Licenčné požiadavky

na IT systémy, analytické nástroje a úschovu aktív

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

Peter Hidasy, Boris Suchovský

Bratislava 9.4.2024

Obsah

- Technologické riešenia CASPov
- Analytické nástroje
- Úschova kryptoaktív klientov
- Peňaženky na správu prostriedkov
- API pre prístup k finančným údajom (FIDA)
- Súlad s DORA
- DORA Workshop v NBS
- Prílohy k žiadosti o povolenie

Technologické riešenia

- Proporcionalita
  - Požiadavky závisia od rozsahu poskytovaných služieb podľa MiCA
- Cloudové služby a interné serverové riešenia
  - Vysoká dostupnosť a odolnosť voči výpadkom
  - Garancia rýchlej obnovy po výpadkoch
  - Business continuity plán
- Bezpečnostné riešenia ochrany pred kybernetickými hrozbami
  - Pokročilé firewall systémy
  - Detekcia a prevencia prienikov do systémov
  - Šifrovanie dát
  - Pravidelný bezpečnostný audit
  - Schopnosť prispôsobiť sa novým hrozbám a vývoju v oblasti cybersecurity

Technologické riešenia

- Nástroj na identifikáciu klienta
  - Zabezpečiť KYC (know your customer)
  - Kontrola živosti klienta (liveness check)
  - Kontrola politicky exponovaných osôb (PEP)
- Nástroj na zabezpečenie súladu s TFR
  - Riešenie by v predmetných prípadoch malo zabezpečiť, aby prevody prostriedkov boli sprevádzané údajmi požadovanými podľa TFR
- Klientské aplikácie
  - Intuitívne a užívateľsky prívetivé rozhrania
  - Použitie bezpečných a šifrovaných protokolov na prenos dát, ako sú SSL/TLS, na zabezpečenie dátových prenosov medzi klientom a serverom

Technologické riešenia

- Nástroj na skríning rizík AML
  - Due-diligence klienta (CDD)
  - Monitoring obchodných aktivít klienta
  - Zahŕňa sankčné a PEP zoznamy
- Nástroj na analýzu blockchainu
  - Podrobná analýza transakcií na blockchaine
  - Upozorniť na prebiehajúce AML riziko (monitoring)
  - Vyhodnotiť rizikovosť peňaženky protistrany (klienta)

Analytické nástroje

Služby

- Vyhodnotenie rizikovosti klienta, vlastný,
- Vypracovaný **systém hodnotenia rizík protistrán**, prehľadnosť, farebná škála/ bodové skóre, s možnosťou úpravy, riziko priame/nepriame
- Adresám priradený názov (zistenie pôvodu kryptoaktív), Clustering adries
- **Sankčné zoznamy** zahrnuté, OSINT informácie
- Školenia pre zamestnancov a osoby zodpovedné za AML, aj so skúškou/ certifikátom
- Investigácia transakcií, prehľadné grafické znázornenie
- Nepretržité **monitorovanie transakcií**
- Možnosť exportu údajov, integrácia API

Výber analytického nástroja

- Testovanie, porovnanie
- Množina pokrytých kryptoaktív, DeFI
- Rýchlosť odozvy (aktualizácia údajov, podpora, nové funkcie)

Úschova kryptoaktív klientov

- MiCA čl. 75 ods. 7
- Návrh zákona o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív
- CASP oddeľuje vlastné kryptoaktíva od klientových
- Klientové kryptoaktíva sú právne oddelené od majetku CASPov
- Kryptoaktíva sú **prevádzkovo oddelené od majetku poskytovateľa** služieb kryptoaktív.

Peňaženky na správu prostriedkov

- Schopnosť spravovať viaceré kryptoaktíva
- Hardvérová bezpečnosť
- Efektívna správa kľúčov
- Viacúrovňová autentifikácia
- Multisig politiky – navrhnúť vhodné riešenie
- Príklad autorizačného flowu:
  - V multisigu 3 z 5 junior operátor iniciuje transakciu
  - Druhý junior operátor skontroluje a potvrdí správnosť transakcie
  - Senior operátor vykoná presun prostriedkov
- Zníženie rizika krádeže – jedna osoba nemá možnosť vykonať transakciu

Zasielanie prostriedkov klientovi

- Whitelisting klientových adries
- Možnosť zaslať prostriedky iba na predschválenú adresu klientom
- Ak je klientov účet ohrozený, útočník vie zaslať prostriedky iba na klientovu adresu
- Travel rule guideline (draft)

Samohostované peňaženky

V prípade, že suma prevodu **prevyšuje 1000 EUR** z alebo na samohostovanú adresu, mal by CASP odosielateľa a CASP príjemcu overiť, či samohostovanú adresu vlastní alebo kontroluje odosielateľ a príjemca, pomocou vhodných technických prostriedkov, ktoré zahŕňajú jedno alebo viac z nasledujúceho:

- pokročilé analytické nástroje,
- overenie identifikácie bez fyzickej prítomnosti ako je špecifikované v "Usmerneniach k použitiu riešení pre onboarding klientov na diaľku v zmysle článku 13 ods. 1 Smernice (EU) 2015/849" so zobrazením adresy,
- overenie identifikácie za fyzickej prítomnosti ako je špecifikované v "Usmerneniach k použitiu riešení pre onboarding klientov na diaľku v zmysle článku 13 ods. 1 Smernice (EU) 2015/849„
- odoslanie preddefinovanej sumy (najlepšie najmenšej menovitej jednotky daného kryptoaktíva), stanovenej CASPom, z a na samohostovanú adresu na účet CASPa,
- vyzvať zákazníka, aby digitálne **podpísal konkrétnu správu** privátnym kľúčom korešpondujúcim k adrese,
- iné vhodné technické prostriedky.

