CYBER LAUNDERING
- hlavní metody a trendy

Lukáš Poznar

17.4.2024

ČSOB
Jednoduše pro vás

Cybercrime x Cyber laundering

Jednoduše pro vás

Cybercrime *(zločin bez hranic)*

***Kybernetický zločin, internetová či počítačová kriminalita** = použití internetu k páchání predikativních trestných činů. Trestné činy, které jsou prováděny v kyberprostoru pomocí elektronické komunikační sítě a informačních systémů. Často zdroj prostředků pro následný cyber laundering.*

Může být dělena do dvou kategorií:

- **Kybernetické zločiny nebo kybernetické události** zahrnují kompromitování nebo získání nezákonného přístupu k počítači nebo počítačovému systému spolu s jeho službami, zdroji a informacemi. Kyberzločinci mohou tyto přístupy využít ke krádeži finančních údajů, údajů o platbách kartou a identity uživatelů. Mezi běžné příklady patří hackování, ransomware a malware.

- **Zločiny kyberneticky podpořené**, kdy zločinci používají počítače nebo počítačové systémy ke spáchání trestných činů, jako je praní špinavých peněz. Tato kybernetická kriminalita je na vzestupu a zahrnuje trestné činy související s duševním vlastnictvím, phishing, vhishing, quishing, milostné podvody, podvody, obchodování se zbraněmi, obchodování s drogami, kompromitace obchodních e-mailů a trestné činy související s online obsahem, včetně sdílení obrázků zneužívání dětí.

Mnoho druhů trestné činnosti, která dříve probíhala v reálném světě, se přesunulo zcela nebo z části do online prostředí nebo je zprostředkováváno online. Některé typy kybernetické kriminality se dostaly do fáze profesionalizace „zločin jako služba“ (Dark Web, BlackMarkets).

Cyber *(on-line)* money laundering

***Cyber laundering** = zločinci používají internet k vytvoření anonymity nebo nevysledovatelnosti praní špinavých peněz.*

Používání online služeb k legalizaci výnosů z trestné činnosti a financování terorismu. Zdroje finančních prostředků jsou obvykle z předchozích aktivit v oblasti počítačové kriminality. Zahrnuje více či méně sofistikovaná schémata a spoléhá na různé typy operací a poskytovatelů finančních služeb, od bankovních převodů, karetních transakcí, výběrů/vkladů hotovosti, využívání virtuálních aktiv, elektronických poukázek a služeb převodu peněz, včetně zapojení bílých koní on-line nebo podpory zločinu ve fyzickém světě.

Řetěz je často „přerušen“ hotovostními či karetními operacemi, které tradičně provádějí bílí koně, po nichž někdy následuje použití tradiční platební služby. V některých schématech lze okamžitě a téměř anonymně převést prostředky do jiné země.

Dva z nejběžnějších typů kybernetického praní jsou:

- ***Instrumental digital laundering** – jeden (nebo více) kroků trestného činu proveden pomocí digitálních metod.*
- ***Integral digital laundering** – celá cesta za zločinem probíhá digitálně.*

Regulatorní výzvy

ČSOB
Jednoduše pro vás

Regulatorní EU balíček

Návrh 6.AML směrnice je logicky návrhem rozšiřujícím předchozí směrnice a klade si za cíl odstranit stávající mezery mezi vnitrostátními právními předpisy členských států a navíc poskytnout jasné vodítko pro budoucí směřování.

V souvislosti se vzrůstající hrozbou kybernetické kriminality a útoků na informační systémy je **zařazena na seznam trestných činů souvisejících s legalizací výnosů z trestné činnosti a financováním terorismu také „kybernetická kriminalita“.** Jde tak i o legislativní harmonizaci predikativních trestných činů praní peněz v členských státech EU.

Kromě přidání kybernetické kriminality na seznam stíhaných trestných činů nová směrnice **definuje iniciátory, facilitátory a podněcovatele trestných činů jako spolupachatele, tedy „napomáhání a navádění“ a sebe-praní bude nově také trestným činem.**

Zároveň je v rámci připravovaného AML balíčku a připravované **jednotné regulace EU v oblasti virtuálních aktiv** velký tlak na „standardizaci“ služeb spojených s virtuálními aktivy a jimi prováděnými transakcemi. **Nařízení EU o trzích s kryptoaktivy (MiCA) a nařízení EU 2023/1113 o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv.**

Nové Compliance povinnosti?

Nové technologie, technologie využívající umělé inteligence, nové platební metody, online distribuce, vývoj ve službách spojených s virtuálními aktivy, elektronická identita, identifikace na dálku, instantní poskytování služeb, směřování komunikace s klientem do on-line prostředí a absolutní automatizace služeb přináší nové výzvy s nimiž se pojí i nutnost rozšíření uvažování o možnostech zneužití nových technologií, procesů a distribucí pro legalizaci výnosů z trestné činnosti a financování terorismu.

