DORA

Kapitola III, čl. 18(3)

Klasifikácia IKT incidentov

RTS/Delegované nariadenie

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

Juraj Kubík, OFI

19. jún 2024

RTS o klasifikácii IKT incidentov

- Kontext RTS s nariadením DORA
- Ciele RTS
- Predmet RTS
- Klasifikácia - kritériá, thresholdy
  - IKT incident, závažný IKT incident
  - Povinné kritérium, ďalšie kritériá
  - Opakujúce sa incidenty
  - Významná kybernetická hrozba
- Relevantnosť závažných IKT incidentov pre CAs v iných členských štátoch
- Ďalší príjemcovia údajov o závažnom IKT incidente
- Technické riešenie ESAs, ECB, NBS
- Q&As

Kontext RTS s nariadením DORA

DORA kapitola III, 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 reportujú závažné IKT incidenty do CA
- FEs na dobrovoľnej báze reportujú významné kybernetické hrozby do CA
- CA potvrdí prijatie a včas poskytne podrobné údaje o závažnom IKT incidente ďalším príjemcom
- ESAs a ECB po konzultácii s ENISA a v spolupráci s CA posúdia cross-border vplyv a informujú relevantné CAs v iných členských štátoch, ECB informuje členov ESCB

Ciele RTS

- klasifikácia IKT incidentov má byť jednoduchá, konzistentná a plne harmonizovaná
- inšpirovať sa doteraz existujúcimi klasifikáciami incidentov a zladiť sa s nimi
- cez klasifikačné kritériá a thresholdy zachytiť relevantné IKT incidenty bez overreportingu
- konzistentný one-size-fits-all prístup pre všetky FEs bez sektorových špecifík
- FEs sa majú sústrediť na handling incidentov a nebyť nadmerne zaťažované klasifikáciou

Predmet RTS

- klasifikačné kritériá pre závažné IKT incidenty
- thresholdy pre závažné IKT incidenty
- kritériá a thresholdy pre významné kybernetické hrozby
- kritériá relevantnosti IKT incidentov pre CA v iných členských štátoch
- aké údaje o závažnom IKT incidente CA poskytne iným autoritám

FEs

CAs

IKT incident

- **IKT incident** je jedna udalosť alebo séria prepojených udalostí, ktoré FE neplánovala a ktoré narúšajú bezpečnosť sietí a informačných systémov a majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo na služby, ktoré FE poskytuje

- incidenty podľa **PSD2**
  - pre subjekty v rozsahu pôsobnosti DORA, t.j. banky, PI, AISP a EMI, sa od 17.1.2025 prestanú uplatňovať požiadavky na nahlasovanie incidentov podľa PSD2, a budú reportovať **prevádzkové alebo bezpečnostné incidenty súvisiace s platbami** bez ohľadu na to, či takéto incidenty súvisia s IKT alebo nie, podľa DORA
- incidenty podľa **NIS2**
  - DORA predstavuje **lex specialis** vo vzťahu k smernici NIS2 pre finančný sektor (banky, obchodné miesta a centrálne protistrany)

Závažný IKT incident

FE klasifikuje IKT incident ako **závažný**, ak je splnené **povinné kritérium „Kritickosť ovplyvnených služieb“**

