Současné telekomunikační hrozby a boj proti nim

Radek Kummer

Radek.kummer@o2.com

Telefónica

O2

Zájmy ohrožené telekomunikačními hrozbami

1. **Soukromí**
   - Ochrana tajemství prepravovaných zpráv (odposlechy, pozmenování obsahukomunikace)
   - Ochrana pred nežádoucím obtežováním (ochrana pred spamem)
   - Ochrana identity (pred nebezpecím falšování identity)
2. **Ekonomické zájmy**
   - Ochrana zákazníku užívajících telekomunikacních služeb
   - Ochrana poskytovatelu telekomunikacních služeb
   - Ochrana zájmu státu (výběr daní)
3. **Podpora činnosti bezpečnostních složek státu**
   - Dostupnost záznamů o telekomunikačním provozu
   - Věrohodnost záznamů o telekomunikačním provozu

Základní klasifikace hrozeb

1. **Chyby technologie**
2. **Hrozby kriminálního charakteru**
   - Ohrožující zákazníky telekomunikačních společností
   - Ohrožující telekomunikační společnosti

Chyby technologie

1. **Dlouhé nerozpojené hovory**

   Technické selhání na pobočkové ústředně může vést k tomu, že po ukončení hovoru jednou ze stran zůstane hovor nerozpojen.

Příklad :

Zákazník „A“. Dlouhý hovor do Belgie od 12.12.2006 do 21.12.2006. Konečná cena hovoru přes 59 000 Kč.

2. **Sekvence volání**

   Některé firmy realizují datové přenosy pomocí vytáčeného telefonního spojení, mnohdy automatizovaně. Selhání může vést ke generování sekvencí hovorů.

Příklad :

Zákazník „G“ listopad 2009. Detekována série krátkých hovorů. Zákazník je kontaktován a upozorněn na neobvyklý provoz. Škoda cca 300 000 Kč.

Faktory ovlivňující výskyt telekomunikačních hrozeb kriminální povahy

Telekomunikační hrozba

Motivace útočníků

- Přímý ekonomický zisk.
- Zisk informací.
- Přímé poškození cíle útoku.
- Získání prestiže.