- **Nové výzvy v oblasti KYC** - ověření, ztotožnění a autorizace klienta
- **Monitoring negativních informací z médií a veřejných zdrojů** z pohledu současných i potenciálních klientů
- **Monitoring z pohledu KYT a zohlednění kybernetického prostředí**, složitosti nových „modus operandi“ a rychlosti technologií. Využívání umělé inteligence pro vyhledávání neobvyklých vzorců chování.
- **Důsledné analýzy a zhodnocení rizik při zaváděních nových technologií** v souvislostech s interním prostředím, ale i důrazem na obecnou globální realitu, sledování nových trendů, zvažování nezamýšlených dopadů a potenciálních budoucích zranitelností.

Cyber laundering

Jednoduše pro vás

3 fáze kybernetické legalizace výnosů

1. fáze: Nezákonné finanční prostředky jsou do digitálního systému zaváděny prostřednictvím anonymních online transakcí.

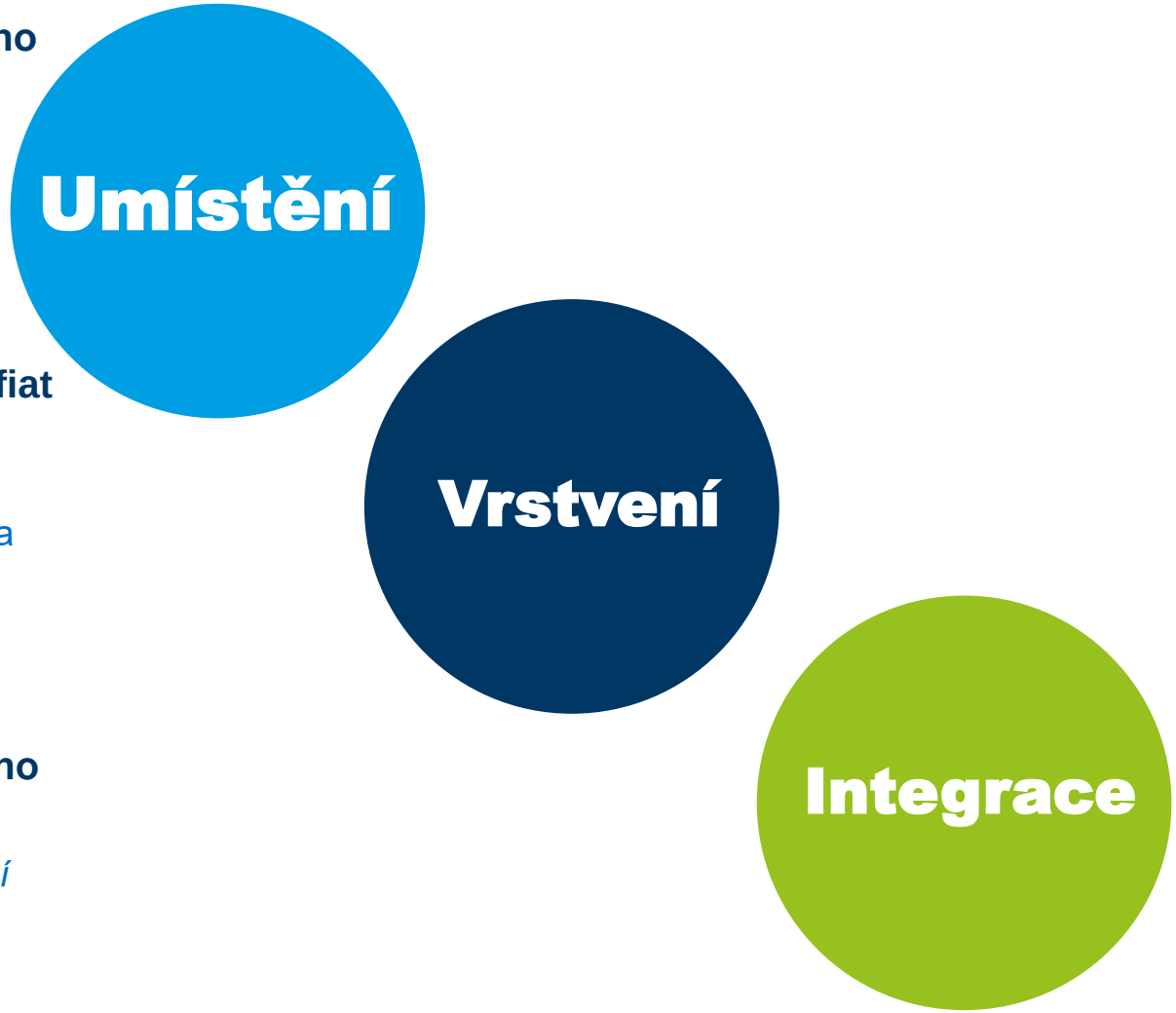
(např. online sázky, nákup on-line kreditů her, nákup virtuálních aktiv)

2. fáze: Prostředky jsou promíchávány a zamaskovány četnými transakcemi, které často přesahují jurisdikce a fiat měny.

