DORA

článok 20

Reporting IKT incidentov

RTS - obsah a lehoty

ITS - formuláre, vzory a postupy

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

Juraj Kubík, OFI

11.12.2024

Agenda

- RTS/ITS a nariadenie DORA
- Predmet RTS a ITS
- Nahlasovanie závažného IKT incidentu, lehoty
  - Všeobecné informácie, počiatočné oznámenie, priebežná a záverečná správa
- Oznamovanie významnej kybernetickej hrozby
- Outsourcing reportingu
- Agregovaný reporting
- Technické riešenie
- GL o odhade súhrnných ročných nákladov a strát
- Ďalšie informácie

RTS/ITS a nariadenie DORA

DORA čl. 17-23:

- FEs vymedzia, zavedú a vykonávajú proces riadenia IKT incidentov s cieľom odhaľovať, riadiť a oznamovať IKT incidenty
- FEs zaznamenávajú všetky IKT incidenty a významné kybernetické hrozby
- FEs ich klasifikujú na základe kritérií
- FEs nahlasujú závažné IKT incidenty do CA
- FEs na dobrovoľnej báze oznamujú významné kybernetické hrozby CA
- ESAs po konzultácii s ENISA a ECB vypracujú RTS/ITS k reportingu
- ESAs po konzultácii s ECB a ENISA vypracujú spoločnú správu o uskutočniteľnosti ďalšej centralizácie nahlasovania závažných incidentov od FEs

Predmet RTS a ITS

- RTS
  - obsah hlásení závažných IKT incidentov
  - lehoty pre počiatočné oznámenie, priebežnú správu a záverečnú správu
  - obsah oznámenia o významných kybernetických hrozbách

- ITS
  - štandardné formuláre, vzory a postupy

- RTS/ITS úzko súvisia s RTS o klasifikácii IKT incidentov (DORA workshop k 1.balíku)

Nahlasovanie závažného IKT incidentu

- harmonizovaný, jednotný prístup bez ohľadu na sektor
- FEs vypĺňajú vzor uvedený v prílohe I podľa data glossary a pokynov v prílohe II

  - Všeobecné informácie
  - Počiatočné oznámenie
  - Priebežná správa
  - Záverečná správa

Report	Mandatory fields	Conditional fields
Initial notification	~~9~~ => 7	~~8~~ => 3
Intermediate report	~~16~~ => 14	~~24~~ => 21
Final report	~~12~~ => 7	~~15~~ => 7
TOTAL	**~~37~~ => 28**	**~~47~~ => 31**

Zdroj: ESAs

zmeny po konzultácii:

- zefektívnenie obsahu vzoru nahlasovania
- zníženie počtu reportovaných polí z 84 na 59
- zjednodušenie initial notification - zo 17 na 10 polí, z nich len 7 povinných
- predĺženie lehôt priebežnej a záverečnej správy
- nahlasovanie počas víkendov a sviatkov
- zavedenie agregovaného reportingu na národnej úrovni pre FEs dohliadané rovnakou CA

Všeobecné informácie

- Typ hlásenia
- Informácie o predkladateľovi - názov, identifikačný kód
- Informácie o ovplyvnenom FE - typ, názov, identifikátor
- Údaje o ďalších FEs, pokiaľ ide o agregovaný reporting
- Údaje o kontaktných osobách (meno, email, telefón)
- Názov hlavného materského podniku skupiny
- Mena vykazovania

Počiatočné oznámenie

- Referenčný kód incidentu pridelený FE
- Dátum a čas detekcie, dátum a čas klasifikácie incidentu
- Opis závažného IKT incidentu
- Kritériá, pre ktoré FE klasifikoval IKT incident ako závažný
- Thresholdy kritéria Geografické rozloženie (dotknuté členské štáty)
- Informácie o tom, ako bol závažný IKT incident zistený a o jeho pôvode
- Informácie, či FE aktivoval plán kontinuity činností
- Ďalšie relevantné informácie (napr. reklasifikácia IKT incidentu zo závažného na nezávažný)

