ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 3:
Zodpovednosť v osobitných oblastiach, Časť. 1

JUDr. Michal Rampášek

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

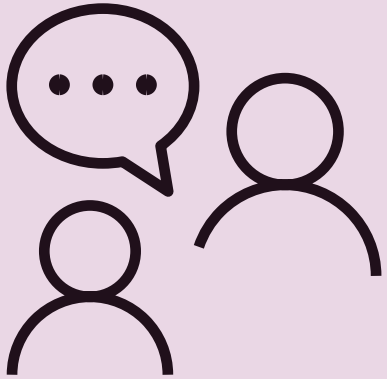
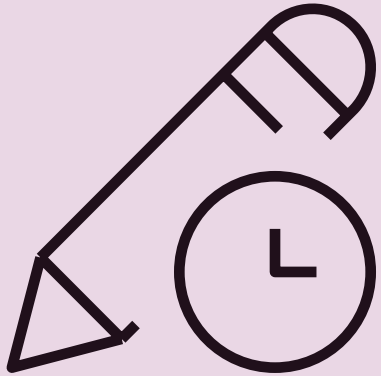
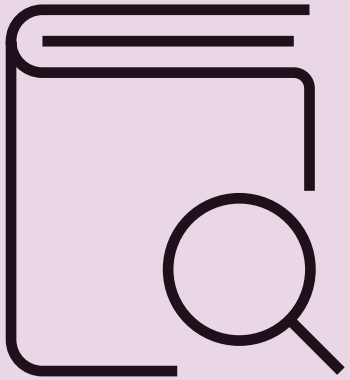
- Kybernetická odolnosť produktov

- Kybernetická bezpečnosť verejnej správy (ITVS)

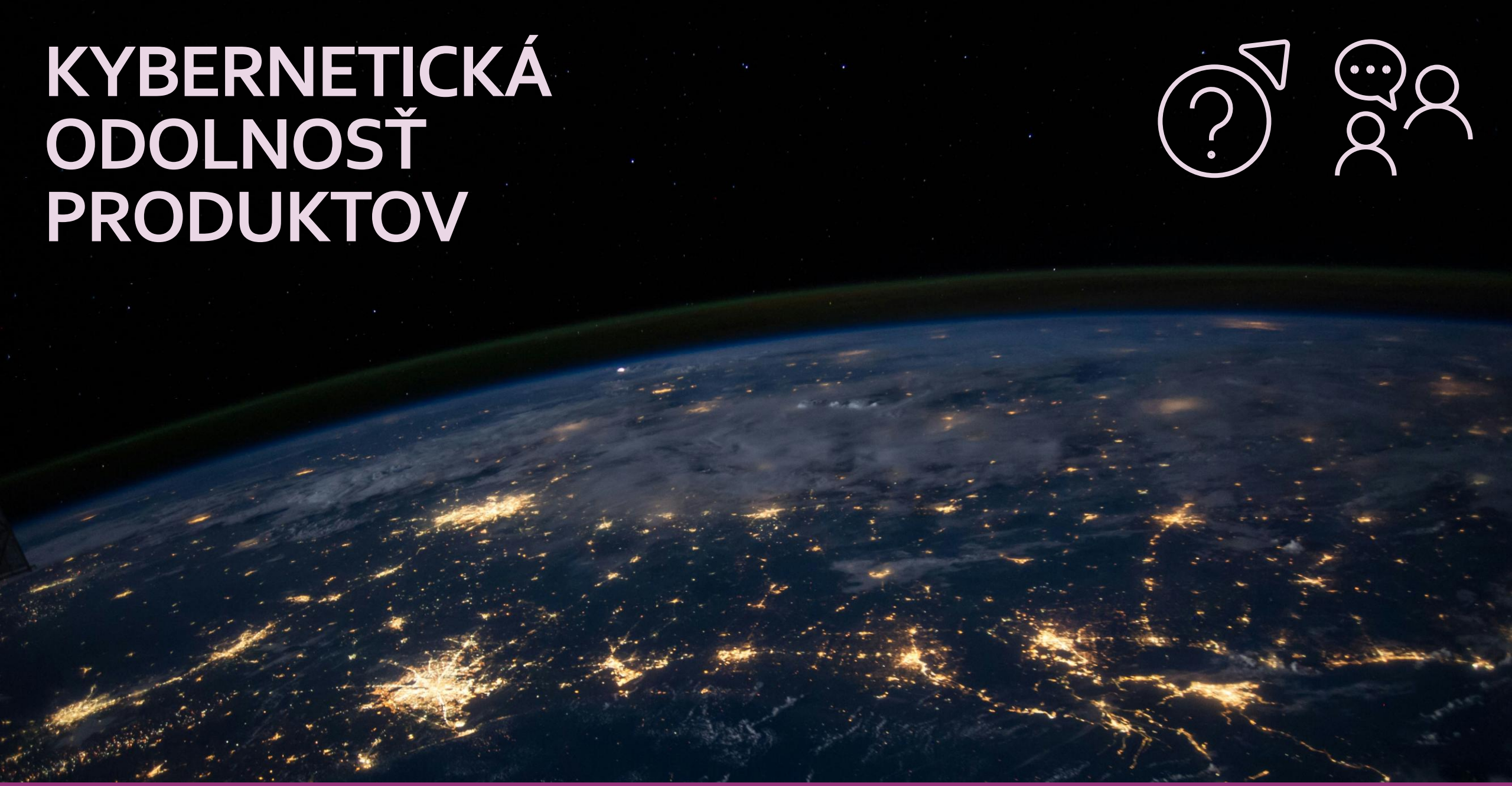
- Kybernetická bezpečnosť v sektore energetika
  - Elektrická energia

- Kybernetická bezpečnosť v sektore doprava
  - Civilná letecká doprava
  - Železničná doprava

ÚVOD

KYBERNETICKÁ ODOLNOSŤ PRODUKTOV



CUSEC

PLÁN OBNOVY

RED
(Rádiové zariadenia)

Smernica o rádiových zariadeniach (RED)

- **Smernica EÚ 2014/53**
- **Čo? bezdrôtovo pripojené zariadenia** napr. cez WiFi a Thread („rádiové zariadenia") predávané v EÚ - mobilné telefóny, tablety, IoT, nositeľné zariadenia, prepojené priemyselné zariadenia etc.
- **Kedy?** od 1. augusta 2025
- Spoločné bezpečnostné požiadavky na rádiové zariadenia VRÁTANE požiadaviek na kybernetickej bezpečnosti. Ochrana zdravia a bezpečnosti osôb a domácich zvierat a ochrana majetku, primeraná úroveň elektromagnetickej kompatibility, efektívne využívanie rádiového frekvenčné ho spektra a podpora jeho účinné ho využívania s cieľom zamedzenia škodlivému rušeniu
- CE označenie
- Delegované nariadenie Komisie (EÚ) 2022/30 z 29. októbra 2021, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/53/EÚ, pokiaľ ide o uplatňovanie základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) uvedenej smernice

Požiadavky

- **Rozšírenie o požiadavky kybernetickej bezpečnosti:** Článok 3 ods. 3 písm. d) až f) zavedený delegovaným nariadením (EÚ) 2022/30, platným od 1. augusta 2025.
- **Ochrana siete (článok 3.3 písm. d) – Zariadenia nesmú poškodzovať siete ani zneužívať zdroje spôsobom, ktorý znižuje kvalitu služieb.**
- **Ochrana údajov a súkromia (článok 3.3 e) – Silné šifrovanie, bezpečné overovanie a opatrenia na ochranu súkromia musia chrániť osobné údaje v každej fáze.**
- **Prevencia podvodov (článok 3.3 f) – Funkcie ako kryptografické podpisovanie FW a mechanizmy proti manipulácii musia zabrániť klonovaniu alebo zneužívaniu zariadení.**

- Nedodržanie predpisov → opatrenia v rámci dohľadu nad trhom, pokuty, stiahnutie výrobkov z trhu a zákaz predaja

EN 18031

- Vykonávacie rozhodnutie Komisie (EÚ) 2025/138 z 28. januára 2025, ktorým sa mení vykonávacie rozhodnutie (EÚ) 2022/2191, pokiaľ ide o harmonizované normy na podporu základných požiadaviek smernice Európskeho parlamentu a Rady 2014/53/EÚ týkajúcich sa kybernetickej bezpečnosti pre kategórie a triedy rádiových zariadení stanovených v delegovanom nariadení (EÚ) 2022/30
- Prvá harmonizovaná normy na kybernetickú bezpečnosť produktov
- = harmonised standards under RED **to demonstrate compliance with cybersecurity provisions**
- EN 18031-1:2024: Časť 1: Rádiové zariadenia pripojené na internet
- EN 18031-2:2024: Časť 2: Rádiové zariadenia spracúvajúce údaje, konkrétne rádiové zariadenia pripojené na internet, rádiové zariadenia na starostlivosť o deti, rádiové zariadenia na hračky a nositeľné rádiové zariadenia
- EN 18031-3:2024: Časť 3: Rádiové zariadenie pripojené k internetu spracovávajúce virtuálne peniaze alebo peňažnú hodnotu

Požiadavky normy

- **33 požiadaviek je rozdelených do 11 skupín** (riadenie prístupu, autentifikácia, bezpečné úložisko, bezpečná komunikácia, odolnosť, monitorovanie siete, riadenie prevádzky, dôvernosť kryptografických kľúčov, všeobecné možnosti zariadení a kryptografia).
- **Výnimky z normy** podľa Vykonávacie ho rozhodnutiq Komisie (EÚ) 2025/138
- EN 18031-1:2024, EN 18031-2:2024 a EN 18031-3:2024 obsahujú viaceré oddiely s názvom „odôvodnenie" (*rationale*) a „usmernenie" (*guidance*). = Oddielmi, ktoré sú v tejto norme označené ako **‚odôvodnenie' (*rationale*) a ‚usmernenie' (*guidance*),** sa nezakladá predpoklad zhody so základnými požiadavkami stanovenými v článku 3 ods. 3 prvom pododseku písm. d) smernice 2014/53/EÚ.
- Body 6.2.5.1 a 6.2.5.2 v EN 18031-1:2024, EN 18031-2:2024 a EN 18031-3:2024 sa týkajú predvolených hesiel. Vďaka týmto ustanoveniam môžu výrobcovia používateľom povoliť nenastavovať alebo nepoužívať žiadne heslo = Touto harmonizovanou normou sa nezakladá predpoklad zhody so základnými požiadavkami stanovenými v článku 3 ods. 3 prvom pododseku písm. d) smernice 2014/53/EÚ, ak pri uplatňovaní jej bodov 6.2.5.1 a 6.2.5.2 je používateľovi dovolené nastaviť si a používať žiadne heslo = **výrobca NESMIE UMOŽNIŤ používateľovi NEZADAŤ heslo**

Prechod k CRA

- K 11. decembru 2027 RED zanikne a bude už len CRA.
- V takom prípade budú kategórie rádiových zariadení uvedených v delegovanom nariadení RED, ak budú uvedené na trh medzi 1. augustom 2025 a 10. decembrom 2027, podliehať základným požiadavkám RED na kybernetickú bezpečnosť, ktoré sa stali uplatniteľnými prostredníctvom delegovaného nariadenia RED. Naopak, ak budú tieto výrobky uvedené na trh 11. decembra 2027 alebo neskôr, po začatí uplatňovania CRA, budú tieto výrobky podliehať základným požiadavkám CRA.
- **Zrušenie delegovaného nariadenia RED s účinnosťou od 11. decembra 2027** neovplyvní dohľad nad trhom Únie a kontrolu súladu rádiových zariadení so základnými požiadavkami RED na kybernetickú bezpečnosť, ak tieto rádiové zariadenia boli alebo sú uvedené na trh EÚ medzi 1. augustom 2025 a 10. decembrom 2027 a podliehali niektorej z týchto základných požiadaviek.
- **EN 18031 je však vhodný začiatok pre prípravu na CRA a ukáže cestu k harmonizovaným normám CRA**

Prechod k CRA

- Podľa článku 69 ods. 1 CRA zostávajú **certifikáty EÚ o typovej skúške a rozhodnutia o schválení** vydané v súvislosti s požiadavkami na kybernetickú bezpečnosť pre výrobky s digitálnymi prvkami, na ktoré sa vzťahujú iné harmonizačné právne predpisy Únie, **ako napríklad delegované nariadenie Komisie (EÚ) 2022/30, platné do 11. júna 2028** (pokiaľ nie je v takýchto právnych predpisoch uvedené inak alebo pokiaľ platnosť certifikátu neuplynie pred týmto dátumom).