(např. řetězec výběrů hotovosti z bankovního účtu / bankomatu a vkladů do BTCmatů, prodej herních kreditů/klíčů pro online hry na online fórech s využitím účtů pod falešnou identitou nebo blockchainových transakcí s cílovou elektronickou peněženkou v jiné zemi.)

3. fáze: Prostředky jsou vráceny do legitimního finančního systému, obvykle nákupem aktiv nebo investic.

(např. používání falešných faktur za neexistující služby, využívání fiktivních společností, výměna virtuálních aktiv za fiat měnu v zemích bez přísné regulace AML.)



ČSOB
Jednoduše pro vás

AML výzvy Kybernetického prostoru

- vysoké využití nových technologií, inovací, jejich rychlost a občas i nečekané kombinace s tradičními zdroji
- nepřipravenost regulátorů, ale i soukromých subjektů a jejich klientů na rizika spojená s technologiemi
- vysoký stupeň anonymity účastníků, často není nutné využít prostředníka
- prostředky instantně překračují hranice států či kontinentů a mění formu, kterou jsou reprezentovány
- obvykle menší finanční náročnost schématu pro pachatele a podpora profesionálními kriminálními nástroji
- velmi ztížená až nemožná dohledatelnost finančního řetězce od počátku do ukončení dokonané legalizace
- povinné osoby zapojené v řetězci transakcí vidí vždy jen část schématu, to ztěžuje detekci podezření

Aktivity zneužívané při Cyber launderingu

(typologie a techniky)

ČSOB
Jednoduše pro vás

Krádeže identity / Podvodné identity

Pachatelé se soustředí typicky na 2 oblasti:

- **Krádeže identity** např. pomocí vylákání autentizačních prostředků / průkazu totožnosti a jejich následného zneužití

Řešení s sebou nese pro pachatele riziko, že si entita, kde má být falešná identita využita, ověří zda nejsou přihlašovací údaje kompromitovány nebo zda se nejedná o odcizený průkaz totožnosti.

Vytvoření podvodné identity a to buď pomocí:

- **kompletně vytvořené podvodné identity** (data nejsou založena na datech reálné osoby/dokladu, pouze tak vypadají)
- **kombinace částečně reálných dat a falešných dat** (např. vylákané číslo průkazu, platnost a úřad, který doklad vydal)

Tato řešení s sebou nesou pro pachatele riziko, že nedojde k potvrzení při ztotožnění osoby v registru občanů.

Videohovor k ověření identity nemusí být nezbytně bezpečná cesta při využití „deep fakes“ (hlas/vzhled) a umělé inteligence ze strany pachatelů.

Opatření: ověření platnosti občanských průkazů (i v evidenci odcizených občanských průkazů), použití silných autentizačních metod, zvýšený monitoring vzdáleně identifikovaných klientů a identifikace klientů, využití technologie pro rozpoznání známek úmyslné změny předložených dokladů..

E-Commerce / POS / Payment button

Relativně novým schématem je **zneužívání obchodníků akceptujících platební karty, schémat jejich obchodních propojení či vytváření podvodných obchodníků** jako takových:

- **Falešný obchodník vytvořený od základu za účelem realizace ML/TF aktivit** či obcházení mezinárodních sankcí
- **Podvedený obchodník jako součást ML/TF schématu** z trestné činnosti či obcházení mezinárodních sankcí
- **Obchodník poskytující nelegální služby** (prodej drog, červené lucerny, apod.)
- **Falešný obchodník** jako součást modelu spolupráce s **PSP v roli prostředníka** (Payment facilitátora, agregátora platebních tlačítek) **nebo Marketplace type of merchant**.

Oblast platebních karet je částečně anonymní, a to proto, že informace o plátci nejsou přenášeny jako součást platebních informací a zahraniční vydavatelé poměrně často nespolupracují (např. ruský region).

Slabými místy pro kybernetické zneužití technologie jsou také **přenosné nebo virtuální terminály** (virtualizované v mobilních zařízeních), **virtualizace košíků v NFC gadgetech a mobilních zařízeních, platby pomocí QR kódů** (zneužívané také ke quishing), platební peněženky třetích stran a platební systémy "close loop" (např. platební řešení pro farmářské trhy, pro hudební festival apod.) se zpětnou výměnou kreditu za fiat měnu nebo možností nákupu snadno směnitelného zboží (iPhony, kredit do online her nebo herní kódy, kredit na telefonní hovory apod.).