Priebežná správa

- Referenčný kód incidentu pridelený CA
- Dátum a čas výskytu závažného IKT incidentu
- Dátum a čas obnovy pravidelných činností FE
- Splnené klasifikačné kritériá (počty, percentá, hodnoty)
- Typ závažného IKT incidentu
- Použité hrozby a techniky
- Dotknuté funkčné oblasti a obchodné procesy
- Vplyv na finančné záujmy klientov
- Informácie o nahlásení závažného IKT incidentu iným orgánom
- Dočasné kroky alebo opatrenia, ktoré FE prijal alebo plánuje prijať
- Informácie o indikátoroch ohrozenia

Záverečná správa

- Informácie o hlavných príčinách incidentu, viacúrovňová klasifikácia
- Informácie o riešení incidentu
- Dátum a čas riešenia hlavnej príčiny
- Dátum a čas vyriešenia incidentu
- Informácie relevantné pre orgány pre riešenie krízových situácií
- Informácie o nákladoch a stratách
- Informácie o opakujúcich sa nezávažných incidentoch
- Dátum a čas výskytu opakujúcich sa incidentov

Lehoty

- Počiatočné oznámenie (initial notification)
  - do 4 hodín od klasifikácie IKT incidentu ako závažného
  - najneskôr do 24 hodín od detekcie incidentu

- Priebežná správa (intermediate report)
  - najneskôr do 72 hodín od predloženia počiatočného oznámenia, a to aj v prípade, že sa stav alebo spôsob riešenia nezmenil
  - aktualizovaná po obnovení pravidelných činností

- Záverečná správa (final report)
  - najneskôr 1 mesiac po predložení poslednej (aj aktualizovanej) priebežnej správy

- ak FEs nie sú schopné predložiť hlásenie, bezodkladne (v rámci lehôt) informujú CA (aj o dôvodoch)
- zohľadnený víkend/sviatok - reporting do 12:00 nasledujúceho pracovného dňa
  - neuplatňuje sa na počiatočné oznámenie alebo priebežnú správu za:
    - banky, centrálne protistrany, obchodné miesta
    - FEs identifikované ako kľúčové alebo dôležité subjekty podľa NIS2
    - FEs, ktoré sú významné alebo majú systémový charakter (môže ich určiť CA)

Oznamovanie významnej kybernetickej hrozby

- na dobrovoľnej báze
- FEs vypĺňajú vzor v prílohe III podľa data glossary a pokynov v prílohe IV

  - Všeobecné informácie
  - Dátum a čas detekcie hrozby
  - Opis hrozby
  - Informácie o potenciálnom vplyve hrozby
  - Splnené klasifikačné kritériá, ak by sa hrozba materializovala
  - Stav hrozby a zmeny v jej aktivite
  - Opatrenia prijaté s cieľom zabrániť materializácii hrozby
  - Informácie o oznámení hrozby iným FE alebo orgánom
  - Informácie o indikátoroch ohrozenia
  - Ďalšie relevantné informácie

Outsourcing reportingu

DORA čl. 19(5):

- FEs môžu zveriť nahlasovacie povinnosti tretej strane formou outsourcingu
- FEs sú plne zodpovedné za plnenie požiadaviek na nahlasovanie incidentov

ITS (outsourcing nahlasovacích povinností):

- FEs o outsourcingu nahlasovania vopred informujú CA hneď po uzavretí dohody o outsourcingu, najneskôr pred prvým nahlasovaním
- FEs poskytnú CA názov, kontaktné údaje a identifikačný kód tretej strany, ktorá za ne bude predkladať hlásenia
- FEs informuju CA aj o ukončení dohody o outsourcingu

Agregovaný reporting

ITS (agregovaný reporting):

