AFS – Stopka pro podvodníky?

Ing. Marek Sušický, Senior Advisor, Fraud management, Profinit, s.r.o.

Anti fraud systémy (AFS) se snaží předcházet vzniku škody tím, že průběžně odhalují nepoctivost a závadné chování. Jejich nasazení pomáhá chránit dobré jméno organizace a ušetřit jí tak nemalé peníze, a to jen samotnou prevencí.

Celosvětové průzkumy ukazují, že množství podvodů se v čase nijak nesnižuje. Nezáleží na pohlaví, rase, náboženském vyznání, vzdělání, ani významu pracovní pozice. Ba právě naopak, čím je pachatel v organizaci výše, tím horší mohou být následky jeho nekorektního chování.

Kdo potřebuje AFS systém?

Antifraud systémy se hodí převážně pro oddělení spojené s bezpečností, vyšetřováním či auditem. Ve státní správě připadá v úvahu jejich použití všude tam, kde by mělo docházet ke kontrole přerozdělování financí, ale i rutinnímu běhu. Vzpomeňme několik případů, kdy byla na základě falešných faktur vylákána nemalá částka. Podobné případy se dějí i s tzv. mrtvými dušemi – nedávno došlo například k odhalení jednoho většího případu na Liberecku. Některé oblasti trhu, jako například stavebnictví nebo obchod pohonnými hmotami jsou tak problematické, že stát přistupuje k alternativním metodám výběru DPH (tzv. reverse charge).

Velkým tématem využití může být kontrola výplat dávek a důchodů, jelikož sociální výdaje našeho státu tvoří podstatnou část rozpočtu. O atraktivitě této oblasti svědčí i velký zájem společností IBM a SAS o implementaci AFS systémů.

Použití AFS v praxi

Každý, kdo má dnes platební kartu, je chráněn antifraudovým systémem. Bez nich by karetní asociace a banky nemohly existovat. Pokud si uděláte výlet do exotičtější destinace, zkuste si někdy večer vybrat z bankomatu hotovost. U některých bank vám kvůli ověření zavolají do pár minut.

Platební karty ale nejsou jediným finančním produktem, chránit lze i mobilní a internetové bankovnictví. V případě pojišťoven je možné sledovat sjednávání smluv či likvidaci pojistných událostí a u zdravotních pojišťoven zase oprávněné čerpání péče.

Prozrazovat principy, postupy a technologie používané při detekci podvodů nelze, jelikož je to to nejcennější, co systémy obsahují. Pokud by se k těmto informacím útočníci dostali, mohli by se snadno přizpůsobit a zůstat v bezpečné šedé zóně.

Proč nasazovat AFS?

Laici možná nebudou souhlasit, ale velkým přínosem AFS systémů je již jen jejich instalace. Vědomí zaměstnanců a zákazníků, že nad nimi bdí „velký bratr“, je neocenitelné. Pověst systému se navíc výrazně zlepšuje, když občas někdo zavolá a zeptá se, proč zaměstnanec dělal to, či ono. Zaměstnanec si pak dvakrát rozmyslí, než se podívá na výpis volání známé osobnosti.

Druhým přínosem jsou samozřejmě finanční úspory, více prošetřených a objasněných případů a více času na jejich řešení. Pokud vyšetřovatelé nemusí pracně data hledat, ale mají je všechny na jednom místě, mohou se více věnovat jádru problému.

Třetím důvodem pro nasazení AFS může být splnění regulatorních či zákonných předpisů. Zde jde hlavně o nařízení ČNB, ČTÚ či parlamentu.

Jak na to…

Při vytváření AFS systému by se ideálně mělo postupovat v pěti krocích. Nejprve je nutné začít **kvalitní datovou základnou**, nad kterou se AFS systém bude tvořit. Bez dat v podstatě nelze dále postupovat. I když však data dostupná jsou, často se nachází ve značně neuspokojivém stavu.

Na straně zdrojových systémů totiž dochází ke vzniku překlepů, duplicit či neúmyslnému pozměnění vstupních dat. Jednou uživatel zadá „nám. Kapitána Jaroše“, jindy „nám. kpt. Jaroše“, což však z pohledu počítačového zpracování rozhodně nemusí být totéž. Pokud by data nebyla pročištěna, údaje v databázi by způsobovaly nepřesné chování algoritmů. Proto existují produkty na čištění, které dokáží většinu problémů automaticky odstranit – jedním z tuzemských dodavatelů je například společnost Profinit.

Druhým krokem je **definice tzv. statických, nebo také expertních scénářů**, které vzniknou ze zkušeností s daným prostředím, případně z rozhovorů s odborníky, kteří se v instituci odhalováním podvodů zabývají. Implementace těchto scénářů je levná, rychlá a přitom „zalepí největší díry“. Jejich vhodným kombinováním lze docílit poměrně dobré úspěšnosti.

Co si pod statickým scénářem představit? Například budeme hledat žadatele o úvěr, kteří v instituci žádali již desetkrát a pokaždé udali jinou výši čistého příjmu (vždy samozřejmě vyšší).