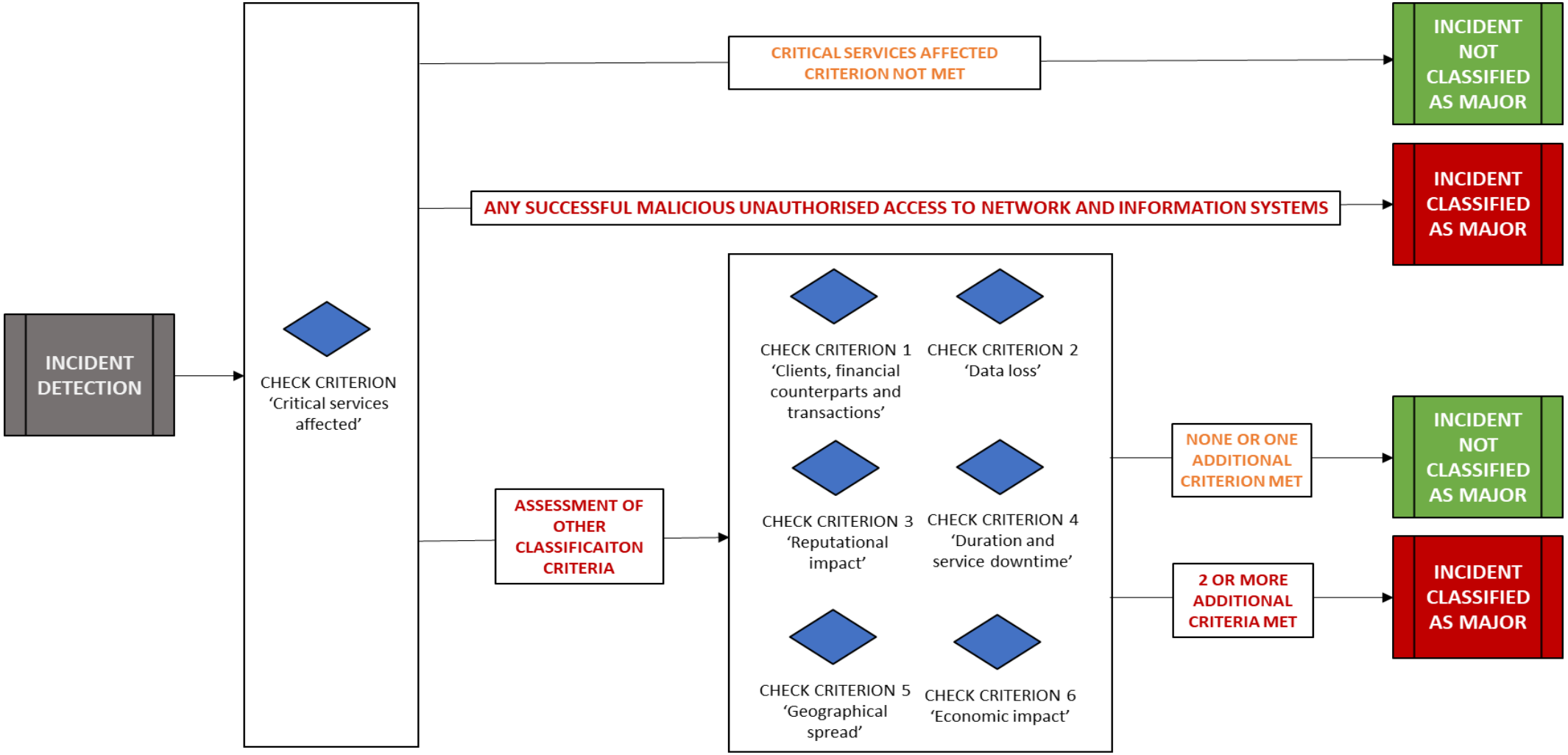
a

a) ak dôjde k **úspešnému škodlivému a neoprávnenému prístupu do sietí a informačných systémov**, ktorý môže mať za následok stratu údajov

alebo

b) ak sú splnené **akékoľvek 2 zo 6 ďalších kritérií**

Závažný IKT incident



Zdroj: ESAs

Povinné kritérium - Kritickosť ovplyvnených služieb

Thresholdy:

FE vyhodnotí vplyv na kritickosť ovplyvnených služieb, t.j. či:

- incident ovplyvňuje alebo ovplyvnil IKT služby alebo siete a informačné systémy, ktoré podporujú CIF FE alebo
- incident ovplyvňuje alebo ovplyvnil finančné služby, ktoré si vyžadujú povolenie, registráciu alebo ktoré sú predmetom dohľadu CAs alebo
- incident predstavuje alebo predstavoval úspešný, škodlivý a neoprávnený prístup k sieťam a informačným systémom FE