- tretia strana, na ktorú FEs outsourcujú nahlasovacie povinnosti, môže poskytnúť agregované informácie o závažnom IKT incidente, ktorý má vplyv na viacero FEs, v jednom oznámení/správe v mene všetkých ovplyvnených FEs
- na vnútroštátnej úrovni pre FEs, nad ktorými vykonáva dohľad tá istá CA
- zapodmienkovaný, všetky podmienky musia byť splnené súčasne

- neuplatňuje sa na významné banky, obchodné miesta a centrálne protistrany (reportujú len individuálne)
- platí, že CA si môže od FE vyžiadať separátne individuálne hlásenie

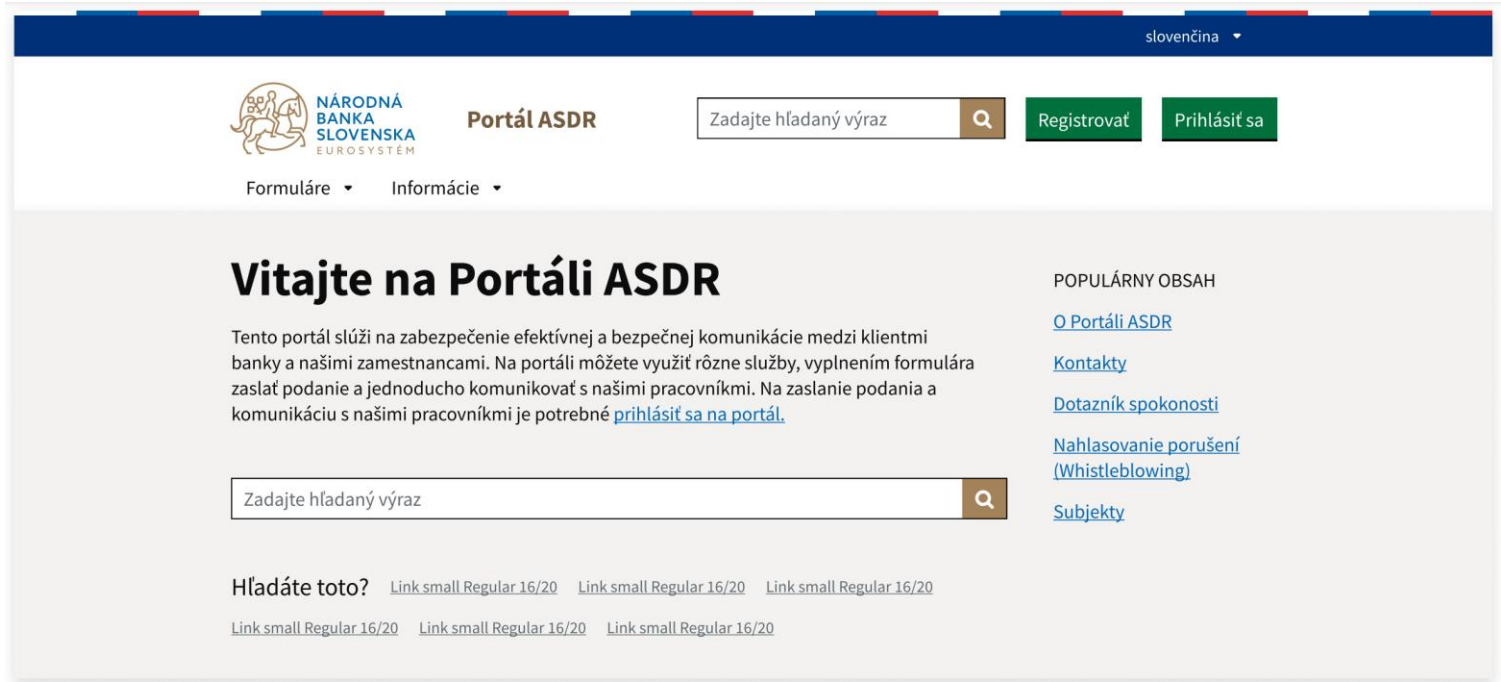
Technické riešenie

ITS (zabezpečené elektronické kanály, ktoré sprístupní CA):