CRA (Produkty s digitálnym prvkom)

Akt o kybernetickej odolnosti

- **Pravidlá kybernetickej bezpečnosti** pri uvádzaní hardvéru a softvéru na trh
- **Povinnosti** výrobcov, distribútorov a dovozcov
- **Základné požiadavky** kybernetickej bezpečnosti na **návrh, vývoj a výrobu** produktov a na procesy **riešenia zraniteľností** počas predpokladaného **obdobia používania** produktov
- Harmonizované **normy**
- **Posudzovanie zhody** podľa úrovne rizika – **"CE"** označenie
- **Oznamovacie** povinnosti
- **Dohľad a monitorovanie**

Akt o kybernetickej odolnosti

- **priamo aplikovateľné**
- **NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (akt o kybernetickej odolnosti)**
- **130 recitálov** („návod" na pochopenie a výklad)
- **71 článkov** (články 13 a 14 kľúčové povinnosti)
- **8 príloh** (Príloha I – základné požiadavky KB = 2x A4)

+ harmonizované normy od CEN/CENELEC (41)

+ delegované akty Komisie

Čo? Produkt s digitálnym prvkom (PDE)

✅ **HW produkty (vrátane komponentov uvedených na trh)**

✅ **SW produkty (vrátane komponentov uvedených na trh)**

... vrátane ich riešení na vzdialené spracovanie údajov (remote data processing solutions) = nie uplne jasný právny pojem

- ✘ **Produkty na vlastné použitie** (pokiaľ nepatria do rozsahu pôsobnosti harmonizačných právnych predpisov EÚ, napr. nariadenie o strojových zariadeniach)
- ✘ **Služby, najmä samostatné SaaS (patrí pod NIS2)**
- ✘ **Vylúčené produkty** (motorové vozidlá, zdravotnícke pomôcky, civilné letectvo, námorné lode)
- ✘ **Náhradné diely**

CRA vs NIS2

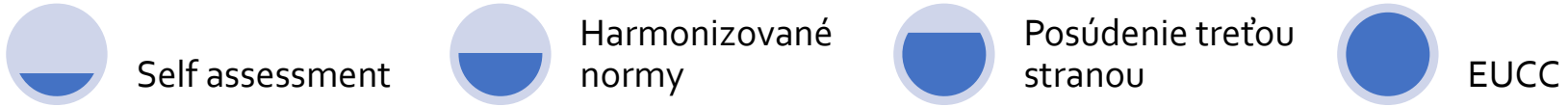
- Recitál č. 12 CRA: Cloudové riešenia predstavujú riešenia diaľkového spracovania údajov v zmysle nariadenia CRA len vtedy, ak spĺňajú vymedzenie stanovené v tomto nariadení.
- Napríklad cloudové funkcie poskytované výrobcom inteligentných domácich zariadení, ktoré používateľom umožňujú ovládať zariadenie na diaľku, patria do rozsahu pôsobnosti nariadenia CRA.
- Na druhej strane webové sídla, ktoré nepodporujú funkčnosť produktu s digitálnymi prvkami, ani cloudové služby navrhnuté a vyvinuté mimo zodpovednosti výrobcu produktu s digitálnymi prvkami nepatria do rozsahu pôsobnosti tohto nariadenia.
- Smernica NIS2 sa vzťahuje na cloudové služby a modely cloudových služieb, ako je softvér ako služba (SaaS), platforma ako služba (PaaS) a infraštruktúra ako služba (IaaS).

Delegované predpisy Komisie

- Odklad zverejňovania oznámení (11. december 2025): Komisia prijala delegovaný akt, v ktorom sa stanovujú podmienky, za ktorých môže CSIRT odložiť zdieľanie správ výrobcov o zraniteľnostiach alebo incidentoch s inými tímami CSIRT.
- Vylúčenie určitých výrobkov (29. júl 2025): Bol prijatý delegovaný nariadenie Komisie (EÚ) 2025/1535 s cieľom vylúčiť z rozsahu pôsobnosti CRA určité výrobky s digitálnymi prvkami, na ktoré sa vzťahuje nariadenie (EÚ) č. 168/2013.
- Technický popis dôležitých/kritických výrobkov (28. november 2025): Vykonávacie nariadenie Komisie (EÚ) 2025/2392 bolo prijaté s cieľom definovať technické špecifikácie pre dôležité a kritické kategórie produktov.
- Predpoklad zhody certifikácie EUCC (očakávané v 4. štvrťroku 2026): Očakáva sa, že budúci delegovaný akt bude špecifikovať, ako budú produkty certifikované podľa schémy EUCC mať predpoklad zhody s CRA.

Kategórie produktov

Bežné	Dôležité Trieda I	Dôležité Trieda II	Kritické
• 90% • Pamätové čipy, mobilné appky, tlačiarne	• Príloha III* • Operačné systémy, AV, VPN, SIEM	• Príloha III* • FW, IDS, IPS, hypervízory	• Príloha IV* • Inteligentné merače, čipové karty, HW s bezp. schránkami



Pre FOSS postačuje self assessment (postup vnútornej kontroly podľa modulu A), ak nejde o kritický produkt.

Technický opis produktov: Vykonávacie nariadenie Komisie (EÚ) 2025/2392 z 28. novembra 2025 o technickom opise kategórií dôležitých a kritických produktov s digitálnymi prvkami podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847

Vykonávacie nariadenie Komisie (EÚ) 2025/2392

PRÍLOHA II

KRITICKÉ PRODUKTY S DIGITÁLNYMI PRVKAMI

Kategória produktu	Technický opis
1. Hardvérové zariadenia s bezpečnostnými schránkami	Hardvérové produkty s digitálnymi prvkami, ktoré bezpečne uchovávajú, spracúvajú alebo spravujú citlivé údaje alebo vykonávajú kryptografické operácie a ktoré pozostávajú z viacerých samostatných komponentov vrátane hardvérového fyzického obalu, ktorý zabezpečuje dôkazy o neoprávnenej manipulácii, odolnosť alebo reakciu ako protiopatrenia proti fyzickým útokom. Táto kategória okrem iného zahŕňa fyzické platobné terminály, hardvérové bezpečnostné moduly, ktoré generujú a riadia kryptografické prvky, a tachografy, ktoré spĺňajú uvedený opis.
2. Prístroje smart meter gateway v inteligentných meracích systémoch vymedzených v článku 2 bode 23 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([1]) a iné zariadenia na vyššie bezpečnostné účely vrátane bezpečného kryptografického spracovania.	Prístroje smart meter gateway sú produkty s digitálnymi prvkami, ktoré riadia komunikáciu medzi komponentmi v pripojených alebo inteligentných meracích systémoch, ako sú vymedzené v článku 2 bode 23 smernice (EÚ) 2019/944, a autorizovanými tretími stranami, napríklad poskytovateľmi verejných služieb. Prístroje smart meter gateway zbierajú, spracúvajú a uchovávajú údaje z merania alebo osobné údaje, chránia údaje a informačné toky prostredníctvom podpory osobitných kryptografických potrieb, napríklad šifrovania a dešifrovania údajov, sú v nich zabudované funkcie firewall a poskytujú prostriedky na ovládanie iných zariadení. Táto kategória zahŕňa okrem iného prístroje smart meter gateway súvisiace s inteligentnými meracími systémami merajúcimi elektrinu, ako sú vymedzené v článku 2 bode 23 smernice (EÚ) 2019/944. Takisto môže zahŕňať prístroje smart meter gateway používané v iných inteligentných meracích systémoch merajúcich spotrebu iných zdrojov energie (napr. plynu alebo tepla) za predpokladu, že prístroj spĺňa tento opis.

Smart meter gateway

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Posúdenie zhody

- **Modul A (internal production control)** zahŕňa samohodnotenie, t. j. výrobca posudzuje zhodu svojho výrobku bez účasti notifikovaného orgánu.
- **V module B (EC-type examination) notifikovaný orgán posudzuje zhodu výrobku (tzv. vzorky). Výrobca potom vyrába všetky ostatné výrobky podľa tejto vyhovujúcej vzorky (modul C (internal production control).** Výrobca musí zabezpečiť, aby každý výrobok bol v zhode so vzorkou z modulu B. Modul B sa musí v CRA vždy kombinovať s modulom C.
- **V module H (full quality assurance)** notifikovaný orgán posudzuje zabezpečenie kvality výrobcu, t. j. notifikovaný orgán kontroluje, či výsledkom procesu zabezpečenia kvality výrobcu sú výrobky, ktoré sú v súlade s CRA. Ak je to tak, výrobca môže vyrábať všetky ďalšie výrobky podľa tohto procesu.

Harmonizované normy

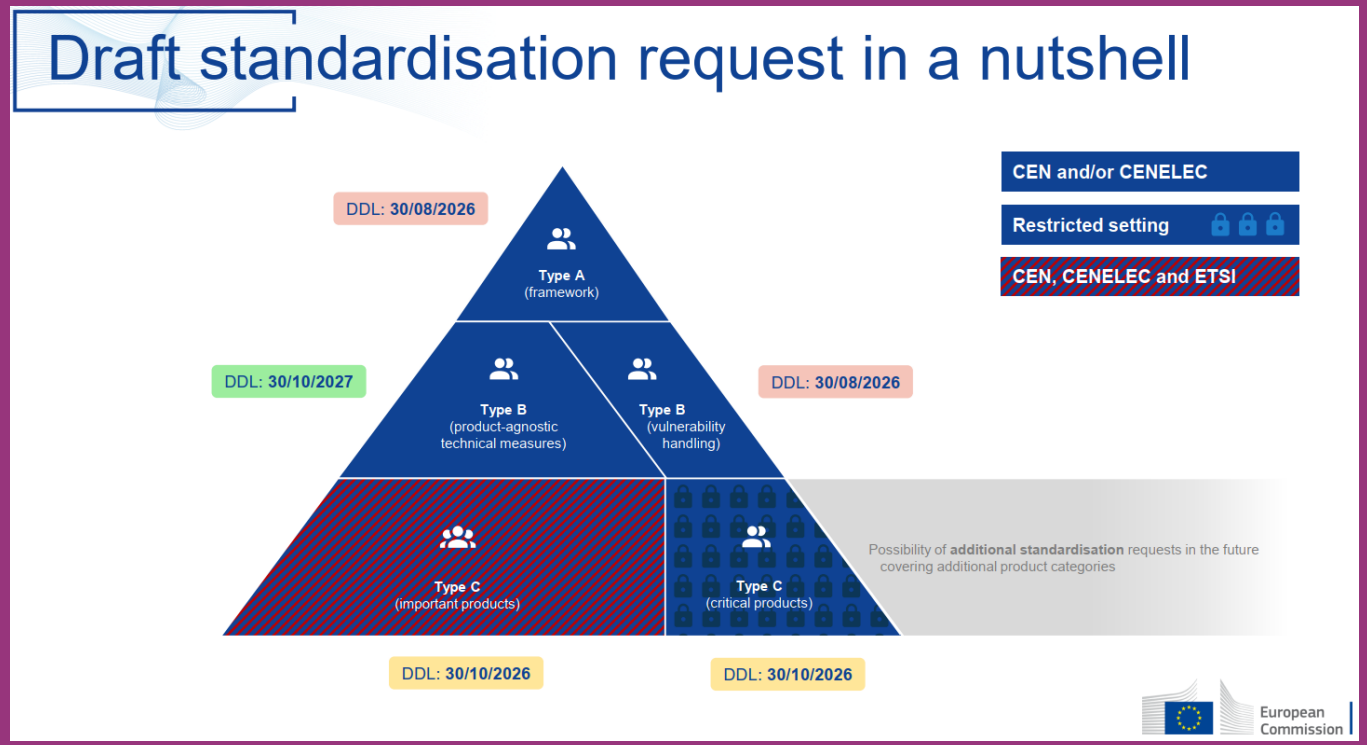
Horizontálne štandardy (1-15)

- Prístup založený na riziku (príloha I k CRA)
- Základné požiadavky (príloha I k CRA časť 1)
- Riešenie zraniteľností (príloha I k CRA časť 2)

Vertikálne štandardy (16-41)

- Dôležité produkty triedy 1 (príloha III k CRA)
- Dôležité produkty triedy 2 (príloha III k CRA)
- Kritické produkty (príloha IV k CRA)

Harmonizované normy



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Posúdenie zhody

- **EU schémy certifikácie kyberbezpečnosti**
- **EUCC schéma** (dve úrovne záruky „významná“ a „vysoká“) Účinnosť 27.2.2025
- **CRA umožňuje, aby certifikácia podľa EUCC pokrývala základné požiadavky na kybernetickú bezpečnosť a povinnosti posudzovania zhody vyplývajúce z CRA, a teda aby sa certifikácia podľa EUCC používala na bezproblémové preukázanie zhody s CRA.**

Cyber Resilience Act implementation via EUCC and its applicable technical elements

Final version: 27/01/2025

The CRA implementation via EUCC and its applicable technical elements report is issued by ENISA based on a request of technical support for the preparation of the implementation of the CRA received from European Commission (July-2023), the subsequent follow-up feedback also provided by the European Commission on April 2024 and the updates in the latest text of the CRA 2024/2847 (23 October 2024).

