HROZÍ RISKAŘŮM ZAKRNĚNÍ?

Když jsem byl požádán o příspěvek zaměřený na vyhodnocení změn v oblasti řízení rizik za posledních deset let, neuvědomil jsem si ihned základní zádrhel, který je způsoben omezením paměti. Jen obtížně se mi přesně vybavuje, zda mé vzpomínky sahají do období před třinácti, nebo osmi lety. Jak z tohoto omezení vybruslit? Jednoduše, až na jednu výjimku se vyhnu jakémukoliv přesnému datování. Zároveň s ohledem na mé dlouhodobé působení v oblasti nefinančních rizik se budu věnovat primárně této části rizik a oblast úvěrových či tržních rizik ponechám stranou.

Mgr. Michal Němec
Česká spořitelna
ředitel Řízení nefinančních rizik

Michal je ředitelem řízení nefinančních rizik v České spořitelně, kde se aktuálně zabývá oblastí prevence praní špinavých peněz, řízením operačních rizik, prevencí podvodů a oblastí GDPR. Má zkušenosti i z oblastí compliance, fyzickou bezpečností, řízením vnitřního kapitálu i krizovým řízením. Na počátku pracovní kariéry získal zkušenosti i na různých pozicích v rámci bankovního dohledu České národní banky.

Přestože základní principy řízení rizik se za posledních deset let příliš nezměnily (stále se řídíme obezřetnostní vyhláškou ČNB č. 163 z roku 2014), byla vydána řada doplňujících technických standardů, doporučení, které tyto principy dále rozpracovávají či upřesňují. Nevnímám však, že by došlo k výraznému posunu z hlediska celkového konceptu pojetí nefinančních rizik. Byly však vydány nové regulace, které zvyšují přístupnost veřejnosti k některých službám (jako příklad mohu uvést regulaci v oblasti platebního styku, která umožnila vstup na trh novým licencovaným subjektům), zabývají se zcela novými oblastmi (např. regulace související s udržitelností) nebo dále zvyšují ochranu spotřebitele. Ale jelikož v rámci tohoto příspěvku bych se chtěl spíše zaměřit na dopady na způsob řízení rizik v obecnější rovině, nebudu se detailně zabývat uvedenými regulacemi a jejich přínosem pro ochranu klientů, společnosti či bankovního systému jako celku. Zamyšlení budu věnovat spíše rozdílům v práci specialistů řízení rizik, kde vnímám za posledních deset let velkou změnu.

Již před deseti lety jsem považoval bankovnictví za komplexní odvětví, a i mezinárodně uznávaní znalci či hlavní metodici České národní banky již připouštěli, že téměř není v lidských silách pojmout veškeré souvislosti vycházející z regulatorních požadavků na banky. Přesto se mi komplexita aktuálních požadavků a nároků na řízení rizik zdá být neporovnatelná.

Můžeme začít vnitřním organizačním uspořádáním některých bank, i když se nejedná o oblast, která přímo souvisí s legislativními požadavky. Spíše reaguje na stále se zrychlující vývoj externího prostředí, které nutí banky k větší flexibilitě a akceschopnosti, než tomu bylo v předcházejících letech. To zvláště platí pro banky, které nechtějí jen pasivně sledovat a reagovat na probíhající změny, ale chtějí se přímo

na nich aktivně podílet, a přispívat tak k samotnému určování nových trendů.