Technologické předpoklady

Technologie poskytování a zabezpečení služby

Techniky a technologie útoku na službu

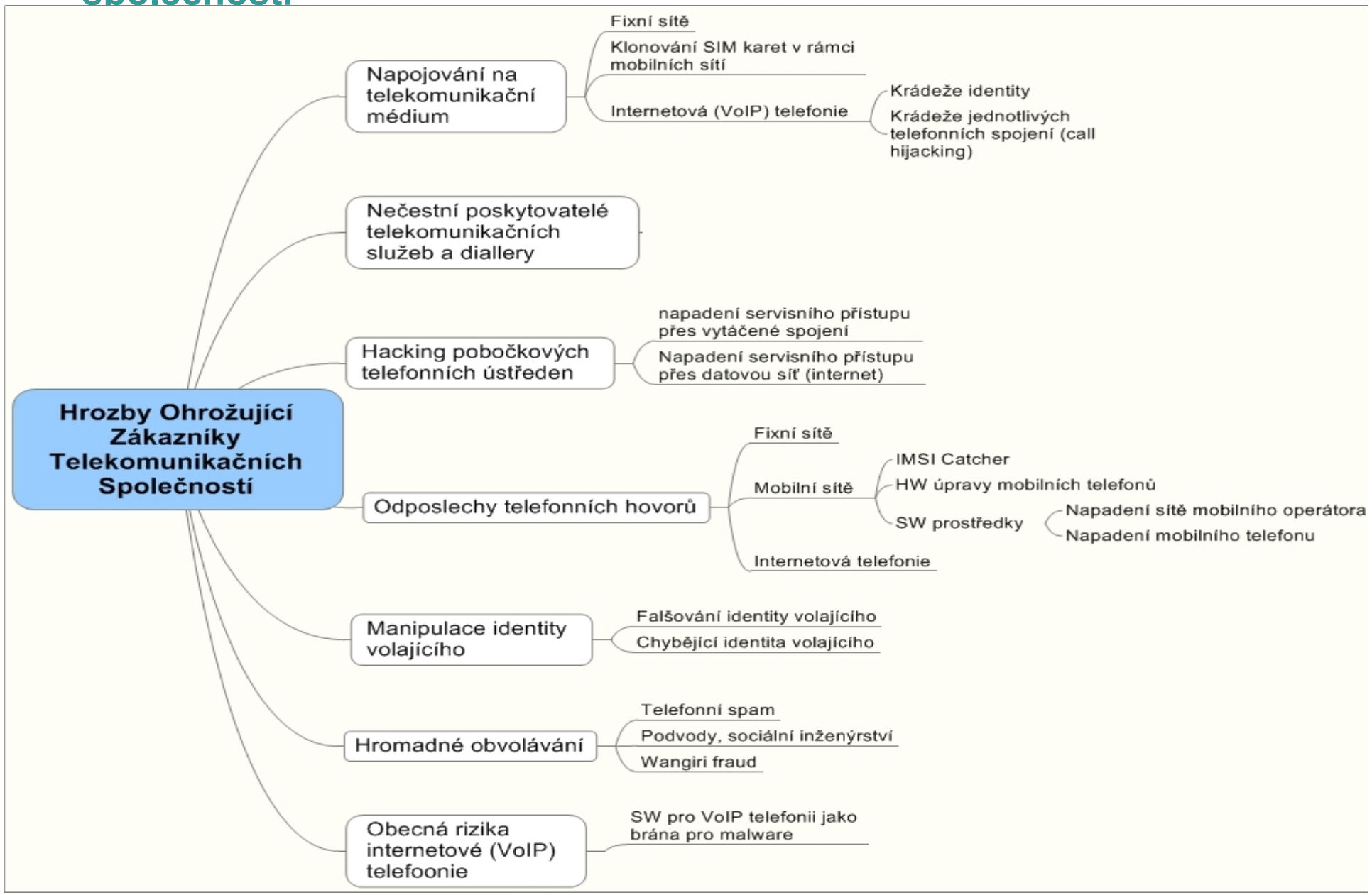
Možnosti postihu útočníka (rizika útočníků)

- Možnosti detekce útoku a zjištění identity útočníka.
- Legislativní možnosti postihu útočníka.

Sociologické pozadí

- Organizovaný zločin.
- Etnické a jiné komunity.

Hrozby kriminální povahy ohrožující zákazníky telekomunikačních společností



Hrozby kriminálního charakteru – interní nepřítel

1. **Neukáznění zaměstnanci firemních zákazníků**
   - Často problémy s firmami v podnájmu
   - Problém strážní služby
   - Nárůsty provozu mohou často být pod prahem zájmu oddělení pro detekci fraud
2. **Nečestní zaměstnanci telekomunikačních společností**
   - Hrozba jak pro telekomunikační společnosti, tak pro jejich zákazníky
   - Možnost napadení infrastruktury telekomunikační společnosti

Příklad napadení infrastruktury telekomunikační společnosti :

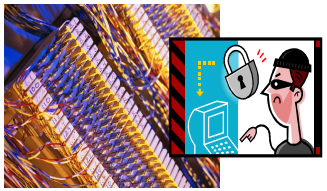
V roce 2006 byla napadena mobilní síť operátora Vodafone v Řecku. Napadení bylo realizováno pomocí instalace speciálního software na centrální zařízení telekomunikačního operátora. Obětí sledování se stalo okolo sta osob včetně ministerského předsedy.

