VoIP:
Klient jednego fraudu

Marcin Gala – Datera *galam@datera.pl*
Radosław Trojakowski – Crowley *r.trojakowski@crowley.pl*

Agenda

Fraud

- Czym jest?
- Dlaczego w ogóle jest?
- Rodzaje nadużyć na VoIP
- „Doświadczeni”
- Objawy, profilaktyka, leczenie
- Jak jest w Polsce?

CROWLEY

Czym jest fraud?

DATERA

Czym jest fraud?

FRAUD - nadużycie:

- świadome oszustwo celem uzyskania korzyści majątkowej lub wyrządzenia szkody drugiej stronie (podmiot prawny, osoba prywatna)
  - kradzież
  - korupcja, przekupstwo, deprawacja
  - przywłaszczenie, defraudacja
  - pranie pieniędzy
  - wyłudzenie

CROWLEY

Dlaczego ludzie popełniają fraud?

DATERA

Dlaczego ludzie popełniają fraud?

Dlaczego powstaje fraud? Jakie są przesłanki, które kierują ludźmi do popełnienia fraudu?

- Motywacja
- Możliwość
- Racjonalizacja

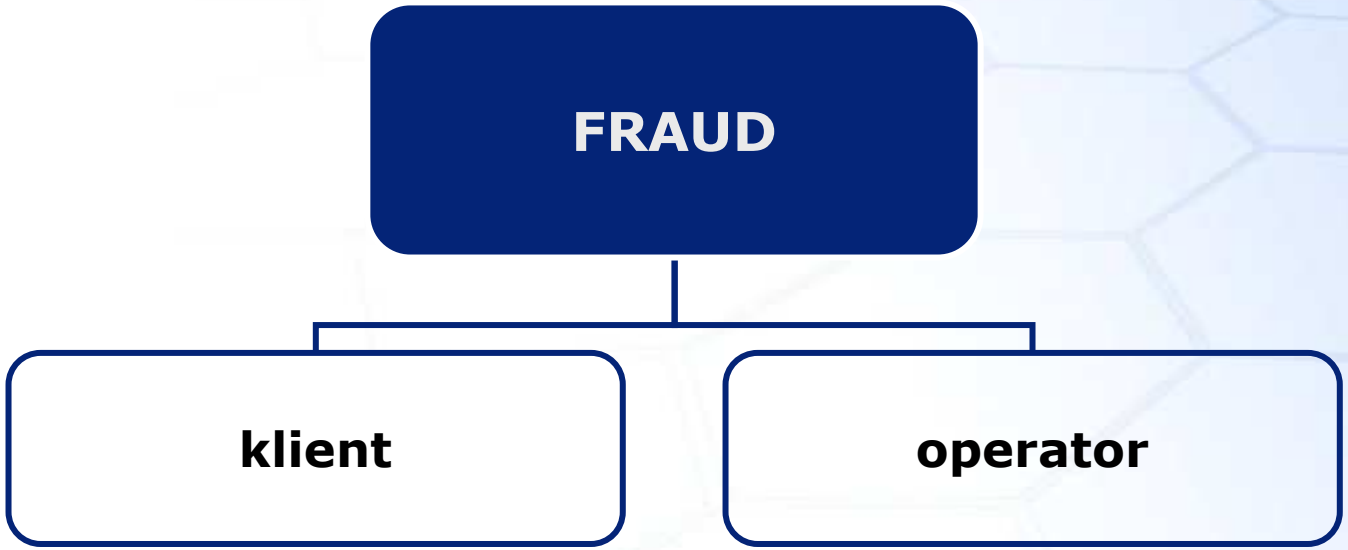
CROWLEY

Jakie są nadużycia w telefonii i na VoIPie?

DATERA

4 marca 2010

Kto jest poszkodowany?



Kto dokonuje fraudu?

Podmiot dostarczający content na numeracji, na którą realizowany jest fraud

Zwykły użytkownik

Dlaczego i jak dokonuje się fraudu w VoIP?