Zmírňující opatření: Kombinace AML a sledování karetních podvodů (autorizace, transakce, kreditní transakce, obraty obchodníků), ověření skutečné existence provozovny obchodníka a zboží, sledování organizačních změn a historie klienta, vyhodnocení neobvyklých složitých obchodních modelů, zajištění nastavení účinných AML procesů u obchodních partnerů a ověření zákonných licencí pro poskytování platební služby, sledování umístění provozovny obchodníka a terminálu, IP adres atd.).

P2P platformy

Peer-to-peer platformy mohou být pro pachatele efektivním nástrojem pro zakrytí původu prostředků, určité anonymizování plátce či zdroje majetku pomocí přetržení platebního řetězce. Na druhou stranu jsou tyto platformy běžně limitované výší uskutečňovaných transakcí či jejich objemem.

Prostředky jsou typicky připsány na sběrný účet a evidovány v systému pod určitým rozlišením (např. variabilním symbolem), jsou tak vnitřně připsány na vrub konta uzavřeného platebního systému, a následně buď odeslány/vybity na jiný běžný účet než z kterého přišly, nebo jsou převedeny na jiné vnitřní konto / konta v daném systému a transakce a teprve poté pokračují vyvedením zpět do běžného bankovního prostředí seskupeny nebo rozděleny na řadu transakcí směřujících na účty, bez vztahu k původnímu plátci.

P2P platformy jsou vzhledem k obvykle limitovanému kontrolnímu prostředí, v porovnání s tradičními bankovními službami, zranitelnější pro možný cybercrime jako zdrojovou trestnou činnost pro nelegálních získání finančních prostředků.

Opatření: Transakční monitoring pracující s informací o platební službě jehož součástí je i požadavek na doložení zdroje příjmů, případně analýza plateb uživatele P2P platformy. V případě obchodního partnera v roli P2P platformy potom i ujištění se o nastavení efektivních AML procesů na jeho straně. Ověřování udělených licencí pro poskytování platební služby.

Virtual Assets

Vysoký stupeň anonymity (pseudo anonymita) **nebo úplná anonymita** (např. Dash, Monero) a zároveň globálně nedostatečně regulovaný obor podnikání (v ČR je již obor regulován v rámci AML zákona) s technickým omezením využití blockchain a technologie DLT. **Údaje o plátcích/příjemcích nejsou součástí informací na blockchain a (zatím) nedoprovází převody finančních prostředků.**

Možná z těchto důvodů jsou opakovaně světové Exchange platformy či Krypto-burzy pod hledáčkem regulátorů a často je možné najít informaci v médiích o vyšetřování daňových úniků a legalizaci výnosů z trestné činnosti např. formou poskytnutí nástroje k vyplacení výkupného z ransomware útoků. Zároveň **z pohledu technologie mohou být agilně vyvíjené systémy náchylnější k prolomení zabezpečení bezpečnostních opatření**.

Statistika Chainalysis statistic pro rok 2023 ukazuje koncentraci finančních prostředků z jednotlivých druhů trestné činnosti : Zneužívání dětí, Ransomware, Odcizené finanční prostředky, Podvodný obchodník, Darknet market a Podvod.

V roce 2023 odeslaly nelegální adresy do služeb kryptoměny v hodnotě 22,2 miliardy dolarů, což je výrazný pokles oproti 31,5 miliardy dolarů odeslaných v roce 2022. Část tohoto poklesu lze přičíst celkovému snížení objemu kryptografických transakcí, a to jak legitimních, tak nelegálních. Pokles aktivity v oblasti praní špinavých peněz byl však strmější, a to o 29,5 % ve srovnání s poklesem celkového objemu transakcí o 14,9 %.

Sofistikovanější pachatelé využívají strategii ML prostřednictvím mixérů (Tornado cash, Sinbad - oba na seznamu OFAC, YoMix) a technologie pro chain hopping prostřednictvím cross-chain bridge.

Zmírňující opatření: Sledování transakcí pracující s informací, že transakce souvisí s virtuálními aktivy. Zvýšená kontrola klienta pracující s informací z veřejné adresy peněženky v blockchainu oproti klientem doloženému důkazu původu transakce. Ověření nastavení účinných AML procesů profesionální protistrany a ověření zákonných licencí pro poskytování služeb virtuálních aktiv (pokud to vyžadují místní právní předpisy). Prověřování mezinárodních sankcí.