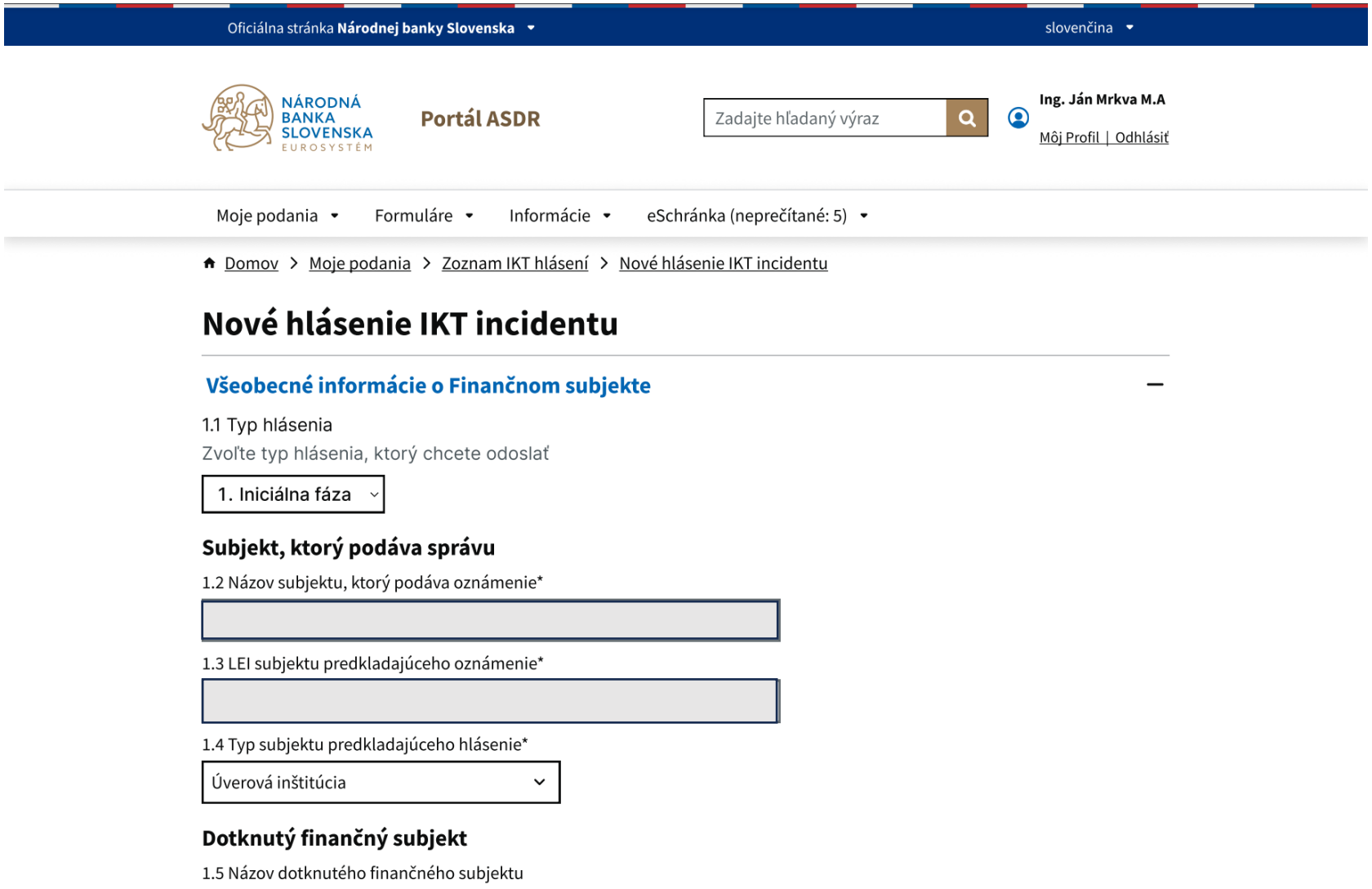
- NBS plánuje na zber závažných IKT incidentov a významných kybernetických hrozieb použiť **novovytvárané portálové riešenie**
  - webový formulár, XLSX file upload, API
  - testovacie a produkčné prostredie
  - formát XLSX, (JSON)
- aktuálny stav - interné testovanie