- W Polsce fraudy mają podłoże zarobkowe

Połączenia na numery:

- krajowe PREMIUM (0-70X)
- krajowe o podwyższonej opłacie
- międzynarodowe „egzotyczne”
- międzynarodowe PREMIUM
- międzynarodowe niegeograficzne (NGN) o podwyższonej opłacie
- inne ☺

CROWLEY

Mądry Polak po…

fraudzie…

DATERA

„Doświadczeni”

Mądry Polak po… fraudzie…

(1) Klient terminujący ruch głosowy na określone międzynarodowe strefy numeracyjne

Objawy:

- brak – spodziewany ruch

Fraud:

- brak sprecyzowanych w cenniku prefiksów (NGN)
- wygenerowanie ruchu międzynarodowego
- rzeczywisty koszt połączeń ok. **90.000 zł**

Działania i zabezpieczenia:

- aneksowanie cennika

„Doświadczeni”

Mądry Polak po… fraudzie…

(2) Klient terminujący hurtowo ruch głosowy

Objawy:

- niezauważalny wzrost liczby połączeń

Fraud:

- zaterminowanie ruchu z konta SIP zalogowanego z innego adresu IP
- wygenerowanie ruchu międzynarodowego
- rzeczywisty koszt połączeń **ok. 16.000 zł**

Działania i zabezpieczenia:

- zmiana hasła konta SIP
- ograniczenie przyjmowania ruchu od klienta – lista adresów IP

„Doświadczeni”

Mądry Polak po… fraudzie…

(3) Klient terminujący hurtowo ruch głosowy

Objawy:

- wystąpienie niespodziewanego ruchu w okresie świątecznym

Fraud:

- zaterminowanie ruchu przez klienta klienta
- wygenerowanie ruchu międzynarodowego (Kuba)
- rzeczywisty koszt połączeń **ok. 70.000 zł**

Działania i zabezpieczenia:

- zablokowanie przyjmowania ruchu przez operatora

„Doświadczeni”

Mądry Polak po… fraudzie…

(4) Klient

Objawy:

- nieustające połączenia międzynarodowe

Fraud:

- odgadnięcie hasła użytkownika na asterisku klienckim
- wygenerowanie ruchu międzynarodowego
- koszt **ok. 90.000 zł**

Działania i zabezpieczenia:

- zablokowanie przyjmowania ruchu przez operatora
- dedykowany VLAN na styku klient – operator

CROWLEY

Dlaczego fraudy częstsze na VoIPie?

DATERA

4 marca 2010

Dlaczego fraudy na VoIPie?

1. Specyfika systemów VoIP

- realizowane jako „ostatnia mila”, do której każdy ma dostęp, w odróżnieniu do fizycznej „ostatniej mili”
- często realizowane na otwartym Internecie, rzadziej w dedykowanej, zamkniętej sieci operatora
- stosunkowo niski koszt realizacji
- realizowane dla klienta niższych segmentów i często klienta anonimowego o bliżej nieokreślonej lokalizacji geograficznej

Dlaczego fraudy na VoIPie?

1. Specyfika systemów VoIP

- urządzenia abonenckie podatne na błędy, przez co wykorzystywane są jako generatory
- umożliwiają realizację wielu jednoczesnych połączeń
- pozwalają na podłączanie do nich praktycznie dowolnych urządzeń, w tym również niestandardowych

Dlaczego fraudy na VoIPie?

2. Podejście abonentów

- niepoprawny optymizm i przekonanie, że „to ich nie spotka”

- brak świadomości skali zagrożenia

  np. możliwości realizowania wielu połączeń jednocześnie

100 połączeń * 8 h * 60 min/h * 2 zł/min

czyli… 96 000 zł w 1 noc

Dlaczego fraudy na VoIPie?

2. Podejście abonentów

- dusigrosze – najważniejszy koszt, przez co oszczędzają na sprzęcie
- hasło „dupadupa” jako szczyt oryginalności
- przecenianie umiejętności konfiguracyjnych swoich urządzeń (asterisk)

Dlaczego fraudy na VoIPie?

3. Podejście operatora

Najważniejsza cena usługi, przez co:

- rezygnują z monitoringu 24/7
- rezygnują z automatycznego monitoringu umów i rozliczeń
- rezygnują z implementowania kosztownych zaleceń billingu (np. OCS – Online Charging System,

  CCF – Credit Control Function)
- rezygnują z wdrożenia i utrzymywania systemu antyfraudowego

Dlaczego fraudy na VoIPie?

