Deloitte.

EBA: Pokyny k užívání moderních řešení pro vzdálenou identifikaci klientů

Dostupnost moderních digitálních technologií spolu se změnami v chování klientů významně urychlily nárůst poptávky finančních institucí po možnostech vzdálené identifikace klientů. Vzhledem k tomu, že pátá směrnice AML EU o boji proti praní špinavých peněz neposkytuje dostatečně jasné informace o tom, co je a co není povoleno při vzdálené identifikaci, vydal Evropský orgán pro bankovnictví (EBA) pokyny, které stanovují společné normy EU pro vývoj a provádění spolehlivých, riziko zohledňujících počátečních kroků CDD (Customer Due Diligence) v procesu dálkové identifikace klientů. Počátek platnosti pokynů byl stanoven na 2. října 2023.

Zásady a postupy týkající se vzdálené identifikace klientů

Zásady a postupy úvěrových a finančních institucí by měly sestávat z obecného popisu řešení pro **shromažďování, ověřování a zaznamenávání** informací v průběhu celého procesu vzdálené identifikace klientů. Měly by také určit kategorii **klientů, produktů a služeb** způsobilých pro dálkovou identifikaci a také objasnit, které kroky jsou plně autonomní a které vyžadují lidský zásah. Zásady se musí týkat také **školicích programů** (úvodního a pravidelného), jež zajistí informovanost zaměstnanců a jejich vždy aktuální znalosti o fungování řešení pro vzdálenou identifikaci klientů.

Správa

Schválení zásad a postupů pro vzdálenou identifikaci klientů a dohled nad jejich správným prováděním je povinností **řídicích orgánů** úvěrových a finančních institucí. **Compliance officer** by měl připravit zásady a postupy pro splnění požadavků CDD a zajistit, aby zásady a postupy pro vzdálenou identifikaci klientů byly prováděny účinně, pravidelně přezkoumávány a v případě potřeby upravovány.

Předrealizační hodnocení a průběžné monitorování

Úvěrové a finanční instituce musí posoudit vhodnost řešení z hlediska **úplnosti a přesnosti shromažďovaných údajů a dokumentů**. Měly by také posoudit dopad používání řešení pro vzdálený přístup ke klientům a rizik v rámci celé instituce, včetně rizika praní špinavých peněz a financování terorismu, operačních, reputačních i právních rizik. Je nutné provést testy k posouzení rizik podvodů, včetně rizik spojených s krádežemi identity a dalších bezpečnostních rizik. Dále je nutné provést komplexní **„end-to-end" testování fungování tohoto řešení**. Úvěrové a finanční instituce by měly začít používat vzdálenou identifikaci klientů až poté, co se ujistí, že je možné ji integrovat do širšího systému vnitřní kontroly dané instituce.
Po zavedení řešení a postupů identifikujících rizika by finanční instituce měly tato řešení průběžně monitorovat, tak aby zajistily **kvalitu, úplnost, přesnost a přiměřenost údajů** shromážděných během procesu vzdálené identifikace klientů. Přezkumy ad hoc by měly probíhat v případě, že u úvěrové či finanční instituce nastanou změny v jejím vystavení vůči riziku praní špinavých peněz a financování terorismu, při zjištění nedostatků ve fungování řešení, v případě zjištění nárůstu počtu pokusů o podvod nebo v případě změn právního či regulačního rámce.

Proces identifikace a ověřování

Úvěrové a finanční instituce zajistí, aby:

- informace získané prostřednictvím řešení pro vzdálenou identifikaci klientů byly aktuální a přiměřené;
- veškeré obrázky, video, zvuk a data byly pořízeny v čitelném formátu a v dostatečné kvalitě, aby byl klient jednoznačně rozpoznatelný;
- proces identifikace nepokračoval, pokud byly zjištěny technické nedostatky nebo neočekávané přerušení spojení.