- alternatívny kanál - dedikovaná emailová schránka

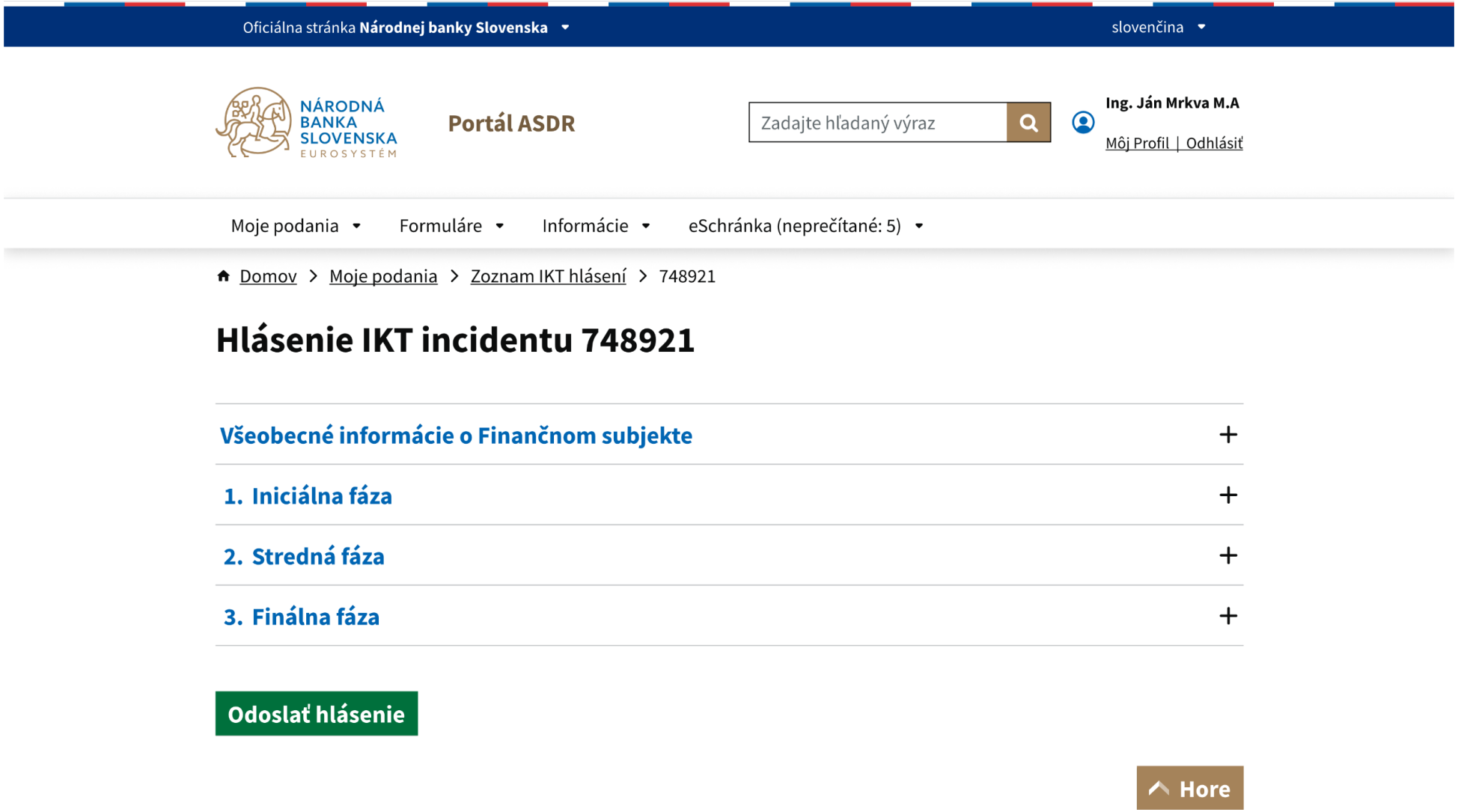
Technické riešenie - screenshots



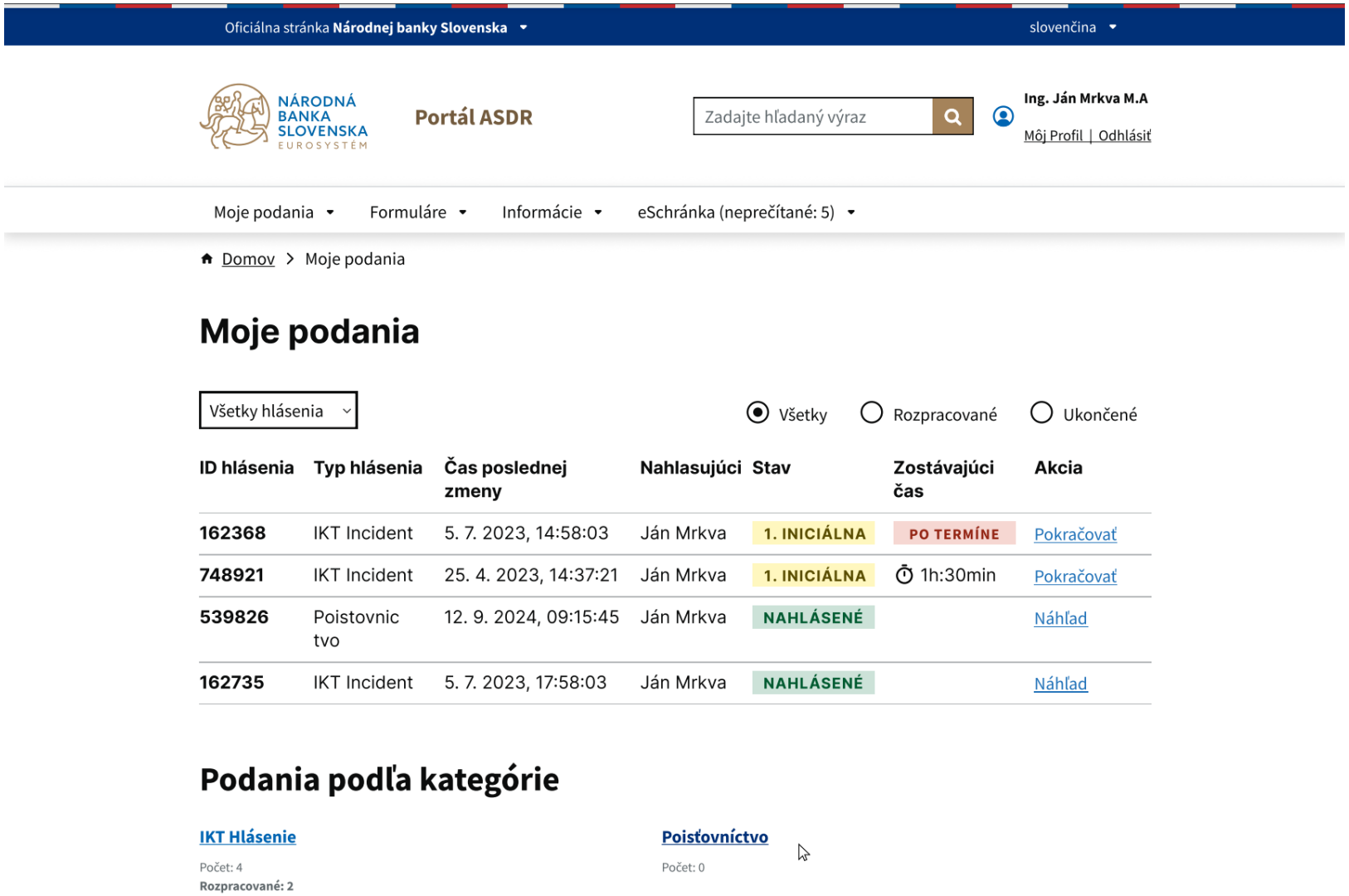
Technické riešenie - screenshots



Technické riešenie - screenshots



Technické riešenie - screenshots



Technické riešenie - dočasné

- **dočasné riešenie**
  - voľná príloha
  - nahlasovanie cez ŠZP - výkaz dor_01
  - formát XLSX

- alternatívny kanál - dedikovaná emailová schránka

Technické riešenie - vzor XLSX

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

General information about the financial entity														Content of the initial notification		
1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9	1.10	1,11	1.12	1,13	1.14	1,15	2.1	2.2	2.3
Name of the entity submitting the report	Identification code of the entity submitting the report	Type of the affected financial entity	Name of the financial entity affected	LEI code of the financial entity affected	Primary contact person name	Primary contact person email	Primary contact person telephone	Second