Ďalšie kritériá

- **Klienti, finančné protistrany a transakcie**
- **Vplyv na dobré meno**
- **Trvanie a výpadok služby**
- **Geografické rozloženie**
- **Straty údajov**
- **Hospodársky vplyv**

Ďalšie kritériá - Klienti, finančné protistrany a transakcie

Thresholdy:

a) >10% všetkých klientov využívajúcich ovplyvnenú službu alebo

b) >100 000 klientov využívajúcich ovplyvnenú službu alebo

c) >30% finančných protistrán v súvislosti s ovplyvnenou službou alebo

d) >10% denného priemerného počtu transakcií vykonaných FE v súvislosti s ovplyvnenou službou alebo

e) >10% dennej priemernej hodnoty transakcií vykonaných FE v súvislosti s ovplyvnenou službou alebo

f) vplyv na relevantných klientov alebo relevantné finančné protistrany

Ďalšie kritériá - Vplyv na dobré meno

Thresholdy:

FE zváži úroveň viditeľnosti, ktorú incident získal alebo pravdepodobne získa vo vzťahu k uvedeným:

a) incident sa objavil v médiách alebo
b) FE obdržala opakované sťažnosti od rôznych klientov alebo finančných protistrán alebo
c) FE nebude schopná alebo pravdepodobne nebude schopná plniť regulačné požiadavky alebo
d) FE stratí alebo pravdepodobne stratí klientov alebo finančné protistrany, čo bude mať významný vplyv na jej obchodnú činnosť

Ďalšie kritériá - Trvanie a výpadok služby

Thresholdy:

FE odmeria trvanie incidentu a výpadku služby v dôsledku incidentu

a) incident trvá dlhšie ako 24 hodín alebo
b) výpadok služby je dlhší ako 2 hodiny pre IKT služby podporujúce CIF

Ďalšie kritériá - Geografické rozloženie

Thresholdy:

FE vyhodnotí vplyv na územiach aspoň 2 členských štátov, najmä jeho významnosť vo vzťahu k:

a) klientom a finančným protistranám v iných členských štátoch alebo

b) pobočkám FE alebo iným FEs v rámci skupiny, ktoré vykonávajú činnosti v iných členských štátoch alebo

c) infraštruktúram finančného trhu alebo tretím stranám, čo potenciálne môže ovplyvniť FEs v iných členských štátoch, ktorým poskytujú služby

Ďalšie kritériá - Straty údajov

Thresholdy:

FE zoberie do úvahy:

a) vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov s nepriaznivým vplyvom na plnenie obchodných cieľov FE alebo na schopnosť plniť regulačné požiadavky alebo

b) úspešný, škodlivý a neoprávnený prístup k sieťam a informačným systémom, na ktorý sa nevzťahuje a), pričom tento prístup môže mať za následok straty údajov

dostupnosť - FEs zohľadňujú, či sa údaje na požiadanie FE, jeho klientov alebo jeho protistrán stali dočasne alebo trvalo neprístupnými alebo nepoužiteľnými

pravosť - FEs zohľadňujú, či incident ohrozil dôveryhodnosť zdroja údajov

integrita - FEs zohľadňujú, či incident viedol k neoprávnenej zmene údajov, v dôsledku ktorej sa stali nepresnými alebo neúplnými

dôvernosť - FEs zohľadňujú, či incident viedol k prístupu neoprávnenej strany alebo systému k údajom alebo k ich poskytnutiu neoprávnenej strane alebo systému

Ďalšie kritériá - Hospodársky vplyv

Threshold:

FEs zohľadňuje konkrétne typy priamych a nepriamych nákladov a strát

- priame a nepriame náklady a straty, ktoré FE vznikli v dôsledku incidentu, presiahli alebo pravdepodobne presiahnu 100 000€
  - FEs zahŕňajú napr. náklady na výmenu alebo premiestnenie softvéru, hardvéru alebo infraštruktúry, náklady na zamestnancov vrátane nákladov spojených s výmenou alebo premiestnením zamestnancov, náborom ďalších zamestnancov, odmeňovaním nadčasov, náklady na kompenzáciu zákazníkov, straty v dôsledku ušlých príjmov, náklady na poradenstvo, náklady spojené s internou a externou komunikáciou, atď.
  - FEs nezahŕňajú náklady, ktoré sú potrebné na bežný chod biznisu, napr. náklady na všeobecnú údržbu infraštruktúry, vybavenia, hardvéru a softvéru, náklady na udržiavanie zručností zamestnancov, náklady na modernizáciu, poistné

