

# Sedem ciest v boji s podvodmi v poisťovníctve

Podvodné poisťné udalosti sú bolestivým trňom v oku všetkých poisťovní. Poisťovacie spoločnosti používajú rozličné taktiky v boji proti poisťným podvodom, aby znížili svoje nemalé finančné straty.

Fingované či nadhodnotené poisťné udalosti spôsobujú poisťovním škody ťažko vyčísliteľných rozmerov. Aj keď presné výšky škôd spôsobených poisťnými podvodmi sú neznáme, odhady v USA hovoria o 20 – 60 miliardách dolárov. Niet pochýb, že tento typ kriminality je silná výzva pre vývoj informačných anti-fraud technológií. Fraud existuje len dovtedy, kým má na svoju existenciu priestor. Jeho existenčný priestor možno výrazne eliminovať modernými detekčnými technológiami.

Keby bolo kriminálne správanie ľudí statické, resp. ľahko definovateľné, odhaľovanie a eliminácia poisťných podvodov by predstavovali jednoduchý problém. Na základe doteraz nadobudnutých skúseností sa ukazuje, že tvorivosť podvodníkov nemožno v žiadnom prípade podceňovať. Ich aktivita si vyžaduje neustálu pozornosť zo strany poisťovní. Trvalý vývoj v tomto smere doposiaľ priniesol množstvo zaujímavých metód na odhaľovanie poisťných podvodov.

## Metóda č. 1: Analýza stresu v hlase

Každý podvod sa začína lžou. Kriminálnik musí byť vlastne profesionálnym klamárom, aby jeho príbeh znel dôveryhodne. Aj keď slová a vety znejú, akoby opisovali skutočnú udalosť, ľudská psychika zanechá na pozadí nášho hlasu vždy informáciu o tom, či klameme.

Nie je stres ako stres. Stres z klamstva súvisí s neúprimnosťou prejavu podvodníka. Technika analýzy hlasu a jeho porovnanie s referenčnými vzorkami umožňuje odhaliť práve také odchýlky v hlase, ktoré sú spôsobené vedomým klamaním.

Analýza stresu v hlase vyhodnocuje elektronický záznam verbálneho interview s poisťníkom. Z jeho hlasu sa extrahujú tzv. stresové signály, ktorých úroveň sa porovnáva s referenčnými obrazcami. Porovnanie korelačných hodnôt indikuje mieru pravdepodobnosti, že prejav hovoriaceho bol falošný. V prípade prekročenia prahovej úrovne sa nastavuje jeden z indikátorov signalizujúcich, že ide o poisťný podvod.

Analýza stresu v hlase sa opiera o faktor ľudskej psychiky, ktorý objektívne nezávisí od veku, pohlavia, reči, prízvuku, vzdelania ani rasy hovoriaceho. Stres z vedomého klamstva skrátka pôsobí na všetkých ľudí kvalitatívne rovnako. Spomínaný test hlasu kvantitatívne vyhodnocuje mieru stresu závislého od lživosti, zašifrovaný v hlase hovoriaceho.

Napriek dokázanému kvalitatívnemu vplyvu nemožno predpokladať rovnaký účinok stresu na všetkých ľudí. Jeho pôsobenie vo veľkej miere závisí od osobnostných daností, ako aj od „trénovanosti“ jedinca. Rôzny stupeň kvantitatív-

neho vplyvu má za následok, že táto metóda je teoreticky veľmi komplexná a technologicky náročná, toho času neustále vo vývoji. Do budúcnosti má analýza hlasu veľký potenciál objektívne vyhodnocovať lož z výpovede hovoriaceho.

Poisťovnía, ktorá verejne používa sofistikované technológie počas likvidácie poisťných udalostí, si získa aj psychologický rešpekt pred podvodníkmi – štatisticky sa zníži počet hlásení poisťných udalostí. Tento fakt však môže mať aj negatívny dosah na portfólio zákazníkov. Používanie záznamových zariadení pri rozhovoroch môže mať negatívny vplyv na vernosť zákazníkov.