Vhishing, Phishing, Social engineering, Romance fraud, Search engine optimization (SEO) poisoning

Všechny tyto metody mají společné znaky – jednoduchost, nízké náklady, využití lidské nepozornosti či důvěřivosti, v některých případech přípravu na základě informací, které o sobě osoba nebo firma zveřejní a velkou účinnost i výtěžnost.

Přesto, že jsou **schémata obvykle připravované v cizině**, **neustále se zlepšuje v nich využívaná česká gramatika**. V extrémních případech se může klient „dobrodinec“ či „zamilovaný“ klient dostat do situace, že transakci vykoná přes všechny překážky mu kladené (např. vybere hotovost, kterou vloží do oběhu v zemi, kde nejsou dostatečně uplatňována AML/sankční opatření nebo využije převodů virtuálních aktiv) a může se tak dostat i do situace, kdy poruší nařízení mezinárodních sankcí.

Většina nelegálně vybraných prostředků pokračuje na jiný účet nebo přímo do blockchainu podle příběhu, který pachatelé trestné činnosti používají. **Většina modus operandi je dobře a mezinárodně organizovaná, včetně vytvoření profesionálních call center a call skriptů, schopnosti plynulé komunikace v místním jazyce, sítě peněžních mul - to vše s hlubokou znalostí role, kterou hrají proti klientovi banky.**

Zmírňující opatření: trx. monitoring velké množství transakcí na účet bez zjevného obchodního účelu, sledování negativních informací o nových "modus operandi" / hoaxech. Ověřování trx. s podezřením na podvod. Opakované vzdělávací kampaně - i když mají omezenou účinnost a někdy klient nevěří ani informacím sděleným při osobním rozhovoru s osobním bankéřem klienta. Sledování a blokování falešných webových stránek, které se vydávají za skutečné společnosti (např. falešné bankovní stránky).

Online aukce, bazarové podvody, scamy

Falešné inzeráty vyžadující platbu předem s tím, že zboží není dodáno. Účty pro platbu mohou být jumbo účty pro dobití elektronických peněženek či předplacených karet s identifikací příjemce pouze variabilním symbolem, což plátce nemusí nutně vědět. Pro vyšší obraty v rámci této podvodné činnosti jsou využívány i bílí koně či produkty sjednané na falešné identity. Prostředky poté putují z předplacené karty či elektronické peněženky v rámci hotovostních výběrů či převodů na jiné peněženky či účty řetězcem transakcí.

Typickým znakem je, že jsou prostředky na prvním médiu / peněžence / účtu uchovány po velmi krátkou dobu a tyto produkty typicky vykazují, a to i přes velký obrat, minimální průběžné zůstatky.

Opatření: Transakční monitoring – velké množství trx. na účet bez zjevného obchodního účelu, monitoring negativních informací o nových „modus operandi“ / hoaxech. Ověřování trx. s podezřením na fraud. Opakované edukativní kampaně – přesto, že mají omezenou účinnost. Vyžádání si detailní doložení dokumentace transakcí od potenciálního pachatele, bude-li komunikovat a mít snahu transakce dokládat a posouzení jejich pravosti.

Fake collections / Crowdfunding abuse

Tato oblast může mít více eventualit, kdy se může se jednat o **ekvivalent bazarových podvodů** kdy:

- **není očekávaná protihodnota** – charitativní účely (např. fiktivní sbírka na pomoc Ukrajině či pomoc neexistujícímu handicapovanému dítěti).

- **je očekávána protihodnota** - formou výhody z investice do komerčního projektu – např. fiktivní investice vydání hudební desky s tím, že existuje určitý příslib např. že všichni investoři do projektu jednu obdrží za zaváděcí (nikoliv komerční) cenu uhrazenou v rámci své investice.

Celé ML/TF schéma může být vytvořeno pouze jako falešná sbírka / crowdfunding a pachatelé mohou pouze hrát role na obou stranách, aby vytvořili fiktivní tok darů na fiktivní neexistující projekt s cílem utajit původ prostředků.

Opatření: Transakční monitoring – velké množství trx. na účet bez zjevného obchodního účelu, monitoring negativních informací o nových „modus operandi“ / hoaxech. Kontrola klienta podezřelého z organizování sbírek / crowdfundingu bez předchozího informování svého poskytovatele platebních služeb (porušení smlouvy či podezřelé jednání s cílem zastření původu prostředků). Ověření existence dokumentace sbírek či projektů a posouzení zda nejeví známky podezřelého obchodu.