Příklad uvedu na fungování týmů, které se podílejí na akceptaci nových produktů nebo ještě obecněji jakýchkoliv změnových procesů. Jako zástupce takového týmu mohu použít operační rizika, která byla jednou z prvních oblastí mého zaměření. Ještě před dekádou byla operační rizika vnímána poměrně odděleně jako úzce specializovaný tým, který se do značné míry věnoval plnění požadavků regulátora. Za tímto účelem se operační rizika zabývala vyhodnocováním řady nástrojů, které byly používány pro dlouhodobé monitorování vývoje tohoto rizika nebo přispívala expertním hodnocením při zavádění nových produktů. Některá z těchto cvičení byla ročně aktualizována, přičemž často se jednalo jen o pouhé drobné korekce, protože mezi jednotlivými roky nedocházelo k výrazným dramatickým změnám. Jednotlivé změny v procesech nebo systémech byly závislé na pravidelných a s velkým předstihem naplánovaných termínech pro nasazování novinek do produkce. Tradiční banky byly rovněž často velmi hierarchické a jednotlivé změny v produktech či procesech procházely schvalovacím procesem na úrovni řídících pracovníků, ať už na úrovni celého představenstva, či jeho poradních orgánů. Z toho důvodu bylo poměrně jednoduché nastavit a udržovat si přehled o změnových požadavcích podléhajících schvalovacímu procesu banky. Postačovalo udržovat kontakty s poměrně úzkou skupinou kolegů, aby příslušné týmy zapojené do posuzování rizik měly jistotu o zapojení do všech relevantních procesů.

V dnešním pojetí vnímám výrazný odklon od tohoto hierarchického uspořádání k větší autonomii jednotlivých týmů, které se zabývají procesy ve svěřené oblasti definované podle typů produktů, klientských segmentů či potřeb klientů. Zároveň v souvislosti s rychlejšími požadavky na nasazování nových funkcionalit dochází často k uvádění nových verzí systémů nebo produktů, jakmile jsou dané novinky vyvinuty a příslušně otestovány. Cílem nejedné společnosti tak může být v podstatě průběžná kontinuální aktualizace používaných aplikací. Tímto rostou požadavky na operační rizika či další obdobné týmy na průběžný sběr informací o chystaných změnách, jelikož vlastní odpovědnost za vývoj a nasazování novinek je často delegována na jednotlivé týmy. Zvláště u menších změn tak není dodržován dříve častěji využívaný centralizovaný systém schvalování, což právě přináší nové výzvy pro kontrolní funkce.

„vlastní odpovědnost za vývoj a nasazování novinek je často delegována na jednotlivé týmy.“

Jak na tuto změnu mohou operační rizika reagovat? Mohou se vydat cestou průběžných a detailnějších kontrol, pomocí kterých se mohou ujišťovat, že jim pod rukama neprobíhají změny bez patřičného vyhodnocení rizik. Tím se však snadno dostanou do vleku událostí a případné dodatečné požadavky se jim budou obtížněji prosazovat. Alternativou je větší specializace členů tohoto týmu, užší zapojení do projektů již při jejich vývoji a do průběžného přispívání k nastavení výsledného produktu. A právě díky větší specializaci může docházet k vyšší přidané hodnotě těchto specialistů. Ta v optimálním případě může přispět i k přímému oslovování těchto funkcí vlastníky nových produktů, protože sami budou více rozpoznávat přidanou hodnotu specialistů z risku.

To ale není jediná změna. Zároveň roste požadavek na vyšší efektivitu využívání jednotlivých nástrojů pro řízení rizik, jelikož dnes už málokoho uspokojí tvrzení, že se jedná o regulatorní požadavek. Přestože je regulace stále významným argumentem, je jednotlivými obchodními týmy vyvíjen větší tlak na její uchopení způsobem, který bude pro všechny účastníky srozumitelný a přínosný. Tento trend vnímám z dlouhodobého hlediska jako velmi pozitivní, protože vede k hlubšímu zamyšlení se nad jednotlivými požadavky. Výstupy z těchto závěrů pak nekončí čistě v týmech řízení rizik za účelem naplnění očekávání regulátora, ale jsou častěji prakticky využívány. Zde vnímám i velmi pozitivní vliv mladé generace, která nemá zábrany upozorňovat na věci, které jí nedávají smysl, a mnohem častěji proaktivně přichází s alternativními návrhy.