Zdroj :

Spy software used in mobile eavesdropping; Kathimerini 3. února 2006 ; http://www.ekathimerini.com/4dcgi/_w_articles_politics_100014_03/02/2006_65958

Hrozby kriminálního charakteru – hacking pobočkových ústředen (PBX)

1. **Napadení servisního přístupu do pobočkové ústředny**
2. **Zneužití služby přesměrování**
3. **Cesty napadení**
   - Z telefonní sítě
   - Přes internet (Často VoIP pobočkové ústředny a zákazníci kombinující přístup přes klasickou fixní síť a VoIP síť)
4. **Čím lepší připojení zákazníka k telefonní síti (např. ISDN), tím rychlejší nárůst škody).**
5. **Ekonomické modely útočníků**
   - Přeprodej telekomunikačního provozu
   - Generování provozu na čísla s drahým tarifem
6. **Specifické směry** (např. 2009/2010 Lichtnštejnsko)

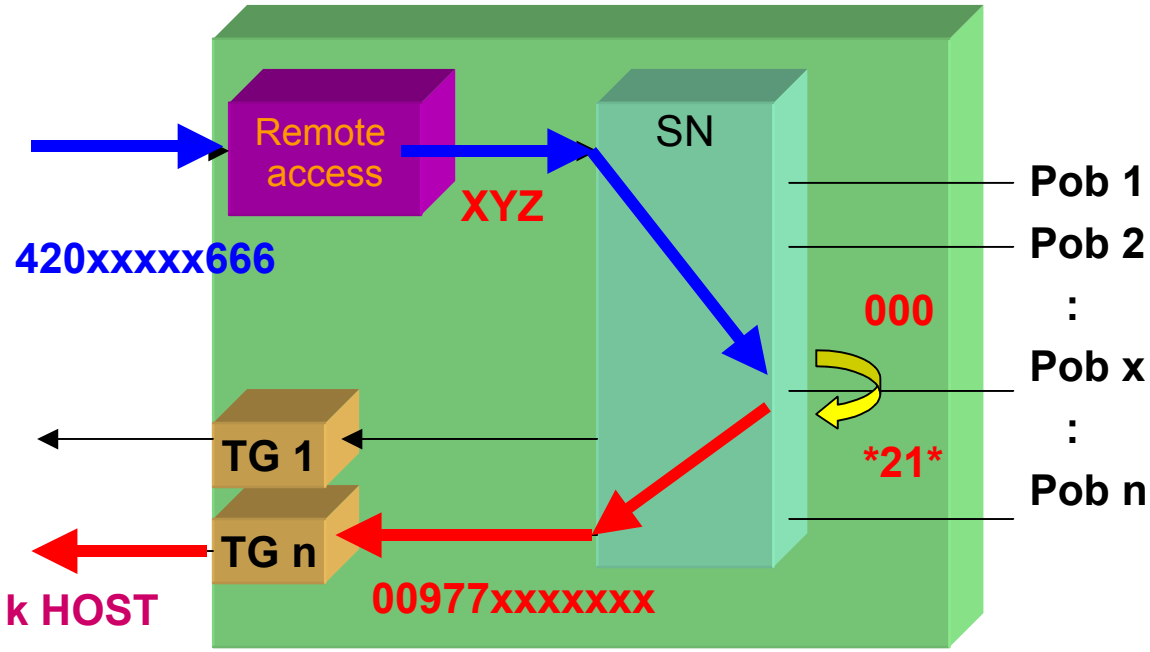


Obrana :

1. Řádné zaheslování servisního přístupu PBX
2. Blokace drahých směrů

Hrozby kriminálního charakteru – zneužití PBX s využitím služby přesměrování

PBX zákazníka



Postup zneužití PBX

- Volání na číslo RA „420xxxx6666“
- Volba čísla pob. „XYZ“
- Přístupový kód pobočky „000“
- Aktivace služby přesměrování např.„*21*“
- Volání libovolného čísla do celého světa „00977xxxxxxx“

Příklad napadení PBX v rámci klasické pevné telefonní sítě

1. Říjen 2009 z PBX xxxx zákazníka „F“ připojené přes ISDN přípojku provoláno během noci cca 212 000,- Kč bez DPH do zahraničí. Volaný směr je +42366 – Lichtnštejnsko.
2. Jedná se o 1565hovorů - 22tis. Minut
3. Zákazník deklaruje provoz jako nechtěný a snaží se o dohodu ohledně placení.

Problém s řešením podobné situace – lze zablokovat provoz zákazníka aniž by byl dopředu informován ?