FOSS

Free and Open Source Software

1. **Je projekt produktom?**

CRA **sa nevzťahuje** na fyzické alebo právnické osoby, ktoré **prispievajú zdrojovým kódom k produktom** s digitálnymi prvkami, ktoré sa považujú za FOSS, za ktoré nenesú zodpovednosť (recitál 18)

NIE ak ide len o službu (SaaS), hosting code repository, prispievanie do iných projektov

2. Je projekt open source?

Je softvér, ktorého zdrojový kód je **voľne dostupný** a ktorý je vytvorený na základe **bezplatnej a otvorenej licencie,** ktorá udeľuje **všetky práva** na voľný **prístup** k nemu, jeho **použiteľnosť, modifikovateľnosť a redistribúciu** (čl. 3 ods. 48)

Čo ale ak licencie nepovoľujú začlenenie do proprietárnych programov (napr. GPL)?

FOSS

3. Je môj projekt komerčný?

... len FOSS sprístupnený na trhu, a preto **dodávaný na distribúciu alebo používanie v rámci obchodnej činnosti (= cielene a jasne komerčný účel)**

- účtovaním **ceny za produkt** s digitálnymi prvkami,
- účtovaním **ceny za služby technickej podpory,** ak nejde len o náhradu skutočných nákladov,
- so **zámerom speňažiť,** napríklad poskytnutím softvérovej platformy, prostredníctvom ktorej výrobca speňažuje iné služby,
- **vyžadovaním použitia spracovania osobných údajov** ako podmienky z iných dôvodov než výlučne na zlepšenie bezpečnosti, kompatibility alebo interoperability softvéru, alebo
- **prijatím darov presahujúcich náklady** spojené s návrhom, vývojom a poskytovaním produktu. Prijímanie darov bez úmyslu dosiahnuť zisk by sa nemalo považovať za obchodnú činnosť.

FOSS

4. Kombinované FOSS a komerčné produkty

= povinnosť výrobcu produktu (nie tvorcu FOSS)

- Výrobcovia uplatňujú **náležitú starostlivosť pri integrácii komponentov získaných od tretích strán** tak, aby tieto komponenty neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami, a to aj pri integrácii komponentov FOSS, ktoré neboli sprístupnené na trhu v priebehu obchodnej činnosti (čl. 13 ods.5)
- **Delegované akty Komisie** na zavedenie programov dobrovoľného osvedčovania bezpečnosti, ktoré programátorom alebo používateľom FOSS.

Kedy?

- **11. september 2026:** oznamovanie **aktívne zneužívaných zraniteľností a závažných incidentov**
- **11. december 2027**: Uplatňujú sa **všetky požiadavky CRA**
- Všetky staré aj nové produkty
- Koncepcia uvedenia na trh sa vzťahuje na **každý jednotlivý výrobok**, nie na typ výrobku, a na to, či bol vyrobený ako samostatná jednotka alebo v sérii.
- Výrobok je sprístupnený na trhu, keď je **dodaný na distribúciu, spotrebu alebo používanie** na trhu Únie v rámci obchodnej činnosti, či už za odplatu, alebo bezplatne. Takýmto dodaním je akákoľvek ponuka (napr. reklamné kampane).
- **Modrá príručka („Blue Guide")** (2022/C 247/01)

Kto?

- **Výrobcovia (č. 13)** … **vyvíja alebo vyrába** produkty **alebo si dáva** navrhnúť, vyvinúť alebo vyrobiť produkty **a predáva ich** pod svojím menom alebo svojou ochrannou známkou, či už za odplatu, speňaženie alebo bezodplatne
- **Dovozcovia (č. 19)** ….uvádza na trh produkt označený menom alebo ochrannou známkou osoby usadenej mimo Únie
- **Distribútori (čl. 20)** osoba v dodávateľskom reťazci okrem výrobcu alebo dovozcu, ktorá na trhu Únie sprístupňuje produkt bez toho, aby ovplyvňovala jeho vlastnosti
- **Kvázi výrobcovia (čl. 21 a 22) = 1)** ak dovozca alebo distribútor uvádza produkt na trh **pod svojím menom alebo svojou ochrannou známkou,** alebo ak podstatne upraví produkt už uvedený na trh. **2) iná osoba,** ktorá vykoná **podstatnú úpravu** produktu s digitálnymi prvkami a sprístupní uvedený produkt na trhu
- **Správcovia softvéru s otvoreným zdrojovým kódom (čl. 24).**. zavedú a zdokumentujú **politiku kybernetickej bezpečnosti.** Uvedenou politikou sa posilní aj **dobrovoľné oznamovanie zraniteľností**… **spolupracujú s orgánmi dohľadu nad trhom** na ich žiadosť s cieľom zmierňovať kybernetickobezpečnostné riziká, ktoré predstavuje produkt FOSS. **Povinnosti oznamovania zraniteľností a incidentov ako výrobca len v prípade ak sa podieľajú na vývoji softvéru alebo ide o siete a informačné systémy správcu**

Podstatná úprava

- ... **ovplyvňuje súlad produktu** s digitálnymi prvkami so **základnými požiadavkami** kybernetickej bezpečnosti stanovenými v **časti I prílohy I alebo** ktorá vedie k **úprave zamýšľaného účelu,** pre ktoré bol produkt s digitálnymi prvkami posudzovaný (čl. 3 ods. 30)
- Ak sa produkty s digitálnymi prvkami následne fyzicky alebo digitálne upravia spôsobom, s ktorým výrobca **pri prvom posúdení rizika nepočítal a** z ktorého **môže vyplynúť, že už nespĺňajú príslušné základné požiadavky** kybernetickej bezpečnosti (recitál č. 38, 39)
- ... ak **aktualizácia prvku mení pôvodné zamýšľané funkcie alebo typ, či výkonnosť** produktu s digitálnymi prvkami a spĺňa vyššie uvedené kritériá, mala by sa považovať za podstatnú úpravu, keďže **pridanie nových prvkov** zvyčajne vedie k širšej ploche útoku, čím sa kybernetico-bezpečnostné riziko zvyšuje

Povinnosti výrobcov v životnom cykle produktu

Design and Development

- **Primeraná uroveň KB na základe analýzy rizík, Základné požiadavky a Posúdenie zhody**
- SBOM v obvykle používanom strojovo čitateľnom formáte
- Security-by-default (ak sa nedohodnú inak pri custom produktoch)
- Ochrana pred neoprávneným prístupom (správa overovania, identity alebo prístupu)
- Ochrana údajov šifrovaním
- Minimalizácia spracúvania osobných údajov
- Dostupnosť hlavných funkcií aj po incidente
- Obnedzenie plochy útokov vrátane externých rozhraní
- Možnosť factory reset, natvralo odstrániť všetky udaje a ich prenesenie

Maintenance

- Automatické bezpečnostné aktualizácie s možnosťou odmietnuť/odložiť. Informácie a kroky.
- Riadenie zraniteľností počas celého životného cyklu
- Zverejňovanie informácie o zraniteľnostiach + CVD politika
- Záznam a monitorovanie interných činností vrátane prístupu a menám (možnosť opt-out používateľa
- Oznamovancie povinnosti (nová platforma ENISA a CSIRT) 1) aktívne zneužívaná zraniteľnosť, 2) závažné incidenty

Changes

- Pokračujú oznamovacie povinnosti
- Zmeny , ktoré môžu vieť k postatnej úprave
- overiť súlad produktu s digitálnymi prvkami s predpismi a prípadne ho podrobiť novému posúdeniu zhody

Obdobie podpory

- Obdobie podpory trvá **najmenej 5 rokov**.
- Ak sa predpokladá, že sa bude používať **menej ako 5 rokov, obdobie podpory musí zodpovedať očakávanému obdobiu používania.**
- Výrobcovia uvedú informácie, ktoré sa zohľadnili pri určovaní obdobia podpory produktu s digitálnymi prvkami, **v technickej dokumentácii** stanovenej v prílohe VII.
- Komisia môže prijať **delegované akty špecifikovaním minimálneho obdobia podpory** pre konkrétne kategórie produktov, ak z údajov dohľadu nad trhom vyplýva neprimerané obdobie podpory

Aktualizácie

- Výrobcovia zabezpečia, aby **každá bezpečnostná aktualizácia,** ktorá bola sprístupnená používateľom počas obdobia podpory, zostala k dispozícii po jej vydaní **minimálne 10 rokov alebo počas zvyšku obdobia podpory, podľa toho, čo trvá dlhšie**.

Dokumentácia dodávateľského reťazca

- Každý výrobca, dodávateľ, či distribútor musí **poskytnúť na požiadanie** orgánom dohľadu nad trhom (čl. 23 CRA):

a) meno a adresu každého hospodárskeho subjektu, **ktorý im dodal** produkt s digitálnymi prvkami;

b) meno a adresu každého hospodárskeho subjektu, **ktorému dodali** produkt s digitálnymi prvkami, ak sú tieto informácie k dispozícii

Hospodárske subjekty musia byť schopné poskytnúť informácie **počas obdobia 10 rokov** po tom, čo im bol produkt s digitálnymi prvkami dodaný, a počas obdobia 10 rokov po tom, čo produkt s digitálnymi prvkami dodali

Informácie a návod

- Príloha II CRA

1. Identifikácia výrobcu, kontaktné údaje (adresa, e-mail, web).
2. Kontaktné miesto pre oznamovanie zraniteľností a politika koordinovaného oznamovania.
3. Názov a typ produktu s digitálnymi prvkami, vrátane jedinečnej identifikácie.
4. Plánovaný účel produktu, základné funkcie a bezpečnostné vlastnosti.
5. Predvídateľné okolnosti použitia alebo nesprávneho použitia s možnými kybernetickými rizikami.
6. Odkaz na EÚ vyhlásenie o zhode (ak relevantné).
7. Informácia o technickej podpore a dátum ukončenia podpory pre bezpečnostné aktualizácie.
8. Návod alebo odkaz naň s informáciami o bezpečnom použití, vplyve zmien na bezpečnosť údajov, inštalácii aktualizácií, bezpečnom vyradení z prevádzky, vypnutí automatickej inštalácie aktualizácií, požiadavkách pre integrátorov.
9. Ak výrobca sprístupňuje SBOM, informácia, kde ho nájsť.

Technická dokumentácia

- Príloha VII CRA

1. **Všeobecný opis produktu** Plánovaný účel, verzie softvéru vplývajúce na bezpečnosť, obrázky hardvéru (ak relevantné), používateľský návod.
2. **Opis riešenia, vývoja a výroby** Návrh a architektúra systému, postupy riešenia zraniteľností (vrátane kontaktu pre hlásenia a distribúcie aktualizácií), výrobný proces a jeho validácia.
3. **Posúdenie kybernetícko-bezpečnostných rizík**
4. **Informácie k obdobiu podpory**
5. **Zoznam noriem a špecifikácií**
6. **Správy o skúškach** Overenie zhody produktu a procesov riešenia zraniteľností.
7. **EÚ vyhlásenie o zhode**
8. **Zoznam SBOM (ak požadovaný orgánom dohľadu)**

Zodpovednosť za chybné výrobky

- **Smernica o zodpovednosti za chybné výrobky (EÚ) 2024/2853 (PLD)**
- CRA a smernica o zodpovednosti za výrobky (PLD) majú odlišnú povahu a navzájom sa dopĺňajú
- Zodpovednosť za chybné výrobky sa vzťahuje na všetky hnuteľné veci vrátane softvéru, a to aj vtedy, ak sú súčasťou iných hnuteľných vecí alebo sú nainštalované do nehnuteľných vecí
- PLD stanovuje pravidlá zodpovednosti za chybné výrobky, aby **poškodené fyzické osoby mohli žiadať náhradu škody, ak bola škoda spôsobená chybnými výrobkami.**
- Výrobca výrobku zodpovedá za škody spôsobené vadou svojho výrobku bez ohľadu na zavinenie alebo nedbanlivosť (objektívna zodpovednosť).
- **Škodou je aj zničenie alebo poškodenie údajov, ktoré sa nepoužívajú výlučne na profesionálne účely**
- Chybovosť výrobku sa posudzuje na základe toho, či výrobok poskytoval bezpečnosť, ktorú možno očakávať, alebo ktorá sa vyžaduje podľa práva. **Chybovosť sa musí posudzovať s prihliadnutím na všetky okolnosti, vrátane požiadaviek na kybernetickú bezpečnosť. CRA napríklad stanovuje výrobcom osobitné povinnosti týkajúce sa bezpečnostných aktualizácií výrobkov s digitálnymi prvkami (príloha I).**
- Výrobca naďalej zodpovedá za akékoľvek vady, **po jeho uvedení výrobku na trh, ak boli spôsobené v dôsledku** a) súvisiacej služby; b) softvéru vrátane aktualizácií alebo modernizácií softvéru; c) nedostatku aktualizácií alebo modernizácií softvéru potrebných na zachovanie bezpečnosti; d) podstatnej zmeny výrobku.. **za predpokladu, že boli pod kontrolou výrobcu**