Další významnou změnou je, že bankovnictví přestalo být úzce izolovaným odvětvím, které poskytovalo pouze základní služby vyplývající z původní bankovní licence. Dříve v podstatě záleželo na strategii banky, které produkty nabídne klientům a jaké parametry u těchto produktů nastaví. Díky tomu bylo jednodušší i řízení souvisejících rizik. V dnešní době, kdy dochází k výrazné digitalizaci nejen v komerčním, ale i státním sektoru, jsou banky stavěny před nové výzvy. Příkladem mohou být nástroje pro ověření identity klienta, které byly dříve vydávány každou institucí výhradně pro jejich vlastní potřebu. Dnes je prostřednictvím Bank ID využívána identita klienta jako nástroj nejen k otevírání produktů či jejich obsluze v jiných bankách, ale i pro přistupování ke státním službám či různým dalším komerčním účelům. V této souvislosti se otevírají nová rizika například v situaci, kdy banka nedostatečně identifikuje klienta, kterému vydává vlastní identitu. Takto získaná identita může být následně využita k různým nežádoucím účelům, např. k neoprávněnému uzavření smlouvy či neautorizovanému přístupu k osobním údajům jiného klienta. Tím se banka vystavuje novým typům rizik, kterými se dříve vůbec nemusela zabývat.

Trendu rostoucí digitalizace a různého využívání bankovní identity nenahrává ani situace stále pokročilejších útoků na klienty jednotlivých bank. Tyto útoky již nesměřují jen k přímému obohacení útočníků prostřednictvím jednorázového převodu peněz či majetku klientů,

ale objevují se i případy pokusů o neoprávněné ovládnutí klientské identity. Tyto pokusy kladou výrazně zvýšené nároky na monitoring i netransakčních aktivit klientů a detekci jakýchkoliv anomálií při využívání identity jako takové. Již tedy nepostačuje sledovat pouze převody prostředků či výběry hotovostí, byť se stále jedná o silné rizikové indikátory. Situaci značně ztěžuje pokročilá manipulace klienty ze strany útočníků, kdy i na přímé dotazy zástupců banky reagují klienti kvůli jejich manipulaci ze strany útočníků úmyslně nepravdivými informacemi. Operátorům tedy již nepostačují prosté dotazy, zda klient prováděl danou operaci, či nikoliv, ale je potřeba využívat aspoň základů psychologie a pokusit se klienta vymanit ze zajetí útočníka. Není výjimkou, když klienti až po delším rozhovoru s řadou otázek, ale i popisu historických zkušeností banky s různými typy útoků připustí, že i oni mohou být obětmi útoku útočníka. Ano, mohlo by být konstatováno, že v této oblasti jdou banky již daleko nad rámec svých povinností, ale na druhou stranu není v zájmu bank zpochybnění bezpečnosti elektronických služeb ze strany jejich klientů, kdyby se tyto typy útoků staly úspěšnějšími. Naštěstí v tomto boji nejsou banky osamocené, ale mohou využívat úzké a prospěšné spolupráce s policejními složkami či přímo s Českou národní bankou.

Nedílnou součástí změn v posledním desetiletí je i oblast využívání nových cloudových technologií, kdy dochází ke stále častějšímu využívání služeb vyvinutých třetími stranami a jejich použití ve vlastních aplikacích. Tento přístup bezesporu urychluje práci vývojářů, na druhou stranu je opět v této oblasti potřeba zvyšovat míru jistoty kvality a bezpečnosti využívaných služeb a nástrojů. Proto je žádoucí nový způsob vývoje podpořit zvýšeným důrazem na testování výsledných řešení, včetně penetračních testů zaměřených na bezpečnost řešení. A to se zatím nezmiňuji o nových modelech stále výrazněji se prosazujících, např. algoritmech založených na principech zpracovávání a vyhodnocování obrovského množství textových informací typu Chat GPT.