Hrozby kriminálního charakteru – spam, sociální inženýrství

1. **Wangiri fraud**
   - Masivní prozvánění zákazníků mobilních sítí často spojené s manipulací identity volajícího. Zákazníci, kteří se nachytají, pak volají do drahých směrů.
2. **Spam**
   - Automatizovaný sběr dat pro marketingové společnosti ???
   - Různé marketingové akce i ze zahraničí, ne vždy poctivé.
   - Často chybí identifikace volajícího – obtíže s blokováním takového provozu.

Příklad 2005 :

Masivní obvolávání ze zahraničí s podvodným sdělením o výhře. „Výherce“ si má zavolat kvůli detailům na drahé audiotextové číslo. Cena za takový hovor je pak až 700 Kč.

Hrozby kriminálního charakteru – diallery

1. **Malware** (často skripty ActiveX) napadající PC a mobilní telefony
2. **Přesměrování vytáčeného připojení na internet**
   - do zahraničí
   - na datový audiotext
3. **Generování sekvencí volání bez vědomí uživatele zařízení**
4. **Specifické internetové stránky**
   - S pornografii, s nelegálním kopírováním hudby, stahováním her, ale mohou se vyskytovat i na stránkách jiných hojně navštěvovaných služeb
5. **Škody až desítky tisíc Kč**
6. **Historický vývoj** – Dříve se týkaly především zákazníků připojených k internetu pomocí modemů z běžných telefonních linek nebo digitálních linek (ISDN) v současnosti představují nebezpečí především pro uživatele mobilních sítí.

Hrozby kriminálního charakteru – odposlechy obecně

1. **Fixní sítě**
   - Pomocí fyzického napojování na vedení
2. **Mobilní sítě první generace a bezdrátové telefony**
   - Komerčně nabízené scanery provozu.
   - HW úpravy mobilních telefonů
3. **GSM mobilní sítě :**
   - šifrovaní komunikace mezi telefonem a základnovou stanicí, teoreticky bezpečné.
   - HW úpravy mobilních telefonů
   - IMSI Catcher
   - Napadení inteligentních koncových zařízení SW prostředky
4. **UMTS mobilní sítě**
   - možnost lepšího zabezpečení podmíněná nasazením USIM karet namísto klasických SIM karet.
5. **VoIP telefonie**
   - Volně dostupné SW na Internetu (VoIPong, UCSniff, ..), útoky typu man in the middle

Odposlechy v rámci GSM a UMTS mobilních sítích – IMSI Catcher

1. **Umělá základnová mobilní stanice**, původně určeny pro lokalizaci mobilních telefonů podle tzv IMSI. Možnost odposlechu hovorů byla dodána teprve dodatečně.
2. **Využití slabiny GSM sítě** - koncové zařízení se identifikuje síti, ale síť se neidentifikuje
3. **Může být relevantní I pro UMTS sítě** – V rámci UMTS sítě se musí identifikovat i sama UMTS síť nicméně ta musí zůstat otevřená I pro GSM zařízení. Navíc pro využití všech předností UMTS sítě je třeba používat namísto SIM tzv. USIM.
4. **Značně nákladné plus silné vedlejší účinky** (zdroj : IMSI Catcher, Daehyun Strobel, 13.Juli 2007, Seminararbeit, Ruhr-Universit¨at Bochum)
   - Sledovaný mobilní telefon musí být přihlášen do určité mobilní sítě
   - Mobilní telefon si vybírá ze základních stanic v jeho dosahu podle síly signálu. Může být problém přehlušit signál nejbližší regulární základnové stanice.
   - IMSI catcher, může zachytit naráz více IMSI ve svém dosahu, problémem může být identifikace správného IMSI
   - V rámci dosahu IMSI catcheru jsou všechny mobilní telefony s výjímkou sledovaného telefonu odříznuty od telefonní sítě.
   - Ani sledovaný telefon nemůže přijímat příchozí hovory
   - Je zamezen přenos identifikace volajícího

