Fraud management

aneb Jak předvídat podvody a jak jim předcházet?

Lenka Blažková

Podvody existují tak dlouho jak lidstvo samo. Některé jsou natolik důmyslné, že namísto pohoršení vzbuzují mnohdy spíše obdiv k člověku, který je dokázal vymyslet a zrealizovat. I finanční podvody, kterým se budeme v našem příspěvku věnovat, se objevují už s vynálezem peněz. Ve starověkém Řecku bylo popsáno několik případů, kdy tehdejší bankéři přijímali úspory svých zákazníků, které poté ovšem nebyli schopni vracet.
I v dávném starověku se můžeme setkat s falešnými mincemi, které byly vyráběny přidáním levnějších kovů ke zlatu či stříbru nebo obrušováním hran pravých mincí. Později se padělaly samozřejmě i bankovky. Kdysi byl tento zločin v některých zemích dokonce trestán smrtí – například v roce 1699 doplatil na svou padělatelskou činnost William Chaloner, kterého usvědčil Sir Isaac Newton. Soud mu určil smrt oběšením.

Slavné podvody z historie

Zločinci jsou tím nápaditější, čím důmyslnější bezpečnostní systém musí překonat. Příběh Franka Abagnala, jednoho z nejúspěšnějších podvodníků Ameriky, jenž si v šedesátých letech minulého století přišel celkem na dva a půl milionu dolarů prostřednictvím falešných šeků a platebních karet, je znám veřejnosti díky filmu Chyť mě, když to dokážeš v hlavní roli s Leonardem di Capriem. Časté jsou i případy zneužití pravomocí k vlastnímu obohacení – za všechny jmenujme Roberta Maxwella, který jakožto správce penzijního fondu využíval důchody svých zaměstnanců k financování vlastního domu v Londýně a půjčil z nich 34 milionů liber svojí společnosti Mirror Group Newspapers. Poslední finanční krize odhalila mezi jinými i Bernarda Madoffa, který díky reputaci solidního a zkušeného obchodníka získal důvěru investorů pro svůj investiční fond. K podvodu využil metodu u nás známou pod názvem letadlo nebo též pyramida, se kterou poprvé přišel jiný slavný podvodník Charles Ponzi. Celý trik spočívá v tom, že zisk je stávajícím klientům vyplácen z vkladů klientů nových. Je pouze otázkou času, kdy nárokovaná výplata převýší vklady nováčků. Madoff připravil svoje klienty celkem o 64 miliard dolarů. Z českých podvodníků nesmíme vynechat Viktora Koženého, který se skrze své fondy obohatil o sto miliard korun. Jako případ počítačového podvodníka uveďme Věnka Henrynka, který coby administrátor v GE Capital Bank převedl neoprávněně v období od roku 1999 do roku 2002 na své účty dohromady 193 milionů korun.

Typy podvodů

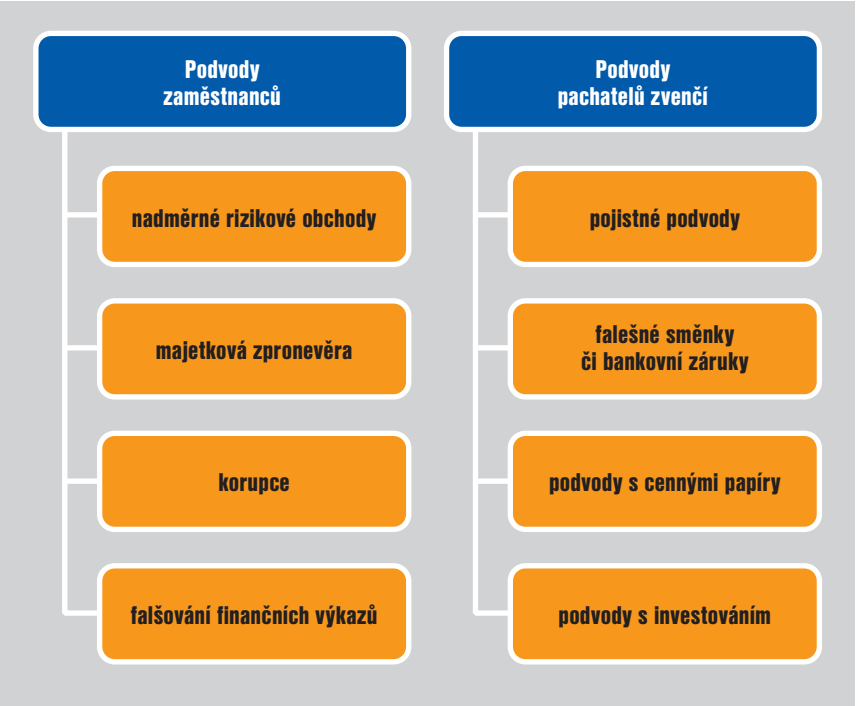
Finanční podvod definujeme jako nenásilný útok proti jednotlivci či společnosti, jehož výsledkem je finanční ztráta. Finanční podvody lze podle hlediska, kdo je pachatelem, rozdělit do dvou skupin: podvody zaměstnanců a podvody spáchané pachateli zvenčí. Nejčastější typy podvodů v obou skupinách znázorňuje schéma na obrázku 1. Samostatně stojí počítačové podvody, praní špinavých peněz, krádež identity a různá podvodná jednání.