contact person name	Second contact person email	Second contact person telephone	Name of the ultimate parent undertaking	LEI code of the ultimate parent undertaking	Reporting currency	Incident reference code assigned by the financial entity	Date and time of detection of the ICT-related incident	Date and time of classification of the incident as major

Content of the intermediate report														
3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11	3.12	3.13	3.14	3.15
Incident reference code provided by the competent authority	Date and time of occurrence of the incident	Date and time when services, activities or operations have been recovered	Number of clients affected	Percentage of clients affected	Number of financial counterparts affected	Percentage of financial counterparts affected	Impact on relevant clients or financial counterparts	Number of affected transactions	Percentage of affected transactions	Value of affected transactions	Information on whether the numbers are actual or estimates, or whether there has not been any impact	Reputational impact	Contextual information about the reputational impact	Duration of the major ICT-related incident

Content of the final report					
4.1	4.2	4.3	4.4	4.5	4.6
High-level classification of root causes of the incident	Detailed classification of root causes of the incident	Additional classification of root causes of the incident	Other types of root cause types	Information about the root causes of the incident	Incident resolution

Reporting instructions | Type of submission | Initial notification | Intermediate report | **Final report** | List reference

Technické riešenie - vzor XLSX

- vybrané detaily
  - dátové polia - povinné (Yes), podmienené (Yes, if), nepovinné (No)
  - aktualizácia predchádzajúcich hlásení
  - kombinácia viacerých typov hlásení
  - agregovaný reporting (in case of aggregated reporting...)
  - reklasifikácia závažného na nezávažný IKT incident
  - opakujúce sa incidenty

4.15	4.16
Information on whether the non-major incidents have been recurring	Date and time of occurrence of recurring incidents