Odposlechy v rámci GSM a UMTS mobilních sítích – SW prostředky

1. **Cesty napadení** (bluetooth, MMS, přes Internet)
2. **Existence komerčně nabízených produktů**
3. **Patrně první aplikace americká FBI** (FBI taps cell phone mic as eavesdropping tool; CNET 1. prosince 2006; http://www.news.com/2100-1029_3-6140191.html)
4. **Další příklad - Sebastian Schreiber na IDC Security RoadShow, Praha2007 :**
   - Prezentováno napadení trojským koněm přes bluetooth
   - Skryté odeslání příchozích SMS na definované telefonní číslo
   - Skrytý příjem hovoru bez vyzvánění a jiného upozornění z definovaného telefonního čísla – odposlech okolí
5. **Teoretické otázky :**
   - Možnost skrytých konferenčních hovorů pro odchozí hovory ?
   - Dnešní pokročilé modely umožňují nahrávání hovorů. Lze takto uložený hovor odeslat mailem ?

Hrozby kriminálního charakteru – manipulace identity volajícího

1. **Potlačení identity volajícího**
   - Nemožnost blokace obtěžujícího provozu.
   - Nemožnost identifikace obtěžujících zlomyslných volání
   - Často, ale ne vždy spojeno s různými telekomunikačními podvody (Wangiri fraud, podvody obecně)

2. **Manipulace identity volajícího**
   - příklad : www.spoofcard.com

„Best practices“ pro uživatele telekomunikačních služeb (1)

1. **Zabezpečení administrátorských přístupů do pobočkových ústředen.** Ve hře je ochrana před napadením hackery a následným zneužitím před voláním na vrub oprávněného vlastníka ústředny.
2. **Dohled nad provozem pobočkových ústředen.** (vyšší typy, které to umožňují) Ochrana před nerozpojenými dlouhými hovory.
3. **Blokace volání do drahých směrů na úrovni pobočkové ústředny.**. U firem používajících sofistikovanější pobočkové ústředny pro klapky, jejichž uživatelé to nepotřebují ke své práci.
4. **Blokace volání do drahých směrů na úrovni telekomunikačního operátora.** Pro organizace nebo řadové zákazníky bez sofistikovanějších pobočkových ústředen, kteří určitě do daných destinací nebudou potřebovat volat.
5. **Aktivace služby hlídaní výše hovorného během účtovacího období.** Někteří telekomunikační operátoři nabízejí služby na hlídání výše hovorného. Zákazníci jsou upozorněni na překročení limitů. Různé varianty ať už zdarma nebo placené.
6. **Ochrana koncových zařízení (osobní počítače a „chytré“ mobilní telefony) před šířením různých zhoubných kódů.** Ochrana před generováním provozu do drahých destinací, přepojováním vytáčeného připojení na internet do drahých destinací a před odposlechem.

„Best practices“ pro uživatele telekomunikačních služeb (2)

7. **Zabezpečení přístupu přes bluetooth u chytrých mobilních telefonů.** Někteří uživatelé nechávají své přístupy přes bluetooth zbytečně viditelné pro okolí nebo si dokonce nechávají defaultní přístupové kódy od výrobce. Vystavují se tak riziku šíření zhoubného kódu (diallery, trojské koně pro odposlech).
8. **Výpisy příchozích a ochozích hovorů mohou ledacos prozradit.** U chytrých mobilních telefonů může výpis příchozích hovorů odhalit odposlech. U ochozích hovorů se jedná o kontrolu vlastních nákladů. V případě vlastní pobočkové ústředny není nutno žádat telekomunikačního operátora.
9. **V případě hlasového spamu (obtěžováním reklamou po telefonu) si stěžovat u svého telekomunikačního operátora.** Je pravděpodobné, že pokud se mu sejde více stížností a budou příznivé technické podmínky, tak přistoupí k blokaci zdroje spamu.

Hrozby kriminální povahy ohrožující telekomunikační společnosti

Boj mezi operátory - nelegální propojování telekomunikačních sítí (bypassy)

1. **Propojení telekomunikační sítě dvou operátorů mimo smluvní koncový bod**
2. **Nečestný operátor si u své konkurence zřídí připojení jako řadový zákazník a přivede provoz pomocí datové sítě**
3. **Vyplatí se u směrování provozu ze zahraničí**
4. **Důsledky :**
   - Postižený operátor přichází o propojovací poplatky.
   - Stát je krácen na výběru daní.