Money Mules (bílí koně)
Hotovostní vklady/výběry

Přesto, že mluvíme o cybercrime či cyber-launderingu, bílí koně mají v těchto schématech také svou roli:

- **Vědomé poskytnutí své identity za úplatu** (bezdomovci, lidé v tíživé finanční situaci, exekuovaní, apod.)
- **Nevědomé poskytnutí identity** (lidé vykonávající činnost jako přivýdělek bez vědomí, že jsou součástí schématu)
- **Vědomý výkon části transakcí v rámci schématu** (přímí účastníci schématu – např. výběr hotovosti z karet odcizených v rámci phishingu, vklad hotovosti zpět do systému a jejich následné zaslání na předem určené účty)

Do této skupiny lze zařadit i klienta s nabouraným elektronickým bankovnictvím / autentizační metodou, jehož účet je využíván k převodu nelegálních finančních prostředků jako zprostředkovatelský účet. Na základě jeho chování může být stíhán pro trestný čin z nedbalosti.

Opatření: Transakční monitoring – velké množství trx. na účet bez zjevného obchodního účelu, monitoring negativních informací o nových „modus operandi“. Ověřování trx. s podezřením na fraud. Vyžádání si detailní doložení dokumentace transakcí, případně doložení „pracovní smlouvy či „brigády“ od potenciálního pachatele / bílého koně, bude-li komunikovat a mít snahu transakce dokládat a posouzení jejich pravosti. Monitoring zaměřený na neobvyklé vklady a výběry v rozporu s informacemi o klientovi. Identifikace vkladatelů hotovosti.

Bankovní převody

Bankovní převody mohou být **součástí kybernetické kriminality,** kdy jsou **kompromitovány platební údaje - typicky přihlašovací údaje nebo celé autentizační metody** (bankovní malware kombinující krádež přihlašovacích údajů a získání autentizačních SMS kódů, podvody s e-SIM, vishing, phishing nebo sociální inženýrství), **nebo mohou být metodou zastírání původu finančních prostředků z nelegální činnosti** (např. podvody s CEO) prostřednictvím řetězce převodů nebo převodů do/z zemí, kde nejsou zavedena přísná opatření proti praní špinavých peněz nebo nejsou v praxi dostatečně prosazována.

Použití okamžitých plateb výrazně zkracuje dobu pro provedení AML šetření celého schématu transakčního řetězce na řádově sekundy, maximálně několik minut.

Bankovní převod je stále jednou z nejpoužívanějších technik nelegálních převodů finančních prostředků.

Opatření: Monitorování transakcí ML/TF se zaměřením na řetězové transakce a transakce z/do vysoce rizikových třetích zemí, které se obvykle provádějí v krátkém časovém období, monitorování neobvykle velkých transakcí nebo naopak podlimitních transakcí ve velkém množství. Vyžadování podrobné dokumentace transakcí nebo zdrojů finančních prostředků. Sledování informací doprovázejících platby. Shoda jména příjemce podle údajů zaslaných v bankovním převodu (Swift) s názvem účtu příjemce registrovaného v systémech banky jako prevence podvodů s CEO.

Lehce směnitelné komodity s online či expresním dodáním

Již téměř od vzniku virtuálních aktiv se o nich mluví jako o komoditě vhodné a hojně využívané pachateli v rámci trestné činnosti a zároveň v rámci legalizace výnosů z trestné činnosti ve všech 3 fázích. Nicméně existuje více typů lehce směnitelných komodit, které jsou běžně využívány pro přerušení platebního řetězce:

- **Světově oblíbené značky elektroniky** (např. Apple, Playstation)
- **Luxusní zboží** (např. šperky, hodinky, oblečení světových značek, drahé automobily)
- **Online umělecká díla** (případně využití „Non-Fungible Token“)**, on-line kredity a herní kódy**
- **Online hazardní hry** (pachatel si může dovolit prohrát sázky s nízkým výnosem).

Opatření: Sledování řetězení transakcí, neobvykle objemných transakcí nebo naopak podlimitních transakcí ve velkém množství, trx. na účet bez zjevného obchodního účelu. Vyžadování podrobné dokumentace transakcí nebo zdroje finančních prostředků. Sledování informací doprovázejících platby. Ověření nastavení účinných AML procesů profesionální protistrany a ověření zákonných licencí pro hazardní hry.

Kombinace platebních služeb / technologií

V rámci sofistikovanějších forem cyber launderingu dochází typicky ke kombinacím, nikoliv využití pouze jedné platební služby – technologie, např.:

Prostředky získané z **bankovního malware** jsou koncentrovány na jeden **účet bílého koně**, který ihned po obdržení sms o zvýšení zůstatku na účtu **vybírá prostředky kartou v hotovosti v ATM**, **zároveň odesílá prostředky na jiný účet** instantní platbou a zbytek se může pokusit vybrat i pomocí **hotovosti fyzicky na pobočce banky**. V případě oddělení limitů výběru hotovosti a pro nákup zboží a služeb na kartě může dojít až ke zdvojnásobení vytěžení účtu platební karty pomocí výběru hotovosti a zároveň **nákupu virtuálních aktiv, dobití elektronické peněženky či předplacené karty**. Využívané produkty mohou být otevřeny na základě **falešných či ovládnutých identit**. (např. identifikace prostřednictvím peněžního převodu – hack/phishing na straně odesílatele peněžního převodu).