2+3. Podejście operatora i abonenta

Niewłaściwe używanie ogólnodostepnych, darmowych systemów

- Brak zabezpieczeń
- Błędy konfiguracyjne
- Brak aktualizacji

Błędy systemowe

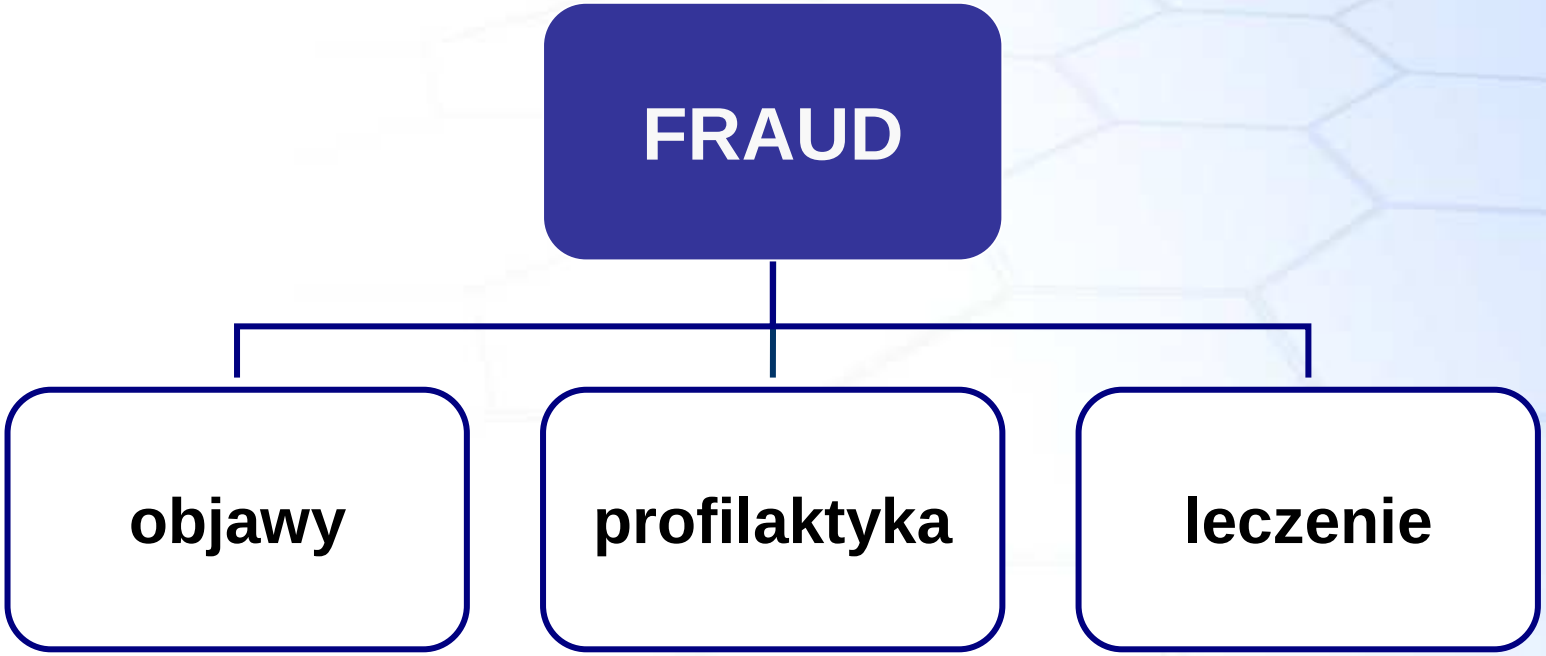
- Specyficzne scenariusze realizacji połączeń

CROWLEY

Kiedy wystąpi fraud?

Zawsze wtedy, kiedy nie pilnujemy ☺

DATERA


FRAUD
objawy
profilaktyka
leczenie

CROWLEY

Jakie są podstawowe objawy występowania fraudu na VoIPie?

DATERA

Objawy fraudu na VoIPie

Perspektywa operatora:

- nagły spadek średniego czasu trwania połączeń

- nagły wzrost liczby niepoprawnych rejestracji kont lub ruchu na interfejsach sieciowych (może ktoś skanuje Twoją sieć próbując łapać konta i hasła)

- nagły wzrost CDR typu NOANSWER (czy aby ktoś nie próbuje łowić naszych abonentów) ?

Objawy fraudu na VoIPie

Perspektywa operatora i klienta:

- szybki przyrost numerów i kont (albo nas fraudują, albo wykorzystują nas do fraudowania kogoś innego)

- nagły wzrost ruchu np. za granicę lub na komórki (nie ciesz się, jak ruch rośnie – sprawdź lepiej czy nie dopłacasz przypadkiem do interesu)

- nietypowy ruch w nocy lub w weekend

CROWLEY

Jak się zabezpieczać, aby minimalizować wystąpienie fraudu na VoIPie?