Detekce :

- Sledování čísel ve vlastní síti s velkým odchozím provozem na mnoho jedinečných telefonních čísel (může se ale jednat I o regulérní korporátní zákazníky)
- Verifikace testovacími hovory ze zahraničí na známá čísla ve své síti.

Protiopatření : stížnost u správního orgánu (ČTÚ).

Boj mezi operátory - zpětná volání (callbacky)

1. **Jde o realizaci telefonního spojení do zahraničí pomocí zahraničního telekomunikačního operátora.**
2. **Zákazník volá zahraničního operátora, který ukončí hovor ve fázi vyzvánění.**
3. **Zahraniční operátor pak následně volá zpětně zákazníka a realizuje požadovaný hovor.**
4. **Volaná a volající čísla zahraničního operátora realizujícího callback se zpravidla liší.**
5. **V mnoha státech je tento model považovaný za legální, to však neplatí pro ČR.**

Detekce :

- Analýza nabídek v tisku a na internetu.
- Vyhodnocení časové souslednosti volání u zahraničních čísel s velkým počtem neuskutečněných příchozích hovorů a u zahraničních čísel s velkým počtem hovorů na velký počet jedinečných čísel. Jde o práci s výstupy ze signalizace SS7

Protiopatření :

Prokázání callbacku u regulačního orgánu a následná blokace příslušných čísel.

Boj mezi operátory – nelegální telekomunikační operátoři

1. Telekomunikační operátoři poskytující služby bez řádné licence od ČTÚ
2. Neplatí ostatním operátorům propojovací poplatky
3. Mají nižší náklady z důvodu neplnění zákonných povinností jako například podpora orgánů činných v trestním řízení
4. Služby zpravidla poskytovány na základě předplacených karet mimo vyhrazenou část číslovacího plánu.

Boj mezi operátory - rizika designu telekomunikačních služeb

Demonstrace na příkladu z praxe

Výchozí situace :

1. Telekomunikační operátoři vybírají propojovací poplatky za směřování provozu do své sítě
2. Operátor “A” poskytne o víkendu hovorné za paušál
3. Operátor “B” se rozhodne se svými zákazníky podělit o propojovací poplatky

Důsledek :

výskyt podnikavého jedince s připojeními u operátora “A” a “B” a automatizovaně generujícího o víkendu provoz ze sítě operátora “A” do sítě operátora “B”.

Hrozby ohrožující zákazníky jako hrozba pro telekomunikační společnosti

1. Pokud zákazník nemá na zaplacení účtu a přitom telekomunikační společnost má za jeho provoz platit třetí straně, je to problém i pro tuto společnost.
2. Nespokojený zákazník může mít tendenci přejít ke konkurenci.
3. Riziko špatné publicity.
4. Ne vždy dá regulační orgán nebo soud v případě sporu za pravdu telekomunikační společnosti.

„Best practices“ pro telekomunikační společnosti

1. **Vyhodnocování provozu zákazníků alespoň jednou denně**
2. **Věnovat péči sběru dat**
   - Jsou sbírány všechny účtované transakce a ve správné formě (společný zájem s revenue assurance)
   - Jsou sbírány i průběžné transakce (průběžné věty u vícedenních hovorů).
3. **Blokace drahých směrů**
   - Individuálně pro jednotlivé zákazníky na vyžádání
   - V závažných případech u směrů s malým objemem provozu kompletní blokace směru nebo povolení provozu pouze přes spojovatelku.
4. **Ochrana vlastní infrastruktury**
5. **Nesnažit se prodávat služby za každou cenu** (raději žádný než neplatící zákazník generující náklady například na propojovací poplatky).
6. **Dbát na řádnou identifikaci zákazníků a řádně uzavřené smlouvy**
7. **Pamatovat na bezpečnost už během designu nových produktů**
8. **Mít na paměti, že škoda zákazníka se může snadno zvrtnout ve škodu vlastní !**

DĚKUJI ZA POZORNOST