Dokumenty a informace shromážděné během procesu vzdálené identifikace by měly být opatřeny **časovým razítkem a bezpečně uloženy v čitelném formátu**. V situacích, kdy nejsou poskytnuté podklady dostatečné, by měl být proces individuální identifikace klienta na dálku **přerušen a znovu spuštěn** nebo přesměrován k **osobnímu ověření**.

- Řešení pro vzdálenou identifikaci klientů zavedená úvěrovými a finančními institucemi zajistí, že existuje shoda mezi viditelnými informacemi o fyzické osobě a poskytnutou dokumentací.
- Pokud je klient právnickou osobou, je provedena kontrola záznamu vedeného ve veřejném registru.
- Pokud je klient právnickou osobou, je fyzická osoba, která jej zastupuje, oprávněna jednat jeho jménem.

Pokud se používá **bezobslužné řešení pro vzdálenou identifikaci klientů** (klient při ověřování nekomunikuje se zaměstnancem), měly by instituce zajistit, aby:

- všechny fotografie nebo videozáznamy byly pořízeny za vhodných světelných podmínek;
- všechny fotografie nebo videozáznamy byly pořízeny v době, kdy klient provádí proces ověření;
- bylo provedeno ověření s detekcí živosti[1];
- byly použity silné a spolehlivé algoritmy k ověření, zda pořízená fotografie nebo video odpovídají fotografii či fotografiím získaným z úředního dokladu nebo dokladů patřících klientovi.

[1] Detekce živosti v biometrii je schopnost systému zjistit, zda je otisk prstu nebo obličej (případně jiné biometrické údaje) pravý (získaný od živé osoby přítomné v místě snímání), nebo falešný (získaný od podvrženého materiálu či neživé části těla).

Pokud se používá **obslužné řešení pro vzdálenou identifikaci klientů** (klient komunikuje se zaměstnancem, který provádí proces ověření), měl by tento proces:

- zajistit, aby kvalita obrazu a zvuku byla dostatečná a umožňovala řádné ověření;
- využívat účasti dostatečně vyškoleného zaměstnance se znalostí platné regulace AML/CFT a bezpečnostních aspektů ověřování na dálku;
- vypracovat průvodce rozhovorem, který by definoval následné kroky procesu ověřování na dálku a také kroky, které se vyžadují od zaměstnance, pokud během ověřování na dálku zpozoruje podezřelé chování.

Další opatření

Pokud je to možné, měla by řešení pro vzdálenou identifikaci klientů zahrnovat **náhodnost** v pořadí akcí, které má klient pro účely ověření provést.

Pro zvýšení spolehlivosti procesu ověřování lze použít následující kontrolní mechanismy:

- první platba je čerpána z důvěryhodného účtu klienta;
- použití náhodně vygenerovaného jednorázového a časově omezeného přístupového kódu zaslaného klientovi;
- pořízení biometrických údajů za účelem jejich porovnání s údaji získanými prostřednictvím jiných nezávislých a spolehlivých zdrojů;
- telefonické kontakty nebo zásilka do vlastních rukou klienta.

Existuje možnost zadat řešení vzdálené identifikace klientů poskytovatelům třetích stran nebo jinému externímu poskytovateli služeb a využít řešení důvěryhodných služeb a národních identifikačních procesů.

Orgán EBA považuje za důležité, aby všechny zúčastněné strany rozuměly možnostem těchto nových řešení a také aby si byly vědomy rizik praní peněz a financování terorismu vyplývajících z užívání těchto nástrojů a přijaly opatření k účinnému zmírnění těchto rizik.

Věděli jste, že společnost Deloitte nabízí komplexní podporu v oblasti vzdálené identifikace klientů a pomůže vám správně nastavit všechny související procesy? **Pro více informací nás kontaktujte.**

Kontakty:

Martin Kubačka
Partner | Deloitte Czech Republic
mkubacka@deloittece.com
+420 776 306 694

Tomáš Mihóčik
Senior Manager| Deloitte Slovakia
tmihocik@deloittece.com
+421 910 820 005

Marie Vichrová
Specialist Lead | Deloitte Czech Republic
mvichrova@deloittece.com
+420 735 715 397