DATERA

Profilaktyka - sposoby zabezpieczeń

Perspektywa operatora (biznesowe):

- Sprawdzenie wiarygodności klienta
- Polityka wyjścia na numerację PREMIUM
- Aktualizacja cenników (prefiksów)
- Zapisy w umowie i regulaminie usługi dotyczące ograniczania możliwości realizacji połączeń w przypadku wystąpienia podejrzenia lub nadużycia
- Case studies – wiedza na przyszłość

Profilaktyka - sposoby zabezpieczeń

Perspektywa operatora (techniczne):

- Monitoring (ruchu, kont, wydatków itp.)
- Aktualizacja oprogramowania
- Określenie źródłowego adresu IP dla połączeń
- Zmiana standardowych portów
- Limitowanie (jednoczesnych połączeń, wydatków na okres np. 1 000 PLN/m-c)
- Systemy antyfraudowe (IDS/FDS), rozwiązania darmowe (Simple Asterisk Based Toll Fraud Prevention Script)

Profilaktyka - sposoby zabezpieczeń

Możliwości zawansowanych systemów antyfraudowych (IDS/FDS – fraud detector)

- polityka bezpieczeństwa (firewall, autoryzacja itp.)
- system decyzyjny
  - regułowy (np. max 100 poł. w ciągu 24h)
  - analizujący anomalie (odchylenia od profilu użytkownika)
- reakcja na zdarzenie
  - informowanie (monit)
  - odrzucanie połączeń
- ciągłe uczenie się systemu, gromadzenie danych

Profilaktyka - sposoby zabezpieczeń

Możliwości zawansowanych systemów antyfraudowych (IDS/FDS – fraud detector)

- wskazywanie połączeń
  - odbiegających od ustalonego profilu abonenta
  - z „podejrzanymi” numerami i krajami (zdefiniowanymi przez operatora)
- informowanie:
  - o połączeniach krótkich i długich w zadanym interwale czasowym (dialery)
  - o przekroczeniu ustalonej kwoty abonentowi za określony dzień, tydzień, miesiąc itp.
  - o globalnym przekroczeniu kwoty przeznaczonej operatorowi

Profilaktyka - sposoby zabezpieczeń

Perspektywa klienta:

- Stosowanie skomplikowanych haseł
- Aktualizacja oprogramowania terminali końcowych (IP-PABX, bramki, telefony, softphone)
- Zabezpieczanie terminali końcowych (hasła, porty, dostęp wyłącznie z intranetu)
- Ograniczenie kierunków na poł. wychodzące, możliwość wyjścia tylko w godzinach XX

Leczenie

Perspektywa operatora:

- Rozłożenie zobowiązania na raty

Perspektywa operatora i klienta:

- Wyciągnięcie wniosków
- Powrót do profilaktyki ☺

A jak jest realnie z fraudem w Polsce…?

4 marca 2010

Jak jest w Polsce?

Co się dzieje, kiedy w Polsce stwierdzi się fraud?

- Po stronie klienta:
  - tworzy się świadomość, że trzeba się jednak zabezpieczyć przed tym i zapobiegać na przyszłość
  - poprawia się konfiguracje systemów

  lub…
  - rozwiązuje się firmę i:
  - zmienia się operatora ☺

Jak jest w Polsce?

Co się dzieje, kiedy w Polsce stwierdzi się fraud?

- Po stronie operatora:
  - aktualizuje się prefiksy i cenniki
  - próbuje się tworzyć lub kupuje się system antyfraudowy
  - ustala się z klientem możliwość spłaty zadłużenia
  - psuje się współpraca z operatorami…

…bo też nie mieli fraud detectora ☺

Jak jest w Polsce?

Fraud traktowany jest jako kradzież bez konsekwencji ☹

- odpowiednie organy nie są zainteresowane ściganiem
- odpowiednie organy nie potrafią ścigać
- nie ma praktycznej możliwości ścigania podmiotu np. na Kubie
- nie ma praktycznej możliwości powiązania sprawcy fraud'u z właścicielem numeracji, na którą jest realizowany

Jak minimalizować wystąpienie fraudów?

- Okresowa analiza ryzyka
- Profilaktyka
- Detekcja, monitorowanie
- Szerzenie świadomości (szkolenia, konferencje)
- Dzielenie się wiedzą

Nie taki diabeł straszny…

Sam nie potrafisz?

Skorzystaj z doświadczenia innych

CROWLEY

DATERA

DATERA

Dziękujemy za uwagę

Marcin Gala – Datera

galam@datera.pl

Radosław Trojakowski – Crowley

r.trojakowski@crowley.pl