## Metóda č. 2: Značkovanie

Na opačnom konci technologického spektra odhaľovania poisťných podvodov stojí dávno známa metóda „červených značiek“. Pri tejto metóde likvidátori cielene vyhľadávajú špecifické reťazce aktivít, osôb, telefónnych čísel a pod. v sieti poisťných udalostí. Využívajúc svoju skúsenosť, poisťný likvidátor označí podozrivé poisťné udalosti červenými značkami. Vytypované poisťné udalosti sa následne detailne vyšetrí. Detailné skúmanie s vysokou pravdepodobnosťou odhalí, či ide, resp. nejde o poisťný podvod.

Značkovací program poisťovne je jednoduchý a pomerne objektívny. Táto tradičná manuálna metóda sa zakladá na používaní súboru pravidiel a atribútov, pomocou ktorých pracovník prvého kontaktu (likvidátor) aj bez dlhoročných skúseností s poisťnými podvodmi zatriedi aktuálne poisťné udalosti do škály pre podozrenie na fraud.

Ako všetky klasické metódy aj metóda značkovania má svoje nedostatky. Po prvé gro odhaľovania podvodov leží na pleciah často preťažaných rutinérov, značkujúcich poisťné udalosti. Detailní vyšetrovatelia následne strávia väčšinu svojho pracovného času analýzou falošných poplachov. Ďalšia nevýhoda značkovej metódy je, že sa výlučne opiera o historickú skúsenosť. Sama metóda bez tvorivého prístupu značkárov a vyšetrovateľov nemá šancu odhaľovať nové, doposiaľ nezaužívané metódy poisťných podvodov. Podvodníci však vo svojej vynaliezavosti často predstihujú vyšetrovateľov poisťovní.

## Metóda č. 3: Prediktívne modelovanie

V záujme odhaľovať poisťné podvody sa mnohé poisťovne v posledných rokoch orientujú na prediktívne modelovanie. Softvérové nástroje typu data mining si vytvárajú vlastnú štatistiku z databázy existujúcich poisťných udalostí, ktorá slúži ako báza znalostí na detekciu podvodov. Štatistická báza znalostí využíva prakticky všetky známe relevantné informácie z minulosti, majúce dokázaný vplyv na to, či poisťná udalosť bola, resp. nebola podvodom. Úlohou používateľa je zadať do takéhoto programu správne dáta. Program potom automaticky stanoví mieru

pravdepodobnosti, či daná poisťná udalosť je podozrivá na podvod.

Prediktívne metódy v súčasnosti nahrádzajú manuálne značkovanie. Vďaka svojej výkonnosti sú schopné automaticky spracovať a rýchlo vyhodnotiť oveľa väčšie množstvo vstupných informácií, ako sa manuálne robilo v minulosti.

Dôležitá však aj tu ostáva kvalita vstupných dát. Sem patria všetky relevantné atribúty poisťnej udalosti štatisticky súvisiace s podvodmi. Najpodstatnejšia je pravdivosť informácie, ktoré poisťné udalosti z minulosti boli skutočnými podvodmi. V neposlednom rade treba vytvoriť taký výber atribútov o poisťnej udalosti, ktorých hodnoty majú relevantný vzťah k faktu, či ide o podvod alebo o normálnu škodu.

Prediktívny model treba neustále aktualizovať referenčnými poisťnými udalosťami so správne vyhodnoteným atribútom typu fraud. Iba tak dokáže model aproximovať najnovšie metódy podvodov.

## Metóda č. 4: Vyhľadávanie v databáze

Vyhľadávanie v centrálnej databáze patrí medzi moderné globálne nástroje podporujúce vyšetrovanie kriminality. Centrálné databázy slúžia na zber a správu dát poskytovaných poisťovníami v národnej, resp. aj v nadnárodnej úrovni. Používatelia a predplatitelia takýchto centrálnych databáz sú poisťovne. Poisťovne jednak poskytujú do databázy svoje prevádzkové údaje, na druhej strane si v nej vyhľadávajú informácie zdieľané všetkými účastníkmi. Vo všeobecnosti sú predplatiteľovi k dispozícii všetky dáta v databáze bez ohľadu na ich pôvod. Efektívne využívanie informácií poskytovaných centrálnymi databázami predpokladá špecifické znalosti používateľa – jednak znalosti v oblasti poisťovníctva, jednak ovládanie technológie konkrétnej databázy.