Zdroje:
Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1113 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849
Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ('The Travel Rule Guidelines')

Budúcnosť: API pre prístup k finančným údajom

- Návrh FIDA (Financial data access) pre open finance
- Zdieľanie vybranej kategórie finančných údajov klientov prostredníctvom technických rozhraní a schémy zdieľania finančných údajov
- V schéme zdieľania budú vystupovať držitelia údajov (CASP, banka) a používatelia údajov (fin. sprostredkovateľ)
- Rozhranie pre klienta, aby mohol manažovať prístupy tretích strán k jeho údajom
- Horizont 2 – 3 rokov

Súlad s DORA

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora (DORA)
- Slovenský finančný trh a inovácie 2023 – prezentácia DORA
- Čo očakávať od digitálnej prevádzkovej odolnosti DORA? (3.10.2023)
- DORA na webe NBS
- Uplatňuje sa od 17.1.2025

Oblasti DORA

- Riadenie IKT rizika
- Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT
- Testovanie digitálnej prevádzkovej odolnosti
- Riadenie rizika IKT tretích strán
- Zdieľanie informácií

DORA Workshop v NBS

- Špecializovaný workshop v NBS v júni
- NBS kontaktuje trh s bližšími informáciami o podujatí
- Vhodné je si naštudovať doterajšie predpisy, prezentácie
- Vopred si pripraviť otázky, nejasnosti a zaslať
- Obsahom budú podrobne rozobraté aktuálne aj pripravované vykonávacie predpisy

Prílohy k žiadosti (Príloha č. 9)

- Žiadateľ musí preukázať súlad so všetkými ustanoveniami DORA
- Technická dokumentácia k:
  - IKT systémom (opis IT systémov - architektúra, sieťové prvky...)
  - DLT infraštruktúre (ak na nej IKT systémy závisia)
  - bezpečnostným opatreniam
  - použitým IKT politikám (bezpečnostná politika - autentifikácia klienta, politika hesiel...)
  - procedúram/systémom/protokolom/nástrojom/ľudským zdrojom na zabezpečenie súladu s DORA
  - výstupom z auditov/testov IKT systémov vykonaných tretími stranami v posledných 3 rokoch vrátane kontroly zdrojového kódu smart kontraktov žiadateľa
- Opis v netechnickom jazyku ku všetkým náležitostiam v bodoch vyššie

Prílohy k žiadosti - postupy a politiky

- plán testovania pre IKT bezpečnosť
- politika pre kontrolu prístupu
- politika pre IKT business kontinuitu
- politika pre IKT incidenty
- politika pre informačnú bezpečnosť v kontexte IKT RMF
- politika pre riadenie IKT aktív
- politika pre riadenie IKT projektov
- politika pre šifrovanie a kryptografické overovanie
- politika pre získavanie, vývoj a udržiavanie IKT systémov
- politiku pre fyzickú a environmentálnu bezpečnosť

Prílohy k žiadosti - postupy a politiky

- politiky a postupy na riadenie IKT operácií pre IKT aktíva
- politiky a postupy pre manažment identít
- politiky a postupy pre riadenie IKT rizík
- postup pre riadenie IKT aktív
- postup pre riadenie IKT projektov
- postup pre riadenie IKT zmien
- postup pre riadenie nadobúdania, vývoja a údržby IKT systémov
- postup pre riadenie opráv (patch-ov)
- postup pre riadenie zdrojov a výkonnosti

Prílohy k žiadosti - postupy a politiky

- postup pre zabezpečenie údajov a IKT systému
- postup pre získavanie, vývoj a udržiavanie IKT systémov
- postupy na ochranu informácií pri prenose
- postupy pre kontrolu logického a fyzického prístupu
- postupy pre riadenie bezpečnosti siete
- postupy pre riadenie zraniteľností
- postupy pre zálohovanie
- postupy, protokoly a nástroje pre logovanie
- register pre certifikáty a úložiská certifikátov

Najčastejšie nedostatky v podkladoch

- Dodať kompletnú dokumentáciu
- Personálne zabezpečenie – zmluva o budúcej zmluve/pracovná zmluva
- Zabezpečiť priestory – budúca zmluva o prenájme
- Zabezpečiť infraštruktúru – budúca zmluva s poskytovateľom

Ďakujeme za pozornosť.

crypto@nbs.sk

Kryptoweb NBS