Kombinace kriminálních metod jsou omezeny pouze znalostmi a fantazií pachatelů.

Kyberzločinci již využívají strojové učení k identifikaci vzorů a mezer ve stávajících bezpečnostních rámcích, což jim usnadňuje proniknout do systémů bez odhalení. Finanční instituce / banky na to musí být připraveny a budovat své pokročilé kontrolní prostředí tak, aby byly schopny těmto výzvám čelit.

Opatření: Vyhodnocení rizik při přípravě nového produktu, služby, distribučního kanálu změny v procesech souvisejících s AML a jejich testování i z hlediska možného zneužití - před jejich uvedením na trh, sledování trendů v modus operandi ML/TF (v globálním prostředí se může vzorec kriminálního chování identifikovaný např. v Asii projevit v Evropě během několika týdnů, využití umělé inteligence k identifikaci neobvyklého transakčního chování napříč segmenty a definovanými shluky v klientském portfoliu.

Závěry

Jednoduše pro vás

Jak naplnit požadavky regulací

Banky / finanční instituce a další povinné subjekty v oblasti AML musí zavést programy AML/CFT založené na riziku, aby se vypořádaly s hrozbami AML/CFT, kterým čelí v důsledku kyberkriminality. V praxi to znamená:

- **Hodnocení ML/TF rizik** zákazníků, produktů, služeb, distribučních kanálů **a nastavení přiměřené reakce v AML procesech společnosti.**
- **Kontrola klienta a ověření jeho identity** musí brát v potaz možnou cyber-kriminalitu a související hrozby ML/TF.
- **Nastavení transakčního ML/TF monitoringu pomocí pokročilých technologií k detekci složitých vzorců chování** se zaměřením na transakce a produkty s vyšším stupněm anonymity.
- **Screening požadavků Mezinárodních sankcí**
- **PEP screening.** PEP jsou obecně vystaveni vyššímu riziku zapojení do kybernetické kriminality praní špinavých peněz.
- **Media monitoring negativních informací:** detekované zprávy mohou naznačovat, že zákazníci jsou či mohou být zapojeni do pokusů o praní výnosů z kybernetické kriminality.
- **Koordinace více orgánů:** Účinná protiopatření vyžadují koordinované úsilí regulačních orgánů, donucovacích orgánů a finančních institucí.

Kyberkriminalita a kybernetické praní jsou rovněž předmětem povinného hlášení regulačním orgánům.

Cyber security compliance

Dohled na splnění veškerých zákonných požadavků a povinností.

Ošetření organizace z technického hlediska i proti sofistikovaným hackerským útokům:

- Kontinuální sledování vývoje v oblasti informační a kybernetické bezpečnosti
- Pravidla bezpečného vývoje, školení zaměstnanců a průběžné testování systémů i zaměstnanců
- Proces pro řešení bezpečnostních incidentů včetně úniků dat a reportingu.

Nastavení kontinuálního a srozumitelného přístupu organizace k informační a kybernetické bezpečnosti a dohled nad dodržováním ze strany zaměstnanců.

Red flags:
FATF Risk indicators for Cyber-enabled fraud

ČSOB
Jednoduše pro vás

„Red flags“ - Transaction patterns

- Rapid or immediate, high or low value transactions after opening of an account, inconsistent with the purpose of the account
- Rapid or immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer in order to empty the account
- Frequent and large transactions, which are inconsistent with the account holder’s economic profile (e.g., sudden international transfers, withdrawals of cash performed through payment cards at foreign ATMs, large purchases of Virtual Assets or goods to be exported abroad, or payments in favor of unlicensed foreign Money Value Transfer Services)
- Transfers of funds to and from high-risk money laundering jurisdictions
- Large frequent transactions with recently established companies and/or whose main activities are not consistent with the activities carried out by the beneficiary or have a general purpose
- Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary
- Round value amount purchases that are frequent and/or in large amounts, which can indicate gift card purchases

„Red flags“- Customer transaction instructions and remarks

- A customer transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful
- A customer’s seemingly legitimate transaction instructions contain a different language vernacular, timing, and amounts than previously verified transaction instructions.
- Transaction instructions include markings, assertions, or language designating the transaction request as “Urgent”, “Secret” or “Confidential”
- A customer presents poorly formatted messages / emails (spelling and/or grammar mistakes) as justification of a transaction.
- Transaction instructions direct payment to a known beneficiary; however, the beneficiary’s account information is different from what was previously used
- The intended beneficiary in the transaction description and the name of the account holder known to the beneficiary bank are inconsistent
- Transfers ordered by natural persons (alleged investors) with no financial experience and expertise, in favor of companies (in many cases established in high-risk jurisdictions) with reasons for payments related to investments and financial products
- Counterparties incommensurate with the business/company name of the account might suggest which may provide cover for the movement of large amounts of funds internationally (e.g., the company reported as a furniture company made multiple large transfer to a company named as petroleum trading company)
- Transactions conducted with device time zone mismatch