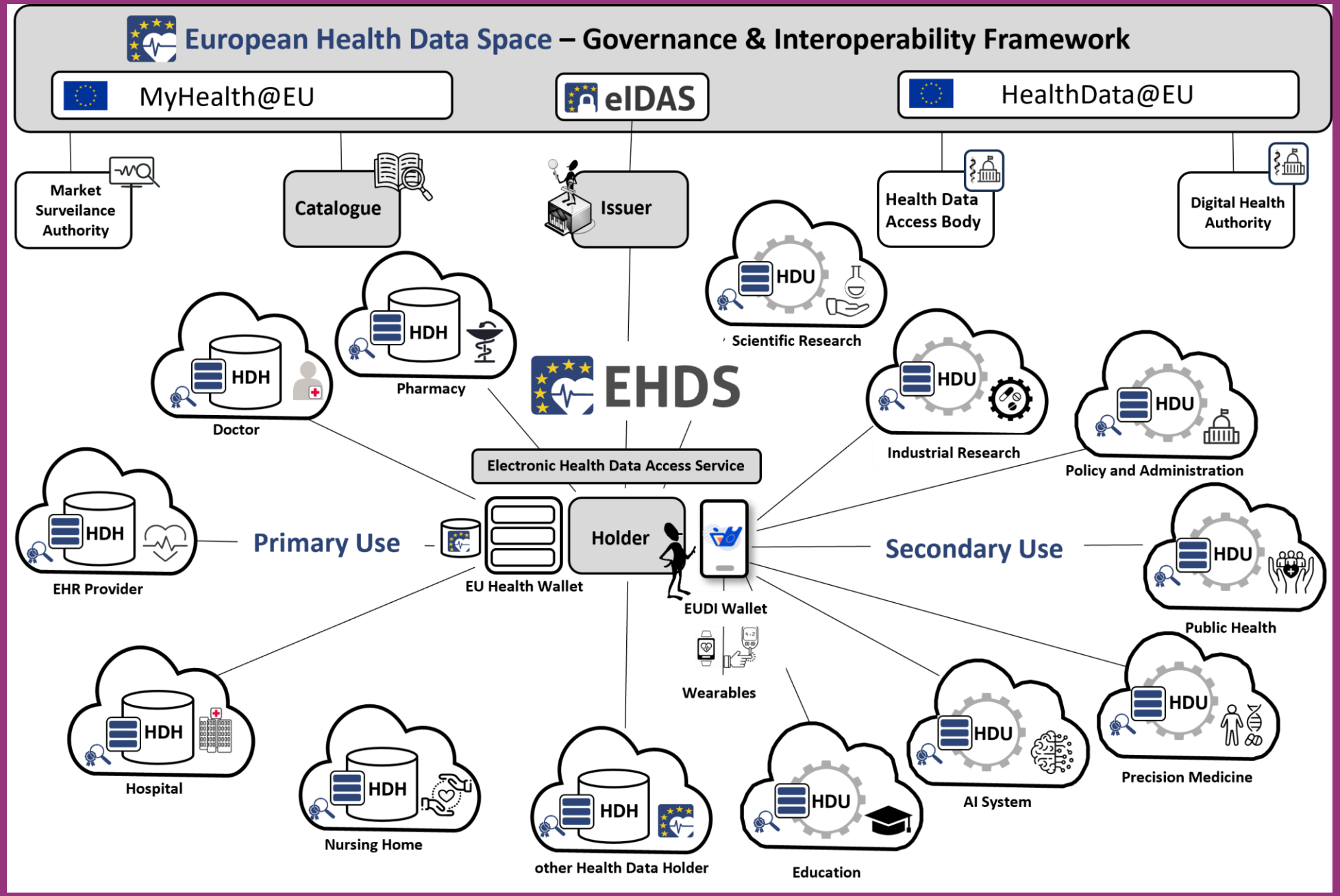
Systémy EHR a wellness aplikácie

EHDS

- Nariadenie o európskom priestore pre zdravotné údaje (nariadenie (EÚ) 2025/327 (EHDS) - od marca 2027/2029/2031
- Pravidlá pre prístup k elektronickým zdravotným údajom na účely primárneho a sekundárneho používania
- Povinnosti, ktoré musia spĺňať systémy elektronických zdravotných záznamov (EHR) a ich dve harmonizované zložky

1. Komponent interoperability ktorý poskytuje možnosť importovať/exportovať údaje v rámci európskeho formátu výmeny elektronických zdravotných záznamov (European Electronic Health Record Exchange Format)
2. Komponent logovania ktorý poskytuje možnosť generovať logy o prístupe

- systém EHR je akýkoľvek systém, v ktorom softvér alebo kombinácia hardvéru a softvéru tohto systému spracúvať osobné elektronické zdravotné údaje a ktoré výrobca určil na používanie poskytovateľmi zdravotnej starostlivosti pri poskytovaní starostlivosti o pacienta alebo pacientmi na prístup k svojim elektronickým zdravotným údajom
- Príklad: Počítač alebo softvér, ktorý bol uvedený na trh a zakúpený nemocnicou a ktorý je určený na ukladanie a prezeranie súhmov o pacientoch pri poskytovaní zdravotnej starostlivosti, môže byť produktom s digitálnymi prvkami v zmysle CRA, ktorý je zároveň systémom EHR v zmysle nariadenia EHDS.



https://www.ehds.io

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Základné požiadavky na harmonizované softvérové komponenty

- PRÍLOHA II EHDS
- 1) všeobecné požiadavky, 2) interoperabilita 3) bezpečnosť
- Systémy EHR
- Uplatňujú sa aj na zdravotnícke pomôcky, diagnostické zdravotnícke pomôcky in vitro, systémy AI a wellness aplikácie v prípade ktorých sa tvrdí, že sú interoperabilné so systémami EHR
- Wellness aplikácia je HW/SW ktorý výrobca určil na to, aby ho fyzická osoba používala na spracúvanie elektronických zdravotných údajov, výslovne na poskytovanie informácií o zdraví alebo na poskytovanie starostlivosti na inej ako zdravotnej starostlivosti.

Požiadavky na bezpečnosť a logovanie (Príloha II časť 3 EHDS)

- Systém EHR určený na používanie zdravotníckymi pracovníkmi musí poskytovať spoľahlivé mechanizmy identifikácie a autentifikácie zdravotníckych pracovníkov.
- Európsky softvérový komponent logovania systému EHR určeného na umožňovanie prístupu poskytovateľov zdravotnej starostlivosti alebo iných osôb k osobným elektronickým zdravotným údajom poskytuje dostatočné mechanizmy logovania, ktoré zaznamenajú o každej udalosti alebo skupine udalostí prístupu aspoň tieto informácie: a) identifikácia poskytovateľa zdravotnej starostlivosti alebo iných jednotlivcov, ktorí prehliadali osobné elektronické zdravotné údaje; b) identifikácia konkrétnej fyzickej osoby alebo osôb, ktoré prehliadali osobné elektronické zdravotné údaje; c) kategórie údajov, ktoré sa prehliadali; d) čas a dátum prístupu; e) pôvod alebo pôvody údajov.
- Harmonizované softvérové komponenty systému EHR obsahujú nástroje alebo mechanizmy na preskúmanie a analýzu údajov logovania alebo podporujú pripojenie a využitie externého softvéru na tieto účely.
- Harmonizované softvérové komponenty systému EHR, ktoré uchovávajú osobné elektronické zdravotné údaje musia podporovať rôzne obdobia uchovávania údajov a prístupové práva, ktoré zohľadňujú pôvod a kategórie elektronických zdravotných údajov.

Posúdenie zhody

- **Požiadavky na kybernetickú bezpečnosť stanovené v CRA a EHDS sú takej povahy, že splnenie požiadaviek buď CRA, alebo EHDS samo osebe nebude plne spĺňať požiadavky druhého nariadenia.**
- **CRA však stanovuje, že v prípade produktov s digitálnymi prvkami, ktoré sú zároveň systémami EHR, môže byť posúdenie rizika kybernetickej bezpečnosti vyžadované nariadením CRA súčasťou posúdenia rizika vyžadovaného EHDS.**
- Vypracuje jediné vyhlásenie o zhode EÚ, ktoré sa vzťahuje na všetky právne akty Únie uplatniteľné na systém EHR. Toto vyhlásenie o zhode EÚ obsahuje všetky informácie potrebné na identifikáciu právnych aktov Únie, na ktoré sa vzťahuje.

Strojové zariadenia

MR

- Nariadenie o strojových zariadeniach 2023/1230) (Machine Regulation, MR) – od januára 2027
- V prílohe III stanovuje základné požiadavky na zdravie a bezpečnosť, pričom sa zaoberá aj rizikami kybernetickej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť.
- CRA aj MR stanovujú pravidlá pre uvádzanie určitých výrobkov na trh. Kým CRA sa vzťahuje na výrobky s digitálnymi prvkami, MR sa vzťahuje na stroje a súvisiace výrobky, s určitými výnimkami.
- CRA stanovuje v prílohe I základné požiadavky na kybernetickú bezpečnosť výrobkov s digitálnymi prvkami. MR stanovuje v prílohe III základné požiadavky na zdravie a bezpečnosť strojov a súvisiacich výrobkov, pričom sa zaoberá aj rizikami kybernetickej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť (t. j. príloha III, oddiely 1.1.9 a 1.2.1).
- Výrobok môže byť zároveň výrobkom s digitálnymi prvkami v zmysle CRA, ako aj strojom alebo súvisiacim výrobkom v zmysle MR. Postupy posudzovania zhody, ako sú stanovené individuálne v CRA aj v MR.
- Napríklad: určitý typ strojového zariadenia v zmysle MR, ktoré sa môže používať napríklad na balenie zeleniny pre supermarkety, môže obsahovať hardvér a softvér na zabezpečenie jeho fungovania. V tomto zmysle môže byť strojové zariadenie na balenie potravín tiež výrobkom s digitálnymi prvkami v zmysle CRA.

Príloha III MR

1.1.9. Ochrana pred zneužitím

1. **Bezpečné pripojenie a komunikácia -**Pri pripojení iného zariadenia (lokálne aj na diaľku) **nesmie vzniknúť nebezpečná situácia**.
2. **Ochrana kritických HW komponentov (signál/údaje) -** HW dôležitý pre pripojenie/prístup ku **kritickému softvéru** musí byť **primerane chránený** proti náhodnému aj úmyselnému zneužitiu. Ak je relevantné, zariadenie má **zaznamenávať dôkazy o zásahoch** (oprávnených aj neoprávnených).
3. **Ochrana kritického SW a dát -** Kritický softvér a údaje musia byť **jasne identifikované** a **chránené** pred zneužitím (náhodným/úmyselným).
4. **Identifikácia nainštalovaného SW potrebného pre bezpečnú prevádzku -** Zariadenie musí obsahovať **identifikáciu bezpečnostne nevyhnutného softvéru** a tieto informácie musia byť **kedykoľvek ľahko dostupné**.
5. **Audit/logovanie zásahov do softvéru -** Zariadenie má **zaznamenávať dôkazy** o zásahoch do SW, jeho úpravách alebo zmene konfigurácie (oprávnené aj neoprávnené).

Príloha III MR

- **1.2.1. Bezpečnosť a spoľahlivosť ovládacích systémov**
- Ovládacie systémy musia byť navrhnuté tak, aby predchádzali nebezpečným situáciám.
- **Odolnosť a bezpečné zlyhanie (fail-safe)** - Odolnosť voči namáhaniu a vonkajším vplyvom (vrátane predvídateľných úmyselných útokov). Porucha HW / logiky ani chyby logiky nesmú viesť k nebezpečným situáciám. Predvídateľná ľudská chyba nesmie viesť k nebezpečným situáciám.
- **Limity bezpečnostných funkcií a zákaz nebezpečných úprav** - Limity sa určia v posúdení rizík výrobcom. Nesmú byť umožnené zmeny nastavení/pravidiel zariadením ani obsluhou (ani počas „učenia"), ak by mohli vytvoriť nebezpečnú situáciu.
- **Povinné logovanie preukázania zhody** - Sledovací log zásahov a informácie o verziách bezpečnostného softvéru nahrávaných po uvedení na trh/prevádzky. Uchovanie 5 rokov od nahratia, iba na účely preukázania zhody na odôvodnenú žiadosť orgánu.
- **Bezdrôtové ovládanie** - Chyba komunikácie/pripojenia ani chybné pripojenie nesmie spôsobiť nebezpečnú situáciu.