Správu databáz väčšinou realizujú súkromné spoločnosti, ale podporujú ju aj štátne autority v záujme všeobecnej prevencie pred kriminalitou.

Doteraz opísané metódy sa snažili poskytnúť poisťovateľovi dôležitú informáciu ešte pred uzavretím konkrétnej poisťnej udalosti. Prvoradým cieľom je tu vyhnúť sa zbytočnému finančnému krytiu v prípade, že ide o poisťný podvod.

Nasledujúce metódy budú retrospektívne. Analyzujú veľký súbor už uzavretých poisťných udalostí. Cieľom retrospektívnych metód je odhaliť väzby navzájom spájajúce podvodníkov. Sem patria aj väzby interných pracovníkov so zákazníkmi (externý a interný fraud). Výstupom retrospektívnych metód a modelov sú štruktúry a reťazce spolupracujúcich osôb, metódy ich práce a v neposlednom rade identifikácia podvodov zrealizovaných v minulosti. Výsledky retrospektívnej analýzy možno použiť na kalibráciu predikčných modelov.

## Metóda č. 5: Hlásenie výnimiek (Exception Reporting)

Metóda hlásenia výnimiek pracuje so systémom absolútnych a relatívnych stredných hodnôt a k nim príslušných stredných odchýlok. Všetky významné odchýlky od povolených intervalov,

resp. ich kombinácie sú následne hlásené kompetentným pracovníkom formou automatických reportov.

Táto metóda sa okrem iného využíva pri monitorovaní (meraní) aktivít pracovníkov poisťovne. Poskytuje spätnú väzbu pre manažment a hrá významnú úlohu pri identifikácii aktivity typu interný fraud.

### Metóda č. 6: OLAP reporting

Kombinácia priameho dopytu do databázy (ad hoc query) s technológiou OLAP (online analytical processing) poskytuje možnosť rýchlo získať agregované prevádzkové údaje podľa okamžitej potreby. Takzvaná kocka OLAP umožňuje používateľovi rýchlu selekciu typických hodnôt prislúchajúcich určitému segmentu zákazníkov a ich následné porovnanie s hodnotou vyšetrovanej poistnej udalosti.

### Metóda č. 7: Link analýza

Kľúčový nástroj na detekciu poistných podvodov je tzv. link analýza. Táto metóda umožňuje identifikovať organizované štruktúry viacerých osôb, spolupracujúcich na poistných podvodoch. Zatiaľ čo doterajšie retrospektívne metódy štatistiky odhaľovali iba jednotlivé faktory vymykajúce sa z bežnej oblasti hodnôt, link analýza štatisticky identifikuje logické kombinácie faktorov, tzv. reťazce. Oproti bežnej štatistike link analýza umožňuje výpočet logicky podmienenej štatistiky z viacerých atribútov. Ich vstup do štatistiky je podmienený splnením určitej vopred definovanej

logickej podmienky (AND, OR).

Link analýza je teda štatistika kombinácií atribútov, ktorá umožňuje identifikovať organizované aktivity, vymykajúce sa z bežného správania.

Výstupom link analýzy je link graf. Atribúty, ktorých hodnoty sa nadpriemerne často súčasne vyskytujú, sú navzájom pospájané čiarami. Hrúbka čiary býva úmerná početnosti výskytu danej kombinácie.

Práca s link analýzou si vyžaduje vysoký stupeň znalostí o štatistickej povahe vstupnej vzorky dát. Vopred treba poznať atribúty, ktorých hodnoty sa často vyskytujú v kombináciách, ako aj atribúty, pri ktorých sú opakované kombinácie hodnôt len výnimočné. Analytik potom zvolí reťazce atribútov, o ktorých štatistiku sa zaujíma. Ďalej nastaví prahovú citlivosť modelu a spúšťa proces.

