Anglický termín fraud management dnes slýcháme častěji než jeho poněkud těžkopádný český ekvivalent řízení rizika podvodů. Slovo podvod většinou asociuje činnosti, jako jsou krádež, korupce, zpronevěra, praní špinavých peněz nebo vydírání. Právní definice podvodu se liší stát od státu, v České republice je podvod definován trestním zákoníkem. V rámci fraud managementu se ovšem této definice nedržíme striktně. Pojem podvod je zde používán v podstatně širším významu.

Definice podvodu podle trestního zákoníku

Trestný čin, jehož se dopustí ten, kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou.

Fraud management

aneb Předcházení podvodům ve finančních institucích

Lenka Blažková

Oblastí, kde se setkáváme s podvody, je mnoho. Nejčastěji jde o případy podvodů spáchaných v pojišťovnách, bankách nebo ve společnostech mobilních operátorů. Běžné typy podvodů jsou zneužití platebních karet, pokusy o neoprávněné získání úvěru nebo hypotéky, pojistné podvody, neoprávněné použití cizí telefonní SIM karty. Všechny ohrožené instituce přirozeně chtějí sebe i své klienty vůči podvodům chránit, návrh a dohled nad bezpečnostními opatřeními spadají do kompetencí oddělení řízení operačních rizik, přesněji do činnosti fraud risk managementu. Samostatnou kategorii pak tvoří tzv. počítačové podvody, kdy se neoprávněná osoba nezákonně naboural do systému společnosti a provádí nepovolené transakce. Nejčastěji se útočníci snaží převést finanční částky na vlastní zahraniční bankovní konta nebo se pokoušejí získat osobních či jinak citlivé údajů z databáze instituce. Odpovědnost za zabezpečení IT infrastruktury a testování její spolehlivosti má oddělení IT bezpečnosti.

Snahou oddělení operačního rizika už zdaleka není pouze včasné odhalení rizikového klienta na základě analýzy chování klientů podobného typu. Taková analýza totiž umožní odhalení pokusů pouze o ty typy podvodů, které se již někdy v minulosti vyskytly. V ideálním případě se ale usiluje i o odhalení podvodů zcela originálních, k nimž neexistují historické „vzory“. Další činnost souvisí s navržením pravidel a preventivních opatření, která případného podvodníka předem od pokusů o ilegální obohacení se na vrub konkrétní instituce nebo podniku odradí. V poslední řadě je zde vytváření strategie pro likvidaci podvodných událostí, k nimž již bohužel došlo.

Samotné řízení jakýchkoli rizik s sebou vždy nese nemalé náklady. Obecně, čím více podvodů budeme chtít identifikovat, tím budou tyto náklady vyšší. V praxi je samozřejmě velmi důležitá především efektivita fraud managementu – chceme mít výkonný fraud management, a to s co možná nejnižšími náklady. Každý podvod s sebou nese nějakou finanční ztrátu, tato ztráta by měla být určitě vyšší než náklady na odpovídající preventivní opatření. Proto je třeba podvody rozdělit do tříd, jak podle výše případné finanční ztráty, tak podle výše rizika, že ke konkrétnímu typu podvodu skutečně dojde. Finanční i časové zdroje lze pak vynaložit na preventivní opatření proti třídám podvodů s případnou vysokou ztrátou, jejichž výskyt má relativně vysokou pravděpodobnost, těmto třídám logicky náleží vyšší priorita.

Podvodníci ve vlastních řadách

Smutnou skutečností je, že pokusy o podvod nevznikají vždy pouze ze strany externích „klientů“, nýbrž s velikostí instituce roste i intenzita podvodů ze strany vlastních zaměstnanců. I těmto podvodům se snaží oddělení fraud risk managementu předcházet. Zejména se snaží vytvořit bezpečné prostředí, poskytuje školení o bezpečnostní politice instituce pro své zaměstnance a vytváří a udržuje firemní kulturu. Často je pro hlášení podezřelých událostí vytvořen interní elektronický systém, kam mohou zaměstnanci zaznamenat svá podezření na podvodné chování, ať už je pachatel uvnitř instituce nebo podniká nelegální činnost zvenčí.

Předcházení podvodům je již několik let záležitostí tisíců institucí po celém světě. Pro dosažení společného cíle je výhodné sdílení zkušeností s podvodnou činností a také s úspěšností zvolených preventivních opatření. Za tímto účelem vznikla celá řada seminářů a konferencí, a to jak na interní úrovni v rámci jednotlivých nadnárodních společností, tak na úrovni národní nebo mezinárodní v rámci jednotlivých oblasti (pojišťovnictví, bankovnictví a další). Předmětem konferencí není pouze diskuse nad interními preventivními programy proti podvodným událostem, ale také nad stávající legislativou týkající se podvodů nebo použitím moderních analytických metod v kombinaci s expertními pravidly. Existují i společnosti, jejichž hlavní činností je poradenství a podpora v oblasti fraud managementu.

IT a fraud management

Současné životní tempo je velice rychlé, a odpovídající jsou i nároky na poskytované služby. S dostupností internetu či mobilního telefonu se objevily i požadavky na on-line služby. Dnešní klienti již nechtějí osobně chodit na pobočky bank a pojišťoven, ani navštěvovat obchody nebo mobilní operátory, ale upřednostňují práci s elektronickými formuláři či internetovou samoobsluhou nebo telefonický kontakt. Zároveň je snazší ve firemních databázích rychle informace o klientech nejen vyhledat, ale také tyto informace sdílet. S výpočetní technikou a moderními statistickými a dataminingovými postupy mají tak finanční instituce i mobilní operátoři možnost vyvíjet dobré prediktivní modely za použití enormního množství historických dat, a navíc také tyto modely mohou okamžitě aplikovat pro účely vyhodnocení rizikovosti klienta nebo k identifikaci podvodné činnosti.

Díky počítačovým simulacím lze uměle simulovat dopad zvolené strategie fraud managementu a porovnat ji s aktuálně používanými postupy. Dobrý risk management zahrnuje i předpověď limitu pro maximální možnou ztrátu způsobenou podvodnou činností pro stanovené budoucí časové období a tzv. backtesting, kdy sledujeme, jak moc se lišila předpovězená ztráta od ztráty, jíž bylo dosaženo ve skutečnosti. Relativně nejnovější metody jsou z oblasti text miningu. S jejich aplikací dosáhneme vyšší efektivity modelů, neboť kromě numerických a kategoriálních údajů z databáze lze jako vstupy pro model použít také zpřesňující informace zakódované ve formě nestrukturovaného textu. Ze zmíněných oblastí je text mining využíván zejména v pojišťovnictví.

Moderní technologie jsou většinou náročné jak na hardwarové vybavení, tak na efektivitu a možnosti používaného analytického softwaru. Aplikace nejnovějších algoritmů je podmíněna zkušenostmi, analytickými znalostmi a schopnostmi specialisty fraud risk managementu. Finanční náklady na kvalitní fraud management tak někdy dosahují na první pohled ohromného rozsahu. Nicméně nutná počáteční finanční investice do moderních technologií a vzdělání analytiků je odměněna spolehlivým bezpečnostním systémem opatření a pravidel, která ve výsledku předejdou ztrátám mnohem vyššího objemu. ■

Autorka je odbornou konzultantkou firmy StatSoft CR.