AI produkty

AI Akt

- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 (AI akt)**
- Upravuje bezpečnosť, dôveryhodnosť a riadenie rizík AI systémov a modelov AI pre všeobecné účely. Zameriava sa na klasifikáciu rizika (zakázané / vysokorizikové / iné ako vysokorizikové), súlad, kvalitu údajov, transparentnosť, ľudský dohľad, presnosť, spoľahlivosť a kybernetickú bezpečnosť (čl. 15).
- Článok 12 rieši situáciu, keď: produkt s digitálnymi prvkami = zároveň vysokorizikový AI systém
- Produkt sa považuje za spĺňajúci požiadavky KB podľa AI Aktu (čl. 15 AI Akt), ak spĺňa základné požiadavky CRA (Príloha I) Požiadavky AI Aktu na presnosť a robustnosť zostávajú nedotknuté.
- Pri posudzovaní zhody sa uplatní postup podľa čl. 43 AI Aktu. AI notifikovaná osoba môže kontrolovať aj CRA požiadavky.
- Výnimka – dôležité a kritické produkty alebo produkty podliehajúce európskej certifikácii a zároveň ide o vysokorizikový AI systém, potom musia absolvovať postup posudzovania zhody podľa CRA.
- AI Akt kladie väčšinu požiadaviek vrátane kybernetickej bezpečnosti len na vysokorizikové AI systémy.
- CRA sa týka všetkých produktov s digitálnymi prvkami vrátane tých ktoré integrujú AI alebo sú systémom AI , ktorý bez ohľadu na kategóriu rizikovosti

Bezpečnosť výrobkov (safety)

GPSR

- Všeobecné nariadenie o bezpečnosti výrobkov (EÚ) 2023/9882 (GPSR)
- „bezpečný výrobok" je akýkoľvek výrobok, ktorý za bežných alebo racionálne predvídateľných podmienok používania, vrátane skutočného trvania používania, nepredstavuje žiadne riziko alebo len minimálne riziká zlučiteľné s používaním výrobku, ktoré sa považujú za prijateľné a sú v súlade s vysokou úrovňou ochrany zdravia a bezpečnosti spotrebiteľov;
- CRA a GPSR stanovujú pravidlá pre uvádzanie výrobkov na trh, ale majú odlišný rozsah pôsobnosti, pokiaľ ide o výrobky a aspekty, na ktoré sa vzťahujú, a požiadavky, ktoré stanovujú. Pokiaľ ide o výrobky, na ktoré sa vzťahujú nariadenia, CRA sa vzťahuje len na výrobky s digitálnymi prvkami, zatiaľ čo GPSR sa vzťahuje na všetky spotrebné výrobky, pokiaľ neexistujú osobitné predpisy s rovnakým cieľom v rámci práva Únie, ktoré upravujú bezpečnosť príslušných výrobkov. GPSR stanovuje bezpečnostné požiadavky na výrobky.
- Výrobok s digitálnymi prvkami môže musieť spĺňať požiadavky CRA aj GPSR. Ak výrobok s digitálnymi prvkami predstavuje aj iné riziká ako riziká kybernetickej bezpečnosti, uplatní sa primárne GPSR (Článok 11 CRA Všeobecná bezpečnosť produktov)
- Napríklad: inteligentné detské pestúnky s kamerou a Wi-Fi pripojením. CRA (Kybernetická bezpečnosť): Keďže ide o produkt s digitálnymi prvkami (obsahuje softvér, pripája sa na sieť), musí spĺňať požiadavky na zabezpečenie proti kybernetickým útokom, šifrovanie dát a pravidelné bezpečnostné aktualizácie. GPSR (Fyzická bezpečnosť): Ako spotrebný výrobok, ktorý používajú spotrebitelia, musí byť bezpečný aj po fyzickej stránke (napríklad aby sa káble neprehrievali, plasty neboli toxické, kamera nepredstavovala riziko udusenia).

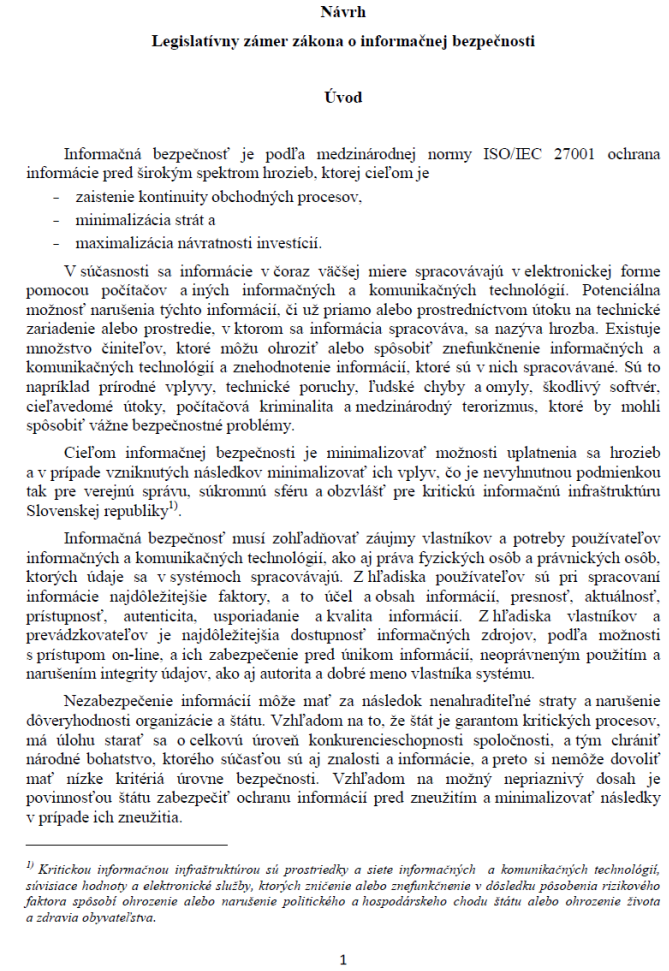
KYBERNETICKÁ BEZPEČNOSŤ VEREJNEJ SPRÁVY

CUSEC

PLÁN OBNOVY

Historický vývoj

- **Legislatívny zámer zákona o informačnej bezpečnosti**
  - rok 2010
  - cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru SR
  - kategorizácia informačných systémov verejnej správy
  - jednotka pre riešenie počítačových incidentov (CSIRT.SK) v SR
  - štandardizácia



Návrh

Legislatívny zámer zákona o informačnej bezpečnosti

Úvod

Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je

- zaistenie kontinuity obchodných procesov,
- minimalizácia strát a
- maximalizácia návratnosti investícií.

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy.

Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky[1)].

Informačná bezpečnosť musí zohľadňovať záujmy vlastníkov a potreby používateľov informačných a komunikačných technológií, ako aj práva fyzických osôb a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie faktory, a to účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejšia dostupnosť informačných zdrojov, podľa možnosti s prístupom on-line, a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Nezabezpečenie informácií môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie a štátu. Vzhľadom na to, že štát je garantom kritických procesov, má úlohu starať sa o celkovú úroveň konkurencieschopnosti spoločnosti, a tým chrániť národné bohatstvo, ktorého súčasťou sú aj znalosti a informácie, a preto si nemôže dovoliť mať nízke kritériá úrovne bezpečnosti. Vzhľadom na možný nepriaznivý dosah je povinnosťou štátu zabezpečiť ochranu informácií pred zneužitím a minimalizovať následky v prípade ich zneužitia.

[1)] *Kritickou informačnou infraštruktúrou sú prostriedky a siete informačných a komunikačných technológií, súvisiace hodnoty a elektronické služby, ktorých zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu alebo ohrozenie života a zdravia obyvateľstva.*

1

Zákon o ITVS

- **Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** (**zákon o ITVS**)
- je sektorová právna úprava (lex specialis)
- cieľom zákona o ITVS je komplexné a jednotné riadenie IT - od plánovania a organizácie cez implementáciu a prevádzku až po monitoring a hodnotenie
- zákon sa nezameriava výlučne na kybernetickú bezpečnosť, ale na celý životný cyklus riadenia ITVS
- ustanovuje jednotné vedenie a riadenie IT vo verejnej správe
- **IT** je na účely tohto zákona prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, **najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby**.
- **ITVS** je **informačná technológia v pôsobnosti správcu** podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú **aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe**.

Bezpečnosť informačných technológií verejnej správy

- §§ 18 - 26
- Povinnosti správcu
- Základná: prijať a realizovať bezpečnostné opatrenia vo vzťahu k ISVS
- Plánovanie a organizácia: najmä zaviesť a udržiavať ISMS, schváliť bezpečnostnej stratégie informácií o zaznamenaných závažných kybernetických bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného výskytu, návrhu opatrení, udržiava bezpečnostnú dokumentáciu, kontrola a hodnotenie súladu, určí osobu zodpovednú za bezpečnosť ISVS
- Obstarávanie a implementácia: najmä určí bezpečnostné požiadavky na ISVS vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania ISVS, vrátane vypracovania bezpečnostnej dokumentácie a bezpečnostného projektu pre ISVS
- Prevádzka , servis a podpora: najmä vykoná bezpečnostné testovanie ISVS, ktorý má rozhranie s verejnou sieťou internet a ktorý spracúva osobitné kategórie osobných údajov alebo chránené/prísne chránené informácie, zabezpečí nepretržitý monitoring informačného systému verejnej správy, 6. zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch

Bezpečnostné opatrenia

- Vyhláška ÚPVII **č. 179/2020 Z. z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- (Návrh)Vyhláška MIRRI z … 2026, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- Zmena koncepcie, s cieľom priblížiť sa k Vyhláške NBÚ č. 227/2025

Nová vyhláška (návrh)

- zaradenie orgánov riadenia a správcov ITVS do kategórií jednotlivých oblastí bezpečnostných opatrení kybernetickej bezpečnosti a informačnej bezpečnosti,
- vzorový výpočet aktív
- obsah bezpečnostných opatrení, rozsah bezpečnostných opatrení pre jednotlivé kategórie vo vzťahu k ITVS
- obsah a štruktúru bezpečnostného projektu
- rozsah zasielaných systémových informácií o aktívach, kontaktných bodoch a evidencii kybernetických bezpečnostných incidentov
- klasifikačná schéma informácií

Nová vyhláška (návrh)

- Minimálne bezpečnostné opatrenia sú rozdelené do Kategórie I, Kategórie II a Kategórie III
- Prekategorizovanie niektorých subjektov smerom do kategórie I
- Minimálne bezpečnostné opatrenia Kategórie I sa vzťahujú na

a) obec do 6000 obyvateľov,

b) obec so štatútom mesta do 6000 obyvateľov,

c) právnickú osobu podľa § 5 ods. 2 písm. e) zákona s výnimkou právnických osôb, ktoré sú kritickým subjektom podľa zákona č. 367/2024 Z.z. o KI

d) osobu podľa § 5 ods. 2 písm. g) zákona,

e) záujmové združenie právnických osôb podľa § 5 ods. 2 písm. h) zákona.