Sofistikované modely link analýzy dokážu samy vyhľadávať reťazce atribútov spomedzi celej vzorky. Zadá sa len dĺžka reťazca (od do) a prahová početnosť výskytu vo vzorke. Výstupom sú grafy všetkých reťazcov, ktorých štatistika spĺňa zadanú podmienku.

Poistovne môžu spomenuté metódy detekcie podvodov používať individuálne alebo vo vzájomnej kombinácii, keďže niektoré metódy sa navzájom dopĺňajú. Vďaka účinnej detekcii podvodov sa poisťovňa dokáže včas a správne rozhodnúť, či vyplatiť, resp. zamietnuť krytie poistnej udalosti. Poisťovňa sa tak vyhne zbytočným finančným stratám a na druhej strane si

získa dôveru poctivých klientov.

■ DAVID WEST, Insurance Practice Research Director, TowerGroup

Článok bol pôvodne publikovaný v časopise *National Underwriter Property & Casualty*. (Z anglického originálu preložil Milan Hronský)

## Nová verzia AVG 8.0 ponúka všetkým používateľom významné rozšírenie ochrany údajov

Spoločnosť AVG Technologies prednedávnom uvoľnila na svetový trh novú verziu svojho bezpečnostného softvéru AVG 8.0. Firma pri jeho vývoji reagovala nielen na potrebu komplexnej ochrany pred známymi či aktuálnymi hrozbami, ale aj na predpokladaný vývoj v oblasti bezpečnostných rizík. AVG 8.0 teda obsahuje nielen antivírus, antispyware, antisipam, antirrootkit či firewall, ale aj unikátnu technológiu ochrany vyhľadávania a webovej prevádzky v reálnom čase **LinkScanner**, zaradenú do produktu po minuloročnej akvizícii americkej firmy Exploit Prevention Labs. Používatelia tým získajú jedno z najlepších a najkomplexnejších riešení v oblasti počítačovej bezpečnosti, ktoré je na trhu k dispozícii.

Pred niekoľkými rokmi patrili medzi najväčšie bezpečnostné hrozby klasické vírusy, v súčasnosti však výrazne narastá intenzita profesionálnych webových útokov zo strany dobre organizovaného počítačového podsvetia. Ich cieľom je nelegálny zisk peňazí či sponožateľných údajov. Technológia LinkScanner však dokáže útok spoľahlivo zastaviť. Ochrana pri bežnom používaní internetu

zabezpečuje v AVG 8.0 **webový štít**, ktorý chráni pred nechceným stiahnutím infikovaných súborov pri prehliadaní internetových stránok aj pri on-line komunikácii pomocou aplikácií ICQ alebo MSN. Technológia dokáže eliminovať aj hrozby zo strany tzv. **exploitov**, ktoré zneužívajú na prienik do počítača



slabé miesta v zabezpečení webových prehliadačov. Riešenie rovnako **v reálnom čase** varuje používateľov internetu pred nebezpečenstvom bez toho, aby museli kliknúť na príslušný odkaz. Vizualne tak dostanú informáciu, či príslušný link vedie alebo nevedie na infikované stránky, a nemusia na ne vôbec vstúpiť.

AVG 8.0 má moderný a prehľadný vzhľad, jednotné používateľské rozhranie, nenáročnú inštaláciu a zjednodušené ovládanie pomocou intuitívnej navigácie. Držitelia komerčných licencií majú navyše k dispozícii nepretržitú profesionálnu technickú podporu, ktorá im poradí v prípade akýchkoľvek problémov spojených s používaním programu. Oľubu produktov so značkou AVG dokazuje skutočnosť, že doposiaľ chráni viac než 70 miliónov počítačov po celom svete. AVG 8.0 pracuje na operačných systémoch MS Windows 2000 a vyšších, pričom podpora doterajšej verzie AVG 7.5 potrvá do konca roku 2008.

