMOŚCI

- Transmisja między komputerem, a serwerami WWW,
  - prawdziwy adres IP zostanie zamaskowany podczas odwiedzania stron internetowych,
  - prawdziwy adres będzie zapisany tylko w dziennikach zdarzeń serwera Proxy.

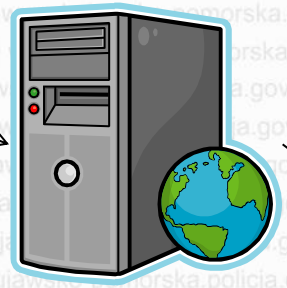
POLICJA

PRZYKŁAD

Hacker

111.111.111.111

Serwer PROXY



333.333.333.333

Docelowy

222.222.222.222

MOTYWY WŁAMAŃ

- "Darmowy dostęp do Internetu" – włamywacz korzysta z darmowego łącza do sieci Internet nie ponosząc dodatkowych kosztów.
- "Szpiegostwo" – włamywacz zostaje wynajęty przez inną osobę lub instytucję w celu włamania i zdobycia lub podmiany informacji w zamian za pieniądze. Szpiedzy mają określony cel i zadanie i atakują konkretny system komputerowy.
- "Nuda i żart" – włamywacz z powodu nudy próbuje uzyskać dostęp do innych komputerów. Przeważnie do włamania wykorzystywane są gotowe skrypty lub programy napisane przez inne osoby.

MOTYWY WŁAMAŃ

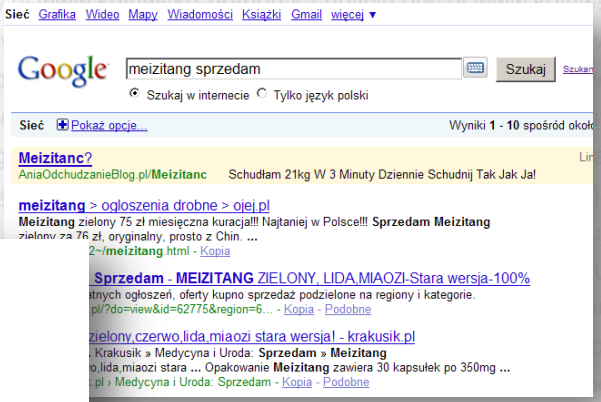
- "Rozgłos" – włamywacz dla rozgłosu włamuje się na znane i w miarę dobrze zabezpieczone serwery/komputery w celu udowodnienia swoich umiejętności.
- "Zemsta" – włamywacz to były pracownik firmy, zwolniony z rożnych względów. Głównym zamiarem jest zaszkodzenie firmie, której pracował.
- "Ignorancja" – włamywacz w trakcie poznawania nowych metod i technik, próbuje przełamać zabezpieczenia innych komputerów.
- "Wandalizm" – włamywacz dla własnej satysfakcji niszczy zasoby innych użytkowników.

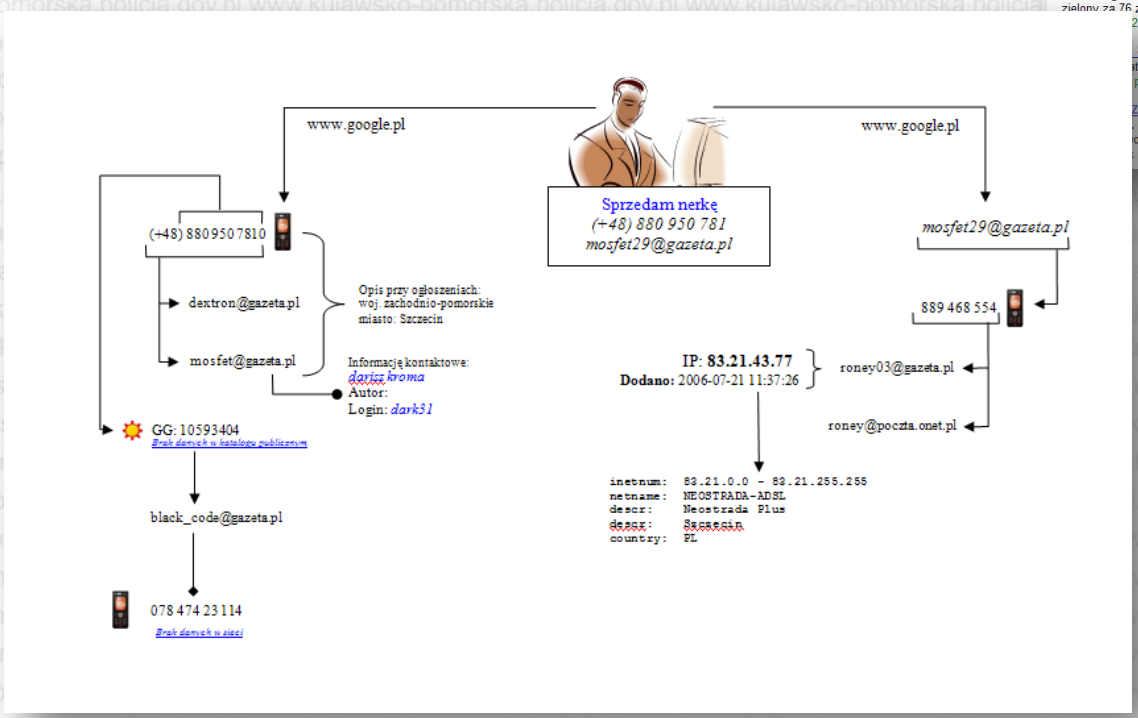
METODY WŁAMAŃ

- **Zbieranie informacji**
  - zebranie jak największej ilości informacji o systemie i użytkowniku z ogólnie dostępnych źródeł taki jak np. strona WWW, książka telefoniczna, prasa, telewizja, itp. W dalszym etapie następuje skanowanie sieci w celu określenia topologii, widocznych hostów, urządzeń sieciowych. Na tym etapie następuje wybranie potencjalnego celu oraz wybór techniki jaka będzie użyta do ataku.
- **Wtargnięcie**
  - próba jak i wejście do chronionego systemu oraz nadanie sobie maksymalnych uprawnień. Ponieważ atak obarczony jest ryzykiem wykrycia musi być przeprowadzony szybko i precyzyjnie.
- **Opuszczenie systemu**
  - modyfikacja przejętego systemu w taki sposób, aby można było się do niego dostać w późniejszym terminie bez konieczności przełamywania zabezpieczeń. Na tym etapie zakładane są wszelkiego rodzaju tylne wejścia, zmieniana jest też konfiguracja systemu na przejętym komputerze.
    W dalszej kolejności następuje zacieranie śladów włamania.

WYSZUKIWANIE INFORMACJI

- Podstawowe techniki wyszukiwania informacji,
- Zaawansowane techniki wyszukiwania informacji,
- Wyszukiwanie prywatnych / poufnych danych.





PORTALE SPOŁECZNOŚCIOWE

Z komputera użytkownika:

Analiza protokołu wymiany danych na portalu społecznościowym zwykle pozwala na znalezienie śladów:

- znajomych,
- dodawanych komentarzy,
- tworzonych wydarzeń,
- wysyłania komunikatów o wydarzeniu do grupy,
- zapisów czatów.

POLICJA

Wydział dw. z Cyberprzestępczością

Komenda Wojewódzka Policji w Bydgoszczy
ul. Powstańców Wlkp. 7
85-090 Bydgoszcz

Tomasz Boroń & Marcin Matysek