# Co řeší banky a pojišťovny v oblasti sdílení a přístupu k dokumentům?

Zdeněk Bínek

Banky a pojišťovny se v dnešní on-linové době snaží maximálním způsobem vyjít vstříc svým zákazníkům, partnerům i zaměstnancům a nabídnout rychlý, komfortní a produktivní přístup k co nejvíce informacím. Na druhou stranu zřejmě neexistuje odvětví, které dodržuje tak vysoké standardy v oblasti ochrany klientských dat, zabezpečeného přístupu, a obecných i specifických regulačních nařízení.

I když tyto na první pohled protichůdné tendence poněkud vnucují myšlenku o vytváření kulatého čtverce, můžeme na základě zkušeností z projektů Acronis v bankách a pojišťovnách ujistit, že získat komfortní, produktivní, a přitom bezpečný a auditovatelný přístup k citlivým informacím ve finančním sektoru je skutečně možné.

## Bankovní scénáře

Pokud se podíváme čistě na bankovní instituce, ty většinou řeší výzvy dvojí druhu – přístup interních pracovníků a přístup externích stran (nejčastěji klientů).

V bankách pracuje zpravidla tisíce až desetitisíce zaměstnanců na stovkách projektů, v rámci kterých využívají nejrůznější pracovní dokumenty. Každý projekt zahrnuje řadu lidí z nejrůznějších pracovních pozic, skupin a oddělení, pro které jejich projektový manažer musí zřídit přístupy k dokumentům, většinou prostřednictvím žádostí na IT helpdesk. Ne všichni pracovníci mají mít přístup ke všem dokumentům, ne všichni mají mít plný přístup včetně zápisu, během projektu někteří odcházejí, pro nové je třeba zřizovat nový přístup atd. Jedná se o velmi komplikovaný proces, který projekty zbytečně prodlužuje. Proto projektoví manažeři v bankách dnes hledají způsoby, jak mohou udělovat přístupy samoobslužně a s dokonalým přehledem o tom, kdo a kdy přistupoval ke konkrétnímu dokumentu –z počítače či z mobilních zařízení – a co s ním prováděl.

Banky neřeší pouze interní přístup, ale také sdílení dokumentů s externími uživateli, ať již dodavateli nebo koncovými zákazníky. Těmito dokumenty bývají často velmi citlivé osobní informace typu oskenovaný identifikační průkaz, důvěrné informace o finanční situaci, čestná prohlášení apod. Aby svým klientům poskytli možnost samoobslužné správy těchto informací, snaží se vytvářet webové portály se zabezpečeným přístupem s cílem urychlit výměnu dat mezi bankou a zákazníkem a zefektivnit zákaznické procesy.

## Pojišťovnický scénář

Podobné výzvy v oblasti sdílení informací s externími uživateli řeší také mnoho pojišťovacích společností. Pojišťovny disponují stovkami externích agentů, kteří prodávají pojišťovací produkty. Ačkoliv nejsou interními zaměstnanci pojišťoven, potřebují stejný přístup k dokumentům uloženým na interních serverech. Specifickým požadavkem ze strany pojišťoven jsou funkcionality umožňující přístup k těmto dokumentům pouze v režimu „read-only“ bez možnosti jejich úprav či dokonce stažení ze serveru. Zde jde především o kontrolu nad tím, aby nedošlo k úniku citlivých informací a k jejich zneužití.

Z těchto zkušeností vycházejí klíčové parametry sdílení souborů pro banky a pojišťovny. Řešení musí být především instalováno na interních systémech. To je hlavní požadavek finančních institucí, které odmítají přenášet data do cloudu, a navíc potřebují, aby vlastní úložiště bylo šifrováno. Vedle toho by mělo poskytovat bezpečný mobilní přístup s nastavitelnými omezeními typu zákazu stahování či tisku dokumentu na lokální tiskárnu. Obecně pak musí obsahovat široké možnosti nastavení uživatelských oprávnění dle konkrétních skupin souborů, režimu přístupu (zápis, download, preview), pracovních rolí či doby expirace přístupu. A nakonec k dispozici musí být funkcionalita umožňující získat kompletní historii přístupu a změn dokumentu ke splnění compliance požadavků. ■

Zdeněk Bínek

Autor článku je ředitelem společnosti Zebra Systems, která na našem trhu zastupuje značku Acronis.

## Acronis Files Advanced

K prověřeným řešením pro sdílení, synchronizaci a přístup k podnikovým dokumentů v oblasti patří Acronis Files Advanced. Mezi jeho hlavní vlastnosti se řadí:

- Acronis Policy Engine pro vytváření přesně nastavených bezpečnostních politik pro konkrétní uživatele, zařízení a soubory;
- Auditní logy o aktivitách uživatelů, o jejich přístupech ke konkrétním dokumentům a o sdílení s autorizovanými uživateli;
- Integrace s hlavními Mobile Device Management (MDM) partnery včetně MobileIron, BlackBerry a Citrix Worx;
- Nasazení on-premise na firemní infrastruktuře.