Přestože se bezesporu jedná o perspektivní oblast, která má potenciál usnadnit práci v mnoha oblastech, je opět před masovějším využíváním těchto technologií potřebné jim detailně porozumět a vyhodnotit nejen jejich přínosy, ale i nová rizika. Mimochodem sám jsem tuto technologii použil zkušebně pro porovnání rozdílů v jednotlivých vyhláškách ČNB zaměřených na obezřetnostní principy platných pro banky a výsledky byly poměrně uspokojivé, aniž by mi to zabralo mnoho času.

„je žádoucí nový způsob vývoje podpořit zvýšeným důrazem na testování výsledných řešení“

Výše uvedená rizika bych zařadil spíše do kategorie provozních rizik, ale nechtěl bych zároveň opomenout charakteristiku, kterou pro bankovní sektor považuji za naprosto zásadní. Tou je důvěra klientů v danou instituci, kterou z pohledu řízení rizik lze zahrnout do kategorie reputačních rizik neboli velmi jednoduše pod riziko ztráty důvěry v danou instituci.

Zde si dovolím zaspekulovat a vyjádřit velmi osobní názor, že dříve se klienti zaměřovali především na stabilitu dané společnosti, tedy, zda banka je dostatečně silná a zdravá na to, aby klientům vyplatila jejich prostředky, kdykoliv je budou potřebovat. V dnešní době, s ohledem na míru stability našeho bankovního sektoru, začala řada klientů stabilitu banky vnímat jako automaticky garantovanou věc, o kterou se v podstatě nemusí zajímat.[1] Klienti tak začali rozlišovat další řadu parametrů, které jsou z jejich pohledu důležité. A tím může být míra dostupnosti jednotlivých klientských řešení, složitost používání bankovních aplikací, včetně jejich instalace, množství informací poskytovaných k jednotlivým produktům či službám nebo rychlost zpracování klientských požadavků, včetně potenciálních reklamačních řízení.

Z pohledu klienta jistě oprávněná očekávání opět mají dopad na pracovníky řízení rizik, kteří stále více musí zohledňovat klientské potřeby a jejich očekávání. A to i v případech, kdy daná opatření mohou být spatřována jako opatření na úkor kvality či bezpečnosti poskytovaných služeb. Cílem je tedy nacházet řešení, která budou uživatelsky stále akceptovatelná, ale na druhou stranu budou stále splňovat požadavky na bezpečnost identifikace klienta, zajištění dané služby či naplnění regulatorních povinností ve vazbě na informační povinnosti. Při hledání cílových řešení se opět vyplácí velmi úzká spolupráce mezi obchodními či produktovými týmy bank a řízením rizik.

Tyto selektivně vybrané ukázky jsem vybíral se záměrem ukázat, jak se i pro zástupce risk managementu významně mění rozsah jejich práce a jak je pro ně podstatné udržovat se ve střehu a vstřebávat celou řadu novinek. Jak jsem uvedl výše, záměrně jsem se nezabýval změnami, které bankám přináší nové regulatorní požadavky.

Přestože bychom jako risk manažeři měli být zvyklí uvažovat o rizicích, které mohou nastat s velmi malou pravděpodobností, netroufám si odhadnout, kam se naše práce posune nejen za dalších deset let, ale i ve výrazně kratším období. Proto za jednu ze základních dovedností pro risk management považuji otevřenost novým směrům a zapálenost pro seznamování se s čerstvými myšlenkami. Zároveň bychom se měli snažit jim porozumět a dokázat nejen rozpoznat významná rizika, ale i vidět budoucí perspektivní využití. Takové nastavení nás, pevně věřím, udrží relevantními partnery pro byznys. Jsem přesvědčen, že náplň práce risk manažera bude sice stále náročnější, ale zároveň i velmi pestrá a zajímavá.

Ať už jste risk manažerem, či kolegou v jiné kontrolní funkci, nebo jste dokonce zástupcem byznysu, přeji vám, aby vás práce naplňovala a nacházeli jste si v ní i krásné poslání. ■

[1] Ponechám na vašem úsudku, jak je toto uvažování klientů ovlivněno i stoprocentním pojištěním vkladů do výše 100 tis. eur.