Fraud management

Z předchozího výčtu možností podvodníků je zřejmé, že služeb oddělení operačních rizik a fraud managementu je ve větších finančních institucích opravdu zapotřebí.

Základem fraud managementu je identifikace příležitostí – určení oblastí, kde může k podvodům dojít. Z tohoto seznamu se zaměřujeme zejména na ty oblasti, u nichž je pravděpodobnost, že k podvodu dojde, vyšší, a kde je zároveň dopad konkrétní události závažnější (a to z různých hledisek: výše finanční ztráty, poškození dobrého jména instituce, právní důsledky apod.). Jednou z nejdůležitějších oblastí jsou informační technologie. Je třeba zabránit neoprávněnému přístupu do systému, následné neoprávněné změně práv, narušení integrity dat nebo bezpečnosti systému. Systém musí být bezpečný vůči útokům jak vnějších podvodníků, tak i vlastních zaměstnanců, kteří systém znají nejlépe. Kromě nastavení interních bezpečnostních předpisů či opatření a ochranných mechanismů proti podvodům zvenčí by každá finanční instituce měla mít přehled o aktuálním riziku, proto je snaha vyčíslit a pravidelně monitorovat expozici vůči

Obr. 1: Finanční podvody lze podle hlediska, kdo je pachatelem, rozdělit do dvou skupin



riziku podvodu. Standardně jsou nastaveny limity pro tuto expozici, které říkají, jaké riziko je ještě přijatelné a jaké už nikoli.

Předcházení podvodům bývá jeden z nejlevnějších způsobů, jak řídit rizika vzniklá podvodnou činností. Nastavíte-li vysoká bezpečnostní opatření, pro podvodníky může být jejich obcházení příliš nákladné, pracné nebo rizikové, aby se jim vyplatilo, a raději zkusí štěstí někde jinde. Míru podvodů sníží i vzdělávání zaměstnanců – školení, kde se dozví, na jaké typy podvodů si mají dát pozor, a budou upozorněni na události, které by měly zvýšit jejich ostražitost, vyslechnou rady, jak se mají zachovat, spolu se systémem, jenž umožňuje reportování podezřelého jednání, přispívají ke včasnému odhalení pokusů o podvod.

Žádný systém nicméně neposkytuje vůči podvodům absolutní ochranu. Pravidelně je nutné monitorovat, zda je systém stále dostačující, a rozšiřovat jej o nové prvky, neboť vnitřní systémy se v průběhu času vyvíjí a i podvodníci přichází s novými a novějšími způsoby, jak se vypořádat se stávajícími opatřeními. Ideální je být před nimi o několik kroků napřed.

Moderní metody pro odhalování podvodů

S nástupem počítačů, elektronických transakcí a platebních karet se jako vhodné nástroje fraud managementu ukazují také moderní metody pro data mining. Finanční instituce mají dnes k dispozici detailní informace o předchozím chování milionů svých klientů, ze kterých lze například usuzovat, jaké chování je pro jednotlivé klienty typické. Vyskytne-li se u klienta (vzhledem k jeho historii) netradiční požadavek, může to být známkou zneužití klientovy identity jinou osobou (jako je krádež platební karty, na kterou může upozornit pokus o výběr nezvykle vysoké finanční částky). Výhodou je, že podobné události lze užitím moderních metod monitorovat a vyhodnocovat automaticky. Navíc lze prostřednictvím data miningu odhalit skryté vztahy mezi jednotlivými klienty, společnostmi nebo událostmi. Efektivní algoritmy si poradí i s analýzou dat o velmi velkém objemu – důležité poznatky a vztahy jsou odhaleny během velmi krátké doby, pro účely fraud managementu jsou proto aktuální, a tudíž i užitečné. Data mining je vhodný i pro sledování efektivity interních kontrolních mechanismů, systematické sledování podvodných událostí a odhalování oblastí, které jsou vzhledem k podvodům nejvíce zranitelné.

Podvody bývají odhaleny i díky e-mailovým zprávám. Každá větší instituce má možnost sledovat e-maily svých zaměstnanců, je-li to nutné. V minulosti bylo mnoho interních podvodů odhaleno právě při kontrole vzájemné komunikace mezi zaměstnanci. Automaticky lze tuto komunikaci sledovat pomocí tzv. text miningu, dojde tak k filtrování zpráv – revizi bude třeba provést jen u zpráv s častějším výskytem slov, která mohou indikovat podvodné jednání.

Bezpečnostní prostředky jsou důmyslnější, než bývaly, a obejít je se podaří jen velmi schopným jedincům či skupinám. Tento fakt by ovšem nikoho neměl uklidňovat, jak jsme poznamenali v začátku našeho příspěvku, sklony k podvodům jsou lidstvu vlastní od nepaměti a je nepravděpodobné, že by se to nyní mělo změnit. I jediný dobře naplánovaný podvod může poškodit mnoho klientů či způsobit finančním institucím existenční problémy. Z tohoto důvodu jsou investice do bezpečnostních opatření i data miningových aplikací velice prozíravé. ■

Autorka je odbornou konzultantkou firmy StatSoft CR.

Inzerce

StatSoft CR s.r.o.
www.statsoft.cz

Statisticky vzato, na finanční podvody obvykle jako první upozorní data. **Naslouchejte jim.**

StatSoft®
STATISTICA