Opakujúce sa incidenty

- ak sa incidenty individuálne vyskytli aspoň dvakrát v priebehu 6 mesiacov, majú rovnakú zjavnú hlavnú príčinu (root cause) a kolektívne spĺňajú kritériá závažného incidentu, sú považované za jeden závažný incident
- FEs ich existenciu vyhodnocujú na mesačnej báze
- príslušné ustanovenia o opakujúcich sa incidentoch sa nevzťahujú na mikropodniky a FEs so zjednodušeným rámcom riadenia IKT rizika

Významná kybernetická hrozba

Kybernetická hrozba je **významná**, ak spĺňa všetky tieto podmienky:

- mohla by ako materializovaná ovplyvniť CIF FE alebo mať vplyv na iné FEs, , klientov alebo finančné protistrany
- má vysokú pravdepodobnosť materializovať sa vo FE alebo v iných FEs
- mohla by ako materializovaná splniť povinné kritérium „Kritickosť ovplyvnených služieb" alebo kritériá „Klienti, finančné protistrany a transakcie" alebo „Geografické rozloženie", FE však na základe typu hrozby a dostupných informácií môže zvážiť aj ostatné kritériá

Relevantnosť pre iné členské štáty

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

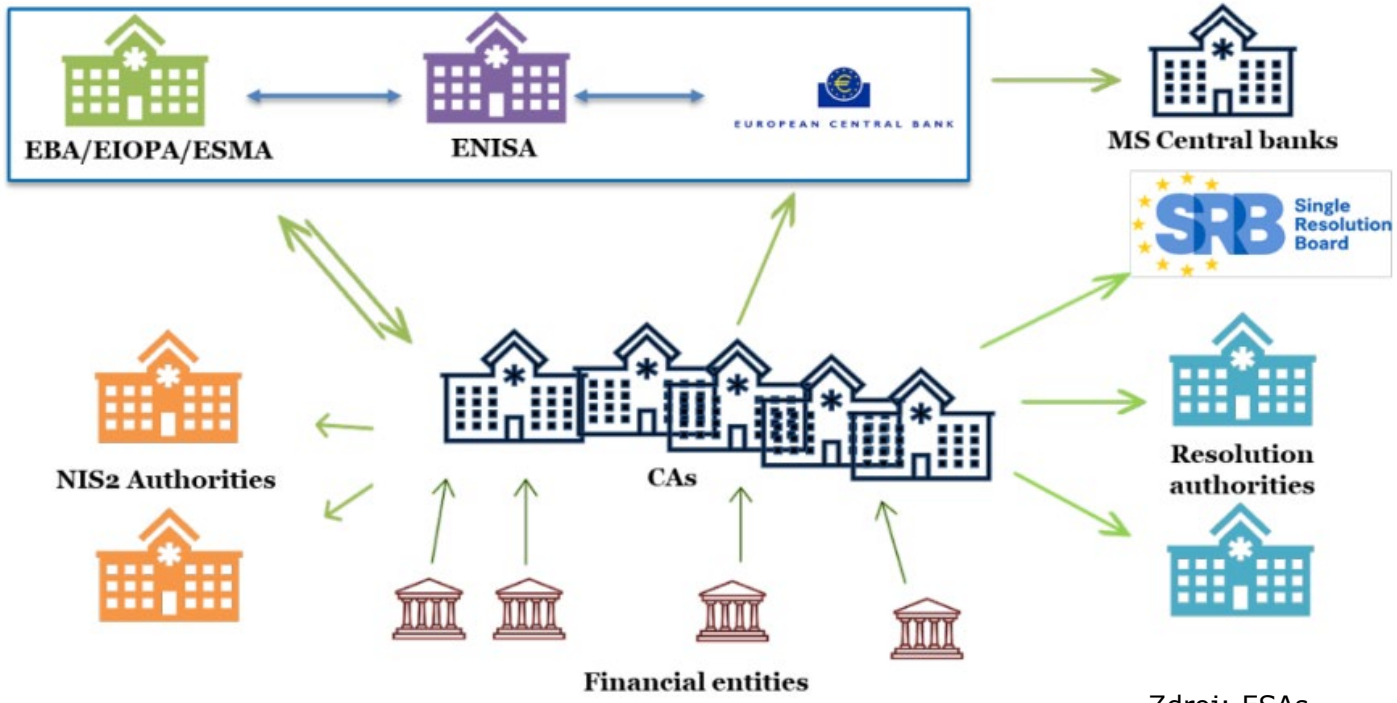
Relevantnosť závažných incidentov pre CAs v iných členských štátoch

