TelPro spol. s r.o.

FRADES

Frades

Fraud Detection System
Informační systém pro detekci podvodného chování v prostředí provozu telekomunikačních služeb

Podvody v telekomunikacích

Poskytování telekomunikačních služeb je spojeno s řadou rizik, která mohou představovat nemalou finanční ztrátu pro operátora a/nebo jeho koncové zákazníky. Statisticky patří mezi hlavní oblasti zneužívání telekomunikačních služeb:

- používání telekomunikačních služeb ze strany zákazníka s úmyslem za tyto služby nezaplatit (subscription fraud)
- zneužití koncového zařízení nebo ústředny útočníkem (hacking)
- zneužívání telekomunikačních služeb ze strany zaměstnanců (insider fraud).

Co nabízí FRADES?

Informační systém Frades nabízí technické řešení, které umožňuje vybrané případy zneužití telekomunikačních služeb detekovat, vyhodnotit a eskalovat, čímž významným způsobem minimalizuje výši případně vzniklé finanční ztráty.

Technické řešení

Systém Frades nabízí následující klíčové funkce:

- průběžné stahování dat z technologického zařízení,
- automatickou analýzu a vyhodnocení dat,
- vytvoření hlášení o „fraud incidentu",
- posouzení incidentu „fraud analytikem",
- eskalaci zjištěného podvodného chování.

Stahování dat - data jsou stahována buď z billingového systému, nebo je jejich zdrojem přímo technologické zařízení (ústředna, soft-switch). Zde se dá vytvořit on-line, nebo souborové propojení.

Automatická analýza - bezprostředně po stažení dat do provozní databáze systému je provedena jejich analýza. Každý záznam o spojení (CDR) je zpracován kaskádou tzv. monitorovacích pravidel. Jednotlivá pravidla vyhodnocují specifické vlastnosti hovorů.

K dispozici je několik desítek typů pravidel sledujících tyto typy veličin:

- vlastnosti individuálních hovorů (cena, délka, zdroj volání, cíl volání apod.)
- vlastnosti množiny hovorů (počet hovorů za jednotku času, součet cen, součet délek apod.)
- analýza trendu (typicky detekování změn provozu, změn chování účastníka apod.)

Hovory jsou vždy zkoumány v kontextu konkrétní monitorované entity. Typicky se jedná o hovory daného zákazníka, účastnické stanice, případně celého svazku.

Vytvoření „fraud incidentu" – v případě, že v rámci procesu automatické analýzy dojde ke zjištění mimořádné situace, je vytvořeno hlášení o incidentu. Toto hlášení obsahuje informace o důvodu vyvolání mimořádné situace včetně detailních informací, které slouží fraud analytikovi k posouzení situace.

Posouzení „fraud analytikem" - posouzení situace (incidentu) fraud analytikem není povinné. U pravidel, která administrátor

systému nastaví jako mimořádně závažná, je možné definovat proces automatické eskalace, čímž je zkrácena doba nezbytná k řešení problému.

Eskalační procedura - eskalační procedura představuje následující soubor procesních kroků:

- vytvoření podrobné sestavy s informacemi o incidentu (log soubor, tisk),
- notifikaci zainteresovaných osob (e-mail, SMS) o incidentu,
- automatickou změnu na technologickém zařízení (př. pozastavení služby).

Technické požadavky na provoz.

Operační systém:

- Aplikační servery: Windows Server 2003, 2008
- Klientské stanice: Windows XP, Vista, 7

Databáze:

- Oracle 10g (verze Standard a vyšší)

Blokové schéma systému

*) Web portál není součástí dodávky