Třetím krokem je **profilování**. Instituce většinou disponují velkým množstvím informací o chování svých zákazníků a mohou je velmi efektivně používat. Představme si člověka v libovolné instituci, který pracuje často s počítačem. Z různých systémů můžeme sbírat záznamy o jeho aktivitě a posílat ho do antifraudového řešení, kde se budou načítat krátkodobé, střednědobé i dlouhodobé charakteristiky.

Z nich například vyplyne, že zaměstnanec chodí v 8:00 do práce, v 17:00 z práce, vyřeší dvacet případů, volá osmi lidem a přenese 300MB dat. Co ale dělat, pokud najednou ve 4 hodiny ráno zaměstnanec řeší 1 000 případů a přenáší 10 GB informací? Porovnání těchto údajů s dostupnými charakteristikami ukáže, nakolik je jeho chování problematické, a zda jde skutečně o útok či krádež údajů.

Zákazníci často poskytují společnostem obrovské množství dat, v němž nemusí být snadné se vyznat. Namátkou lze zmínit karty Tesco na nákup potravin. Pokud využijeme data z těchto karet, budeme vědět, kdy a jak často k nám zákazník chodí, jak a u koho platí a co a v jakém objemu kupuje. Co když chodí často k jedné pokladní a kupuje jen jeden rohlík? Algoritmy dokáží určit, že jde o netypické chování, které je potřeba prozkoumat. Možná o nic nejde, ale co kdyby…

V posledních letech zažívají obrovský boom sociální sítě a lidé jsou na nich ochotni prozradit úplně vše. Ačkoliv se za poslední rok se situace výrazně zlepšila, stále někteří uživatelé nedbají na nastavení soukromí a ochranu osobních dat, takže se lze k těmto informacím snadno dostat. Mnoho institucí má dnes navíc na Facebooku stránky, jejichž prostřednictvím získávají přístup k určitým datům svých fanoušků. I ta lze nahrát do AFS a zapojit mezi zdrojová data k předchozím scénářům.

Na co si dát pozor?

Nejčastější chybou při nasazení AFS jsou špatně nastavená očekávání zákazníka. Není pravda, že stačí systém nainstalovat, zmáčknout velké zelené tlačítko a od té doby bude vše krásné a bezpečné. Ladění a přizpůsobování trvá obvykle několik měsíců a provoz je během na dlouhou trať. Podvodníci si totiž nacházejí stále nové a rafinovanější způsoby.

Další potenciální bariérou může být nepřipravenost zákazníka, který čeká, že se vše povede hned. Nelze si myslet, že si lidé nevezmou dovolenou ani nebudou nemocní a že data potřebná pro systém sama vyskočí z datového skladu. Vyjednávání, domlouvání a papírování ukrojí z realizace velkou část.

Posledním problémem je nepřipravenost implementátora. Ten často nezná detailně prostředí, do kterého jde systém nasadit, a to s sebou nese nepříjemnosti. Obtíže samozřejmě časem zmizí, ale zpočátku mohou klientovi způsobit lehký šok.

Společnost Profinit většinu svých klientů zaujala nástrojem SVAT, který lze napojit na mnoho datových zdrojů. Nad informacemi je možné spouštět pokročilou SNA analýzu (analýza sociálních vazeb) či zvýrazňovat důležité skutečnosti. Každý se rád myšlenkami vrátí na základní školu, a tak je SVAT plný barev, obrázků a „šoupacích nastavovátek“. Grafické vyobrazení je totiž obvykle přehlednější než velká tabulka.

Čekat se nevyplácí

Většina organizací typicky problematiku podvodů vůbec neřeší. Své priority kladou zcela jiným směrem – například na růst obratu, nabírání zaměstnanců apod. K nasazení AFS systémů pak dochází až po nějakém velkém a bolestivém problému, který v organizaci stane.

Dalším faktorem, který instituce odrazuje od pořízení systému, je také cena a případné organizační změny, které s sebou zavádění AFS nese. Při rozumné implementaci se však náklady velice rychle vrátí. Vzpomeňme pojišťovny, které díky lepšímu vyhodnocováním škod snížily platby za povinné ručení téměř o polovinu.

Systémy jsou v zásadě financovány standardní objednávkou licencí a implementačních prací. Není obvyklé, že by zákazníci platili dohodnutý podíl na úsporách – tzv. success fee, jelikož se obávají, že by se při velkém množství případů model nevyplatil a navíc by pokazil jejich dobrou pověst.

Blízká budoucnost řešení AFS

Potenciál antifraud systémů lze vidět v NoSQL databázích, in memory real-time řešení a možná i v novém konceptu spolupráce institucí s klienty – assisted security. Do dalšího vývoje AFS se určitě promítne i již zmíněný trend sociálních sítí. Jak například hodnotit vztah, kdy byli dva klienti na stejné akci? Nebo když jsou přátelé? Znamená to, že se vážně znají, nebo jde jen „o náhodu“? Sociální sítě nabízejí mnoho podobných otevřených otázek, jejichž zodpovězení lze v následujících letech předpokládat. Kdo ví, možná jednou nedostanete půjčku jen proto, že máte známého podvodníka v přátelích na sociální síti.