„Red flags“- Suspicion in account holder’s profile

- Account holder is unwilling or unable to pass CDD checks
- Account holder is unfamiliar with the source of the funds moving through their account or claiming they are transacting for someone else
- Frequent changes of legal entities’/sole proprietorships’ names using foreign expressions and terminology
- The customer shows to have inadequate knowledge on the nature, object, amount or purpose of the transaction/s or relationship or provides nonrealistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting as a mule.

„Red flags“ - Suspicion in account user’s identity

- The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email)
- Frequent changes of contact details, phone numbers, email addresses after opening of the account
- E-mail addresses that do not seem compatible with the name of the account holder, or a pattern of similar email addresses seen across multiple accounts
- Irregularities in customer profile particulars, such as shared credentials (e.g., shared by two or more users) with other accounts
- Abnormalities identified via online behavior, such as hesitation inputting data, keystroke delays, signs of automation, multiple failed login attempts, etc.
- Accounts relating to entities who could be expected that they are no longer active in the jurisdiction (e.g., overseas students’ account sold when completed study) IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions
- Use of virtual private networks (VPNs), compromised devices (such as IoT devices), and hosting companies that may mask a user’s IP address
- Multiple IP addresses or electronic devices associated with a single online account
- Single static IP address or electronic device associated with multiple accounts of various account holders
- Remote desktop connection access to an account through computer ports used by applications such as TeamViewer etc. which prevents the true device and location to be seen
- Accounts operated with excessively quick keystrokes or navigation suggesting possible bot control

„Red flags“ - Adverse information on the account holder

- Presence of material relevant and verifiable negative news on customer or counterparties, e.g., account held by a known or suspected previous victim of scam, mule, or identity takeover activity
- Fraud report or recall from a correspondence institution, or other 3rd party fraud databases
- Presence of wire transfers’ recall requests
- Presence of adverse information provided by FIUs or LEAs (Law Enforcement Agencys) about persons involved in a transaction

„Red flags“- VA transactions and other

- Sending/receiving large volumes or high frequency low amounts worth of VAs to unhosted wallet addresses; or addresses associated with darknet marketplaces, child sexual abuse material platforms, cyber exploit marketplaces, ransomware groups, mixing/tumbling services, high-risk jurisdictions, gambling sites, and scammers
- Maxing out daily funding limits at Bitcoin ATMs
- No documents proving the origin of VA or of the money converted in crypto-assets
- Transfers of VAs to wallets linked to illegal activities on the dark web (e.g., terrorism, child pornography, narcotics, etc.)
- Transactions involving more than one type of VAs, particularly those that provide higher anonymity
- Abnormal transaction activity of VAs from peer-to-peer platform associated wallets with no logical business explanation

„Red flags“ - Other

- Mismatch of account number and name of the holder of the account
- The user is seen on the phone or accompanied by an individual through Closed Circuit Television (CCTV) and being instructed or coached during the transaction
- Beneficiary companies manage Internet Web Sites providing trading/investment services, in many cases not authorized or listed by the domestic Supervisory Authority

Zajímavé zdroje

ČSOB
Jednoduše pro vás

Zdroje:

European Commission: Anti-money laundering and countering the financing of terrorism legislative package

The EU Cybersecurity strategy

Europol: European Cybercrime Centre – EC3: Internet organized crime threat assessment

The Financial Action Task Force (FATF): Opportunities and challenges of new technologies for AML/CTF

Illicit Financial Flows from Cyber-Enabled Fraud (November 2023)

European Commission: Council of Europe Convention on Cybercrime

Moneyval: Research report: Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction

Other sources :

- University of Bialystock, Poland: Wojciech Filipkowski – Cyber laundering: An Analysis of Typology and Techniques
- Tallinn university of technology, Estonia – Zaghum Wahab Awan- Analytical comprehensive approach to cyber laundering and its solutions
- Nyman Gibson Miralis : Cyber laundering: What are some key challenges in detection and regulation?
- Eurasian Group on Combating Money Laundering and Financing of Terrorism : Typology Project - Cybercrime and Money Laundering
- Chainalysis . Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group

Thank you for your attention

Lukáš Poznar

Compliance advisor – Prevence praní peněz a podvodů

Československá obchodní banka, a. s.