- EBA, ESMA alebo EIOPA a ECB po konzultácii s agentúrou ENISA a v spolupráci s CA posúdia, či má incident root cause pochádzajúcu z iného členského štátu alebo či incident má alebo mal významný vplyv v inom členskom štáte v súvislosti s:
  - klientmi alebo finančnými protistranami alebo
  - pobočkou FE alebo inými FEs v rámci skupiny alebo
  - infraštruktúrou finančného trhu alebo treťou stranou s možným vplyvom na FEs
- po tomto posúdení EBA, ESMA alebo EIOPA čo najskôr náležite informujú relevantné CAs v iných členských štátoch, ECB informuje členov ESCB
- CAs v relevantných prípadoch prijmú všetky nevyhnutné opatrenia s cieľom ochrániť bezprostrednú stabilitu finančného systému

Ďalší príjemcovia údajov

Aké údaje o závažnom incidente CA poskytne ďalším príjemcom

- po prijatí počiatočného oznámenia, priebežnej správy a záverečnej správy od FE CA včas poskytne podrobné údaje o závažnom IKT incidente ďalším príjemcom bez anonymizácie



Zdroj: ESAs

Technické riešenie ESAs, ECB, NBS

- požiadavky na európske technické riešenie
  - zber, analýza, assessment, dissemination, varovania, štatistiky
  - data format - Excel, JSON; data exchange - manual upload, bulk file upload, M2M reporting
- ESAs identifikovali riziká - harmonogram, komplexita projektu, omeškania, závislosť na ITS
- ESAs použijú systém CIRAS (nástroj ENISA)
- ECB zvažuje vlastné automatizované riešenie
- NBS plánuje na zber incidentov a hrozieb použiť webové formuláre a API

Q&As

Klasifikácia incidentov

- platí, že pokiaľ incident spĺňa klasifikačné kritériá, FE ho ako závažný nahlasuje do NBS

Spolupráca s NBÚ, zdieľanie incidentov a hrozieb na národnej a európskej úrovni, spätná väzba

- detaily výmeny informácií medzi ESAs, CAs, NIS2 autoritami a CSIRTmi ešte nie sú finálne dohodnuté
- uvažuje sa nad zriadením jednotného centra EÚ (single EU Hub), do 17.1.2025 majú ESAs s ECB a ENISA vypracovať feasibility study pre ďalšiu centralizáciu nahlasovania incidentov
- NBS komunikuje s NBÚ o možnostiach spolupráce vrátane možnosti jednotného predkladania hlásení o incidentoch jedným kanálom (prostredníctvom NBS), prebieha analýza návrhov vykonávacích predpisov k reportingu incidentov
- NBS zatiaľ neuvažuje o zmenách v kanáloch pre komunikáciu so subjektmi, pri nahlásenom závažnom incidente NBS v prípade potreby podnikne príslušné kroky (napr. ad hoc posúdi konkrétny prípad, upovedomí dotknuté strany, vydá adresné varovanie)

Ďakujem za pozornosť