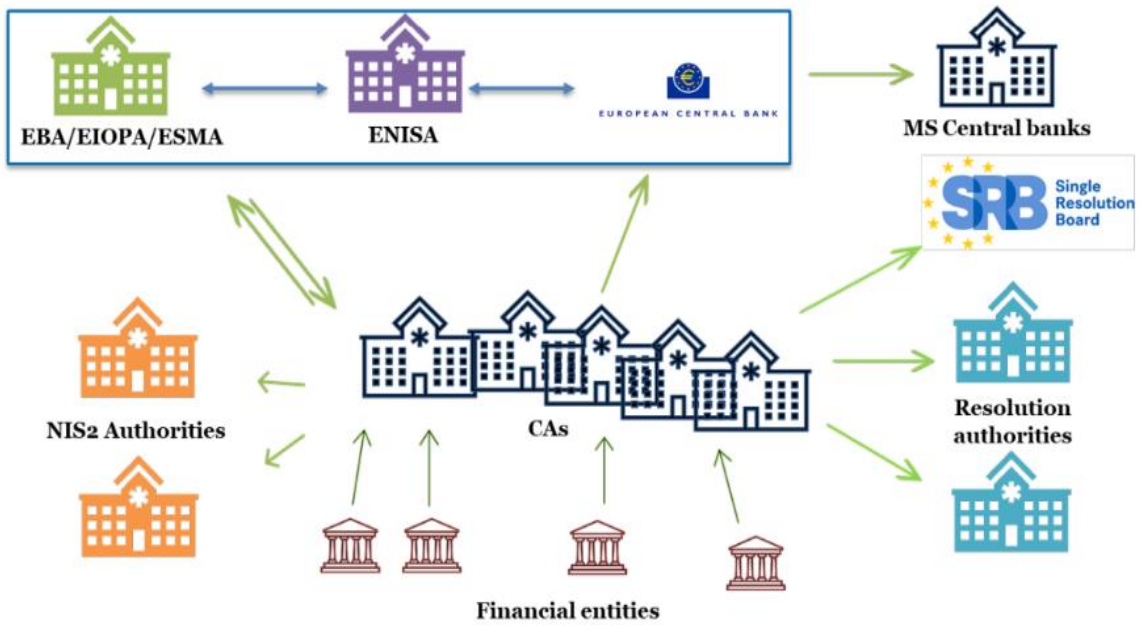
General information about the financial entity
1,1
Type of submission
Major incident reclassified as non-major
Initial notification
Intermediate report
Final report
Major incident reclassified as non-major

- dátové typy
  - alphanumeric, numerical integer, percentage, monetary
  - choice, multiselect
  - ISO standards
  - boolean Yes/No

- validačné pravidlá
  - Blocking, Warning, zapracované chybové hlášky

EÚ zber a distribúcia hlásení

- NBS ⟶ ESAs cez upravený CIRAS (systém ENISA)
- NBS ⟶ ECB



Zdroj: ESAs

- interim riešenie (ad-hoc tool)
- long-term riešenie (tool predbežne v apríli 2025)

GL o odhade súhrnných ročných nákladov a strát

DORA čl. 11(10,11):

- FEs iné ako mikropodniky oznamujú CAs na ich žiadosť odhad súhrnných ročných nákladov a strát spôsobených závažnými IKT incidentmi

- odhady ročných costs & losses aj financial recoveries za:

  - závažné IKT incidenty, za ktoré FE predložil záverečnú správu v príslušnom referenčnom roku
  - závažné IKT incidenty z predchádzajúcich referenčných rokov, ktoré mali kvantifikovateľný finančný vplyv na FE v príslušnom referenčnom roku

- podľa vzoru jednotlivo pre každý závažný IKT incident aj súhrnne za príslušný referenčný rok

4.13	4.14
Amount of gross direct and indirect costs and losses	Amount of financial recoveries

Ďalšie informácie

- od 17.1.2025 národný reporting pre všetky FEs v scope DORA
  - výkaz dor_01 v ŠZP ako dočasné riešenie
  - pripravovaný portál - testovanie aj za účasti FEs, migrácia zo ŠZP
- omeškanie RTS/ITS k reporting IKT incidentov
- v závislosti od zverejnenia týchto RTS/ITS aj GL on costs and losses
- do 17.1.2025 ESAs v spolupráci s ECB a ENISA predložia feasibility study k centralizácii nahlasovania incidentov pomocou single EU Hub

Ďakujem za pozornosť