Príloha č.2 Minimálne bezp. opatrenia(návrh)

Položka	Bezpečnostné opatrenia pre organizáciu a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti prijíma správca informačných technológií verejnej správy tak, že:	Kat. I	Kat. II	Kat. III
1.	je určená osoba zodpovedná za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, ktorá je nezávislá od štruktúry riadenia prevádzky a vývoja služieb informačných technológií verejnej správy, a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO
2.	manažér kybernetickej bezpečnosti predkladá návrhy bezpečnostných opatrení a oznamuje informácie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti priamo štatutárnemu orgánu správcu alebo ním poverenému riadiacemu pracovníkovi		ÁNO	ÁNO
3.	je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k ITVS a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a ITVS podľa príslušnej bezpečnostnej politiky	ÁNO	ÁNO	ÁNO
4.	je určená osoba, ktorá je zodpovedná za riešenie kybernetických bezpečnostných incidentov, ako aj prijímanie a evidenciu hlásení voči príslušným regulátorom	ÁNO	ÁNO	ÁNO
5.	je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti a informačnej bezpečnosti, vrátane pridelenia úloh, rolí ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie		ÁNO	ÁNO

Ďalšie povinnosti orgánu riadenia

Aktuálne znenie rozlišuje medzi tým či je orgán riadenia zároveň PZS alebo nie:

- Hlásenie kybernetických bezpečnostných incidentov
- poskytnúť MIRRI súčinnosť a spoluprácu pri plnení jeho úloh a plniť pokyny MIRRI pri výkone jeho oprávnení podľa § 23a,
- zasielať najmenej 1x do roka orgánu vedenia zoznam aktív
- zasielať spôsobom VJ CSIRT určené systémové informácie
- zverejniť na svojom webovom sídle pravidlá na oznamovanie zraniteľností

- prijať alebo upraviť bezpečnostné opatrenia, po incidente, penteste, zistenej zraniteľnsoti a oznámiť VJ CSIRT prijaté bezpečnostné opatrenia,
- viesť evidenciu kybernetických bezpečnostných incidentov, postupov na riešenie kybernetických bezpečnostných incidentov,
- určiť a zverejniť na svojom hlavnom webovom sídle kontaktné údaje na kontaktný bod alebo primeraný počet kontaktných bodov na nahlasovanie kybernetického bezpečnostného incidentu.

VJ CSIRT

- **Dve lokality**
  - Bratislava
  - Košice
- **Medzinárodná spolupráca**
  - FIRST (USA)
  - TF CSIRT / Trusted Introducer (**certified team**)
  - ENISA – CSIRTs Network (EÚ) (**ENISA Expert level team**)
  - National coordinator haveibeenpwned.com
- **Vnútroštátna spolupráca**
  - SK-CERT a iné CSIRT tímy
  - Univerzity (UPJŠ KE, STU BA, TUKE, APZ)
  - Spolupráca a súčinnosť (PZ SR, SIS, CKO)

VJ CSIRT (MIRRI)

- metodicky usmerňuje správcov a zvyšuje povedomia správcov a verejnosti v oblasti kybernetickej bezpečnosti vo verejnej správe,
- na žiadosť orgánu riadenia môže vykonať hodnotenie zraniteľností alebo posúdenie bezpečnosti
- na žiadosť správcu vykonáva činnosti nepretržitého monitorovania ITVS v jeho správe,
- vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby ITVS poskytovaných cez internet alebo prostredníctvom Govnetu,
- s predchádzajúcim súhlasom správcu vykonáva hodnotenie zraniteľnosti služby, ktoré boli zistené pri pravidelnom neinvazívnom hodnotení zraniteľnosti
- zbiera, spracúva a vyhodnocuje systémové informácie správcov,
- môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia kybernetického bezpečnostného incidentu, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti.

Služby VJ CSIRT

CSIRT.SK

- Od posúdenia zraniteľnosti k CTI a výskumu zraniteľností

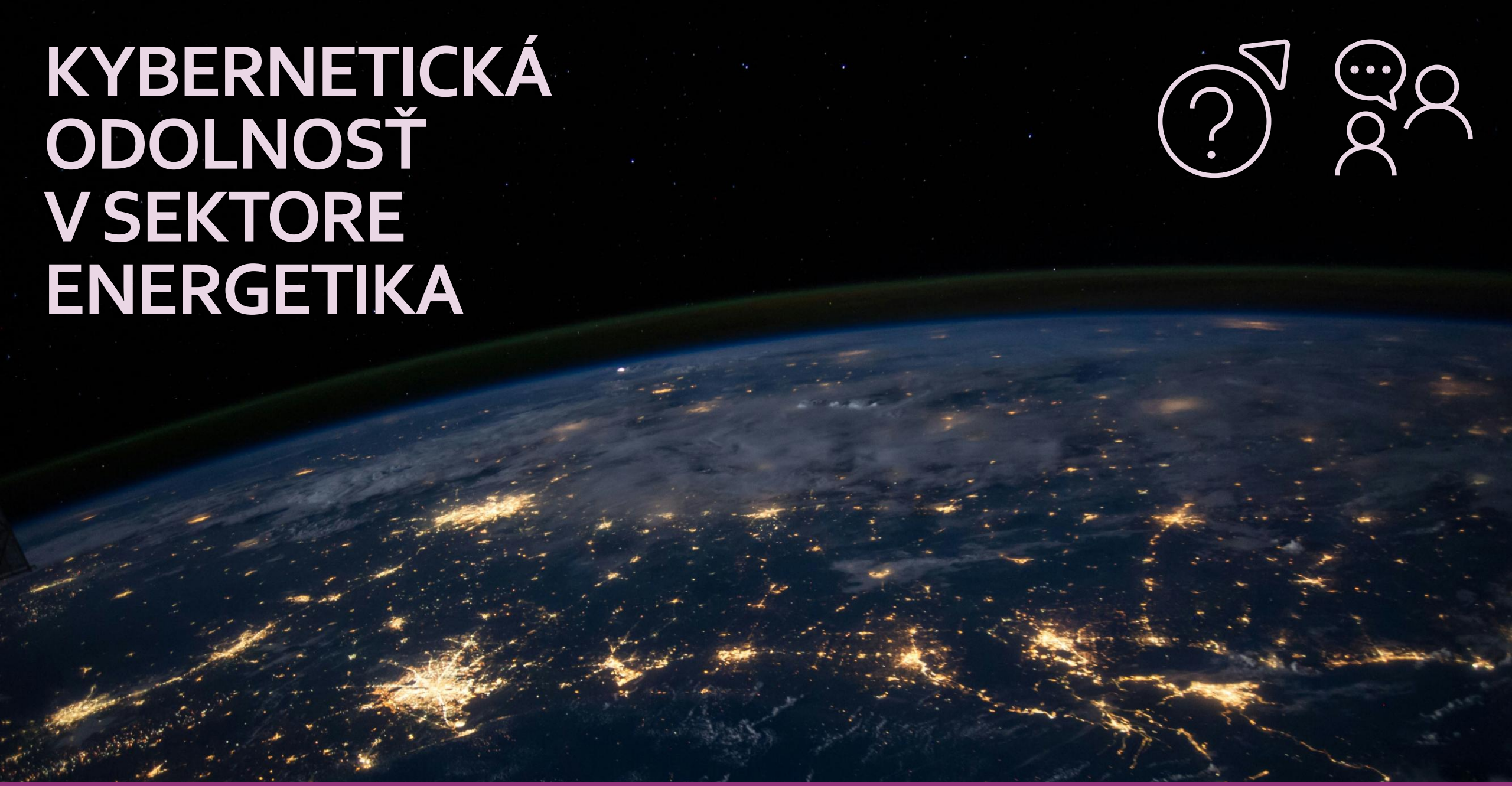
- Poloautomatické hodnotenie zraniteľností (Achilles)
- Informácie o hrozbách a korelácia údajov (Afrodita/MISP)
- Penetračné testovanie a výskum zraniteľností (Ares)

MISP AFRODITA

ARES by CSIRT.SK ATTACK TO PROTECT

ACHILLES

KYBERNETICKÁ ODOLNOSŤ V SEKTORE ENERGETIKA



CUSEC

PLÁN OBNOVY

NCCS a Elektrická energia

- Nariadenie (EÚ) 2019/943 z 5. júna 2019 o vnútornom trhu s elektrinou (ciele energetickej únie, integrovaný trh s elektrinou, pravidlá pre cezhraničné toky elektriny, etc.) Nariadenie (EÚ) 2019/943 dopĺňa smernicu NIS2 a nariadenie (EÚ) 2019/941 stanovením osobitných pravidiel pre odvetvie elektrickej energie na úrovni Únie.
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 z 5. júna 2019 o pripravenosti na riziká v sektore elektrickej energie (pravidlá spolupráce medzi členskými štátmi v záujme prevencie kríz dodávok elektriny, prípravy). Dopĺňa smernicu NIS2 tým, že sa ním zabezpečuje riadne určenie kybernetických incidentov v odvetví elektrickej energie ako rizika a riadne zohľadnenie opatrení prijatých na ich riešenie v plánoch pripravenosti na riziká.
- **Network Code on Cybersecurity (NCCS) - Delegované nariadenie Komisie (EÚ) 2024/1366, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 stanovením sieťového predpisu pre odvetvové pravidlá týkajúce sa aspektov kybernetickej bezpečnosti cezhraničných tokov elektriny**
- Týmto delegovaným nariadením sa ďalej dopĺňajú ustanovenia smernice NIS2 týkajúce sa odvetvia elektrickej energie vo všetkých prípadoch, keď ide o cezhraničné toky elektriny.

NCCS vs NIS2

- Uplatňovanie NCCS závisí od vnútroštátnej transpozície EÚ NIS2 a EÚ NCCS nadväzuje na NIS2 tým, že špecifikuje povinnosti špecifické pre daný sektor a opiera sa o kľúčové prvky NIS2 (určenie subjektov, orgánov dohľadu, rámcov riadenia rizík), ktoré musia existovať vo vnútroštátnom práve.
- Recitál 15 NCCS: Súlad subjektu s požiadavkami na riadenie kybernetickobezpečnostných rizík stanovenými v NCCS by príslušné orgány podľa smernice NIS2 mohli považovať za zabezpečovanie dodržiavania zodpovedajúcich požiadaviek stanovených v uvedenej smernici, resp. naopak.

NCCS

- V kontexte prepojených digitalizovaných elektrizačných sústav nemožno považovať prevenciu a riadenie krízy dodávok elektriny súvisiacej s kybernetickými útokmi za výlučne vnútroštátnu úlohu.
- Posúdenia kybernetickobezpečnostných rizík na úrovni Únie, členských štátov, regiónov a subjektov v tomto nariadení možno obmedziť na riziká vyplývajúce z kybernetických útokov v zmysle nariadenia DORA, čím sa vylúčia napríklad fyzické útoky, prírodné katastrofy a výpadky v dôsledku straty zariadení alebo ľudských zdrojov (ktoré sú už súčasťou nariadenia 2019/941, 2017/1485 a smernice CER)
- Pojem „subjekty s veľkým a kritickým vplyvom" je základom na vymedzenie rozsahu subjektov, na ktoré sa budú vzťahovať povinnosti podľa NCCS - sú predovšetkým subjekty, ktoré majú priamy vplyv na cezhraničné toky elektriny v EÚ.
- Agentúra Európskej únie pre spoluprácu regulačných orgánov v oblasti energetiky (ACER).
- Prevádzkovatelia prenosových sústav (PPS) a prevádzkovatelia distribučných sústav (PDS) majú osobitné povinnosti v oblasti kybernetickej bezpečnosti. Ich európske združenia, konkrétne Európska sieť PPS pre elektrinu (ENTSO pre elektrinu) a Európsky subjekt PDS (subjekt PDS EÚ) podporujú kybernetickú bezpečnosť v spolupráci s príslušnými orgánmi a regulovanými subjektmi.

Subjekty s veľkým vplyvom alebo s kritickým vplyvom

Ak sú identifikované ako subjekty s veľkým vplyvom alebo subjekty s kritickým vplyvom v súlade s článkom 24 NCCS:

- elektroenergetické podniky,
- nominovaní organizátori trhu s elektrinou,
- organizované miesta obchodovania alebo „organizované trhy“,
- poskytovatelia kritických služieb IKT,
- ENTSO pre elektriny, subjekt PDS EÚ,
- samostatné subjekty zúčtovania,
- prevádzkovatelia nabíjacích bodov,
- regionálne koordinačné centrá,
- poskytovatelia riadených bezpečnostných služieb

Index ECII

„Index vplyvu na kybernetickú bezpečnosť elektrizačnej sústavy“ (ECII) je index alebo klasifikačná stupnica, ktorá zoraďuje možné dôsledky kybernetických útokov na obchodné procesy v rámci cezhraničných tokov elektriny

V metodikách posudzovania kybernetickobezpečnostných rizík na úrovni Únie sa opisuje, ako budú vymedzené hodnoty ECII, pokiaľ ide o prahové hodnoty veľkého a kritického vplyvu.

ECII a prahové hodnoty veľkého a kritického vplyvu, príslušné orgány používajú podľa článku 24 ods. 1 a 2 na identifikáciu subjektov s veľkým a kritickým vplyvom

Tabuľka 1: Predbežné ECII pre subjekty. Všetky ECII sa merajú v megawattoch (MW).

1. Prevádzkovatelia distribučnej sústavy - Maximálne zaťaženie PDS za predchádzajúci rok
2. Prevádzkovatelia prenosovej sústavy - Najvyššia z nasledujúcich hodnôt: maximálne celkové zaťaženie za predchádzajúci rok; maximálny agregovaný výkon výroby za predchádzajúci rok; maximálny dovoz za predchádzajúci rok; maximálny vývoz za predchádzajúci rok.
3. Výrobcovia - Súčet maximálnej kapacity všetkých výrobných jednotiek prevádzkovaných subjektom na konci predchádzajúceho roka (v MW).

Prahové hodnoty

Tabuľka 2: Predbežné prahové hodnoty.

Členský štát	Prahová hodnota vysokého vplyvu	Prahová hodnota kritického vplyvu
Slovensko	500 MW	3,000 MW
Česko	500 MW	3,000 MW
Poľsko	1,000 MW	3,000 MW

Zdroj: ENTSO: PROVISIONAL ELECTRICITY CYBERSECURITY IMPACT INDEX (ECII)

https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Network%20codes%20documents/NCCS/Provisional%20ECII.pdf

Každý príslušný orgán pomocou ECII a prahových hodnôt veľkého a kritického vplyvu, identifikuje subjekty s veľkým a kritickým vplyvom vo svojom členskom štáte.

Každý príslušný orgán do 9 mesiacov po tom, ako ho ENTSO pre elektrinu a subjekt PDS EÚ informoval o správe o posúdení kybernetickobezpečnostných rizík v celej Únii, a v každom prípade **najneskôr do 13. júna 2028 informuje subjekty uvedené v zozname, že boli identifikované ako subjekty s veľkým alebo kritickým vplyvom v danom členskom štáte.**

Povinnosti pre subjekty

V závislosti od úrovne vplyvu subjektu musia byť zavedené minimálne a pokročilé opatrenia kybernetickej bezpečnosti, a to aj pre dodávateľské reťazce IKT.

Od roku 2027

Riadenie kybernetickej bezpečnosti (čl. 26 – 32) Zavedenie CSMS, vymedzenie rozsahu aktív na základe rizika nachádzajúcich sa v perimetroch veľkého vplyvu a kritického vplyvu, a implementácia minimálnych a pokročilých bezpečnostných kontrol.

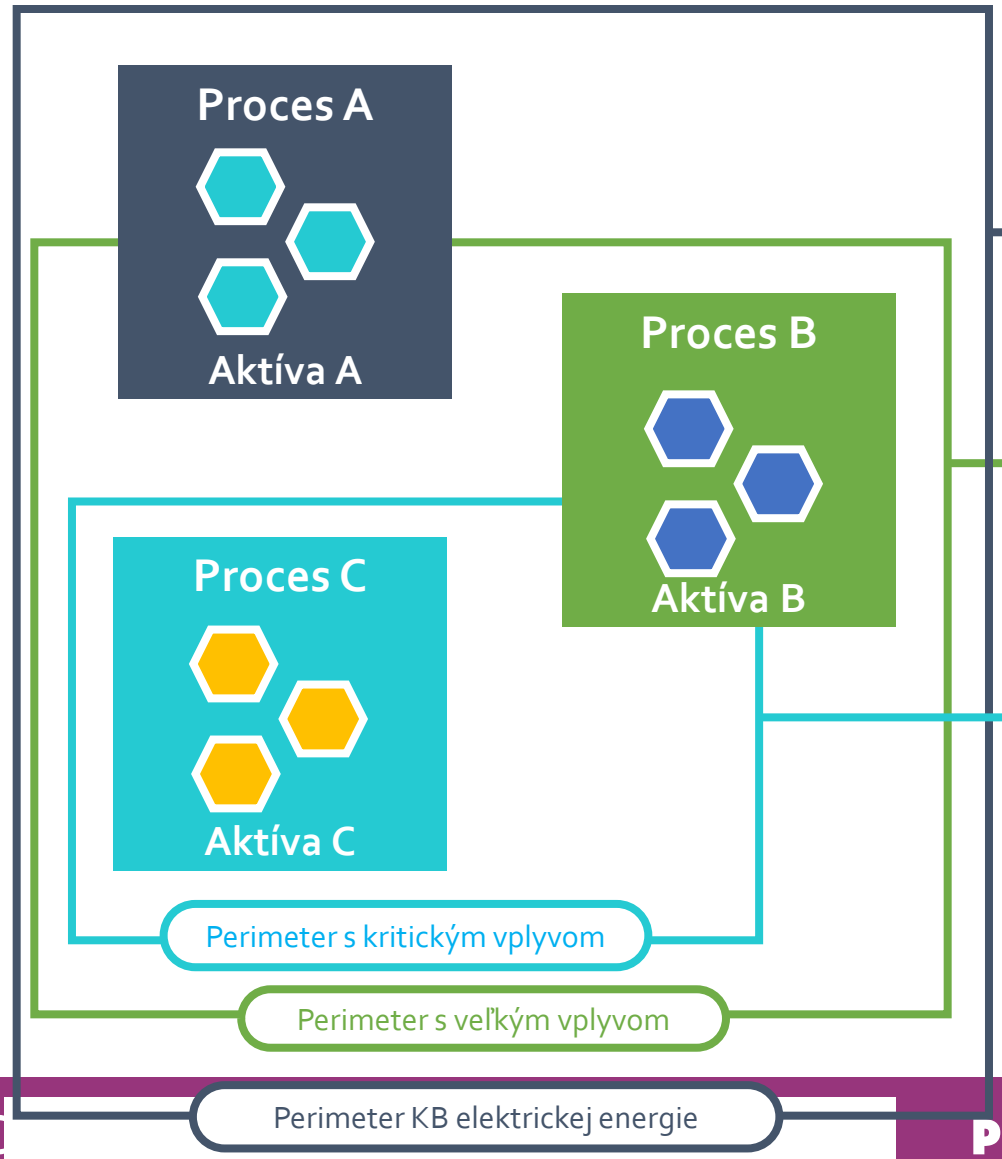
Bezpečnosť dodávateľského reťazca (čl. 33 – 34) Požiadavky na kybernetickú bezpečnosť v procesoch obstarávania a overovanie súladu dodávateľov s predpismi pomocou produktov s certifikáciou bezpečnosti alebo interného zabezpečenia.

Výmena informácií, kyberútoky a krízové riadenie (čl. 37 – 42) Povinnosti včasného varovania, povinné hlásenie a riešenie kybernetických útokov a účasť na koordinovaných postupoch reakcie. Povinnosť mať (aspoň v minimálnom rozsahu) funkcie typu SOC – operačné centrum kybernetickej bezpečnosti

Kybernetickobezpečnostné cvičenia (čl. 43-45) subjekt s kritickým vplyvom do 31. decembra roka po informovaní subjektov s kritickým vplyvom a následne každé tri roky vykoná kybernetickobezpečnostné cvičenie vrátane jedného alebo viacerých scenárov s kybernetickými útokmi, ktoré priamo alebo nepriamo ovplyvňujú cezhraničné toky elektriny a súvisia s identifikovanými rizikami

Spoločný rámec pre kybernetickú bezpečnosť

Zdroj: ENTSOE.eu



Riadenie kybernetickobezp. rizík (čl. 26)

Systém riadenia kybernetickej bezpečnosti (čl. 32)

Overovanie spoločného rámca /aj audit (čl. 31)

Spoločný rámec pre kybernetickú bezpečnosť (čl. 28)

Minimálne kontroly kybernetickej bezpečnosti (čl. 29)

Pokročilé kontroly kybernetickej bezpečnosti (čl. 29)

Matica mapovania na tech. normy (čl. 34)

Oznamovanie kybernetických útokov (čl. 38)

„**kybernetický útok**" je **zlomyseľný incident súvisiaci s IKT** spôsobený prostredníctvom pokusu, ktorého sa dopustil akýkoľvek **aktér hrozby**, o zničenie, odhalenie, zmenu, znefunkčnenie, krádež alebo získanie neoprávneného prístupu k aktívu, alebo o neoprávnené použitie aktíva (odkaz na definíciu podľa nariadenia DORA)

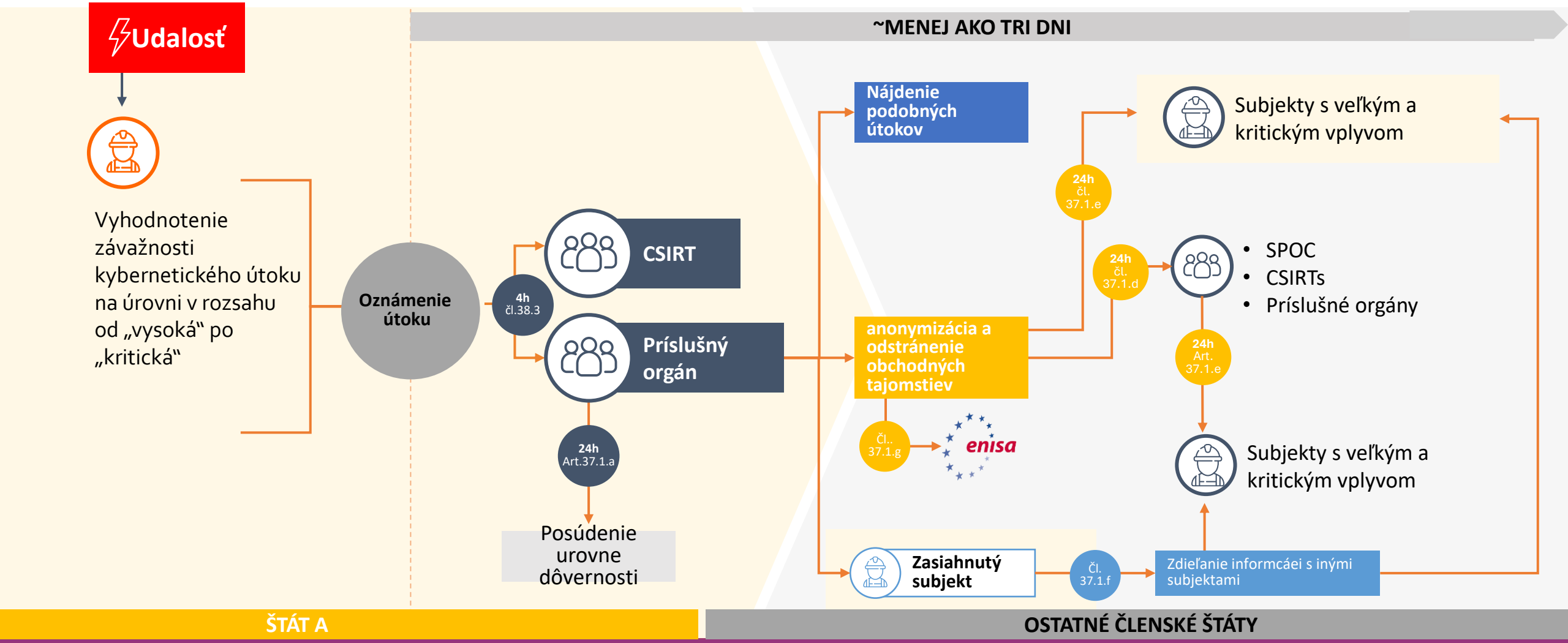
Každý subjekt s kritickým alebo veľkým vplyvom musí **bez zbytočného odkladu, najneskôr do štyroch hodín** od zistenia, že kybernetický útok podlieha oznamovacej povinnosti, poskytnúť relevantné informácie o kybernetickom útoku svojej jednotke CSIRT a príslušnému orgánu.

Podlieha oznamovacej povinnosti, ak zasiahnutý subjekt vyhodnotí závažnosť kybernetického útoku na úrovni **v rozsahu od „vysoká" po „kritická"** na základe metodiky určenia klasifikačnej stupnice kybernetických útokov (5 úrovní klasifikácie, a vychádza z posúdenia týchto parametrov: a) potenciálny vplyv vzhľadom na exponované aktíva a zóny, a b) závažnosť kybernetického útoku)

Ak subjekt **už nahlási významný incident podľa čl. 23 smernice NIS2** a toto hlásenie už obsahuje všetky relevantné údaje, ktoré sa inak vyžadujú aj pri hlásení kybernetického útoku podľa čl. 38 ods. 3 NCCS, tak toto jedno hlásenie sa považuje aj za splnenie povinnosti podľa NCCS

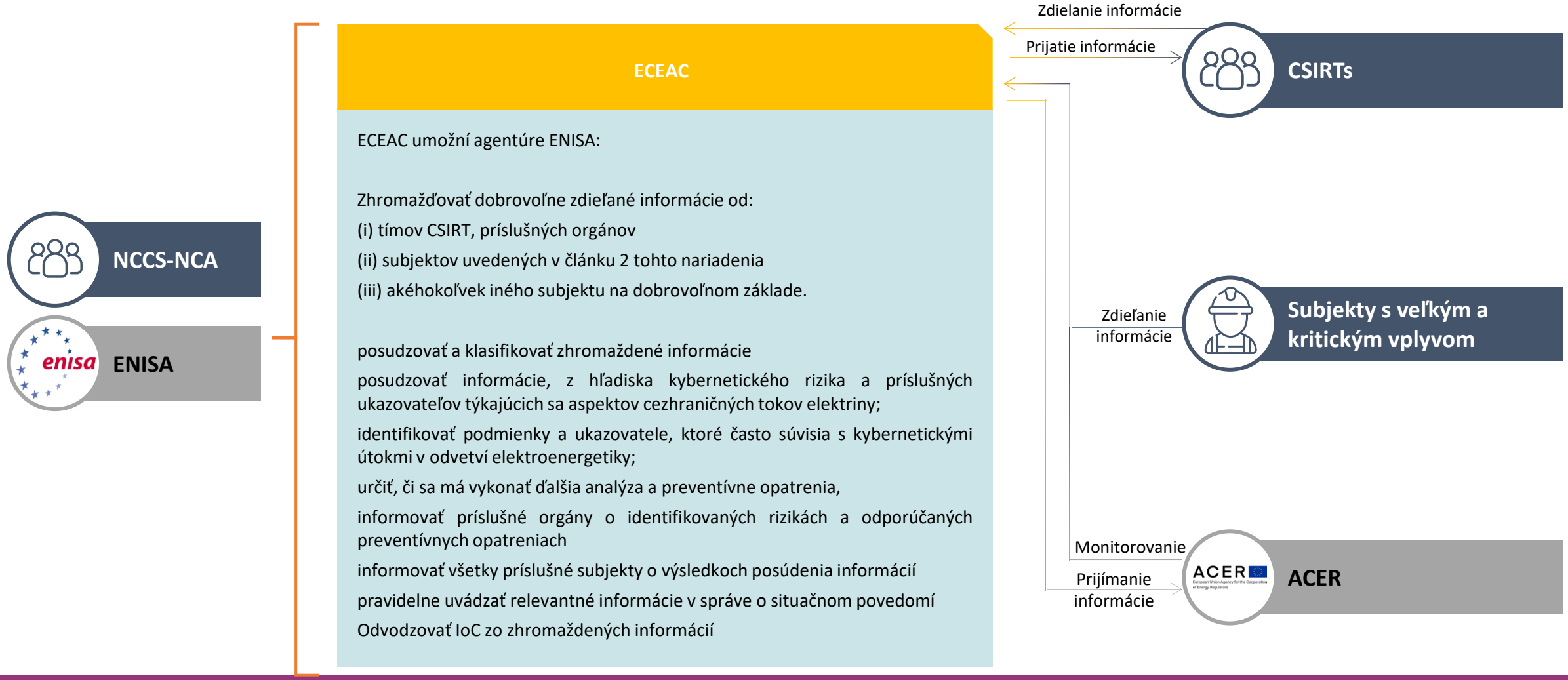
Oznamovanie kybernetických útokov

Zdroj: ENTSOE.eu



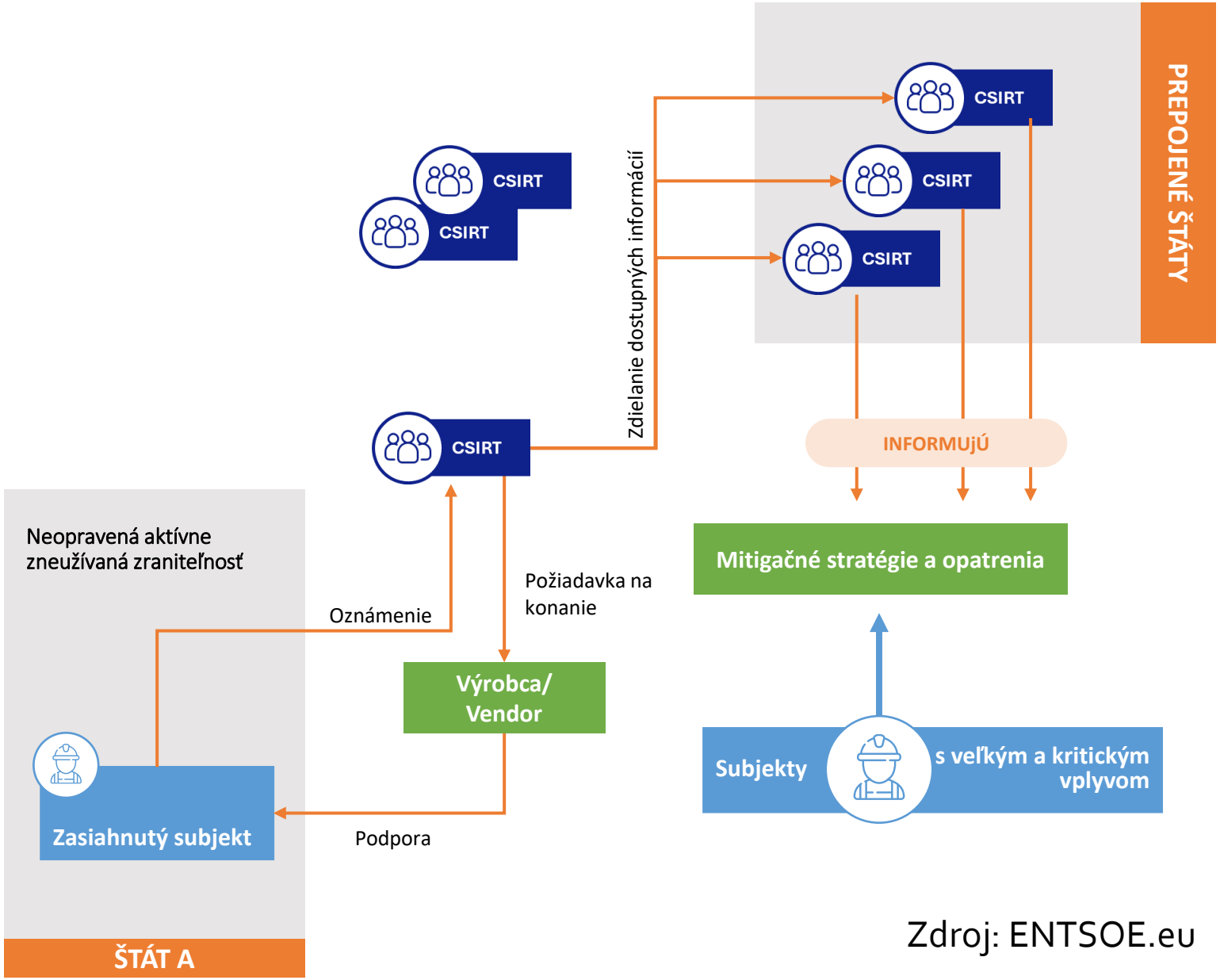
Včasné varovanie v oblasti kybernetickej bezpečnosti elektrizačnej sústavy (ECEAC) (čl. 42)

Zdroj: ENTSOE.eu



Oznamovanie neopravených aktívne zneužívaných zraniteľností

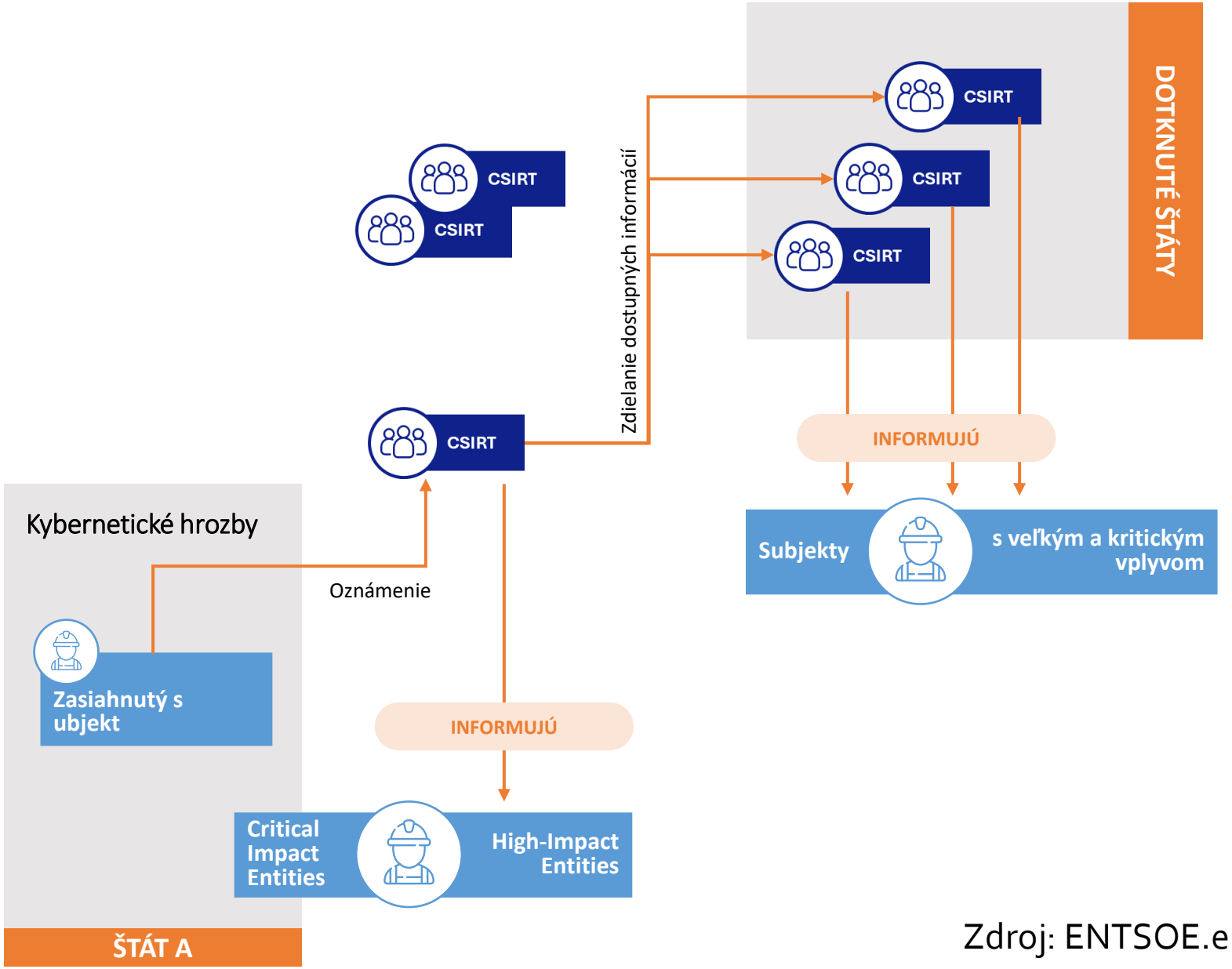
= zraniteľnosť, ktorá ešte nebola zverejnená a opravená a v prípade ktorej existujú spoľahlivé dôkazy o tom, že niekto spustil zlomyseľný kód v systéme bez povolenia vlastníka systému



Zdroj: ENTSOE.eu

Oznamovanie kybernetických hrozieb

ak je splnené aspoň jedno:
a) ide o informácie, ktoré sú relevantné pre iné subjekty
b) identifikované TTP použité v súvislosti s útokom vedú k informáciám, ako sú kompromitované URL alebo IP adresy, haše, iné atribúty, pomocou ktorých možno zistiť kontext a súvislosti útoku;
c) možno ďalej posúdiť a dať do súvislosti s ďalšími informáciami, ktoré poskytnú poskytovatelia služieb alebo tretie strany.



Zdroj: ENTSOE.eu

Minimálne a pokročilé kontroly v dodávateľskom reťazci (čl. 33)

Minimálne kontroly v dodávateľskom reťazci musia zahŕňať:

- Odporúčania pre obstarávanie produktov, služieb a procesov IKT
- Overovanie pozadia dodávateľovho materiálu
- Životný cyklus vývoja bezpečných systémov
- Zero trust
- Bezpečný prístup dodávateľa k aktívam
- Vysledovateľnosť uplatňovania požiadaviek
- Podpora bezpečnostných aktualizácií
- Monitorovanie, poreskúmavanie a audit KB
- Posúdenie rizikového profilu dodávateľa
- Zmluvné záväzky (aj pri nežiaducich udalostiach a okolnostiach, ako je vypovedanie zmluvy a jej prenos v prípade nedbanlivosti zmluvného partnera)

Pokročilé kontroly v dodávateľskom reťazci zahŕňajú:

Overovanie špecifikácií kybernetickej bezpečnosti produktov, služieb a procesov IKT prostredníctvom:

- Európskych systémov certifikácie kybernetickej bezpečnosti
- Overovacích činností vybraných subjektom

NEZÁVÄZNÉ

- **Odporúčania týkajúce sa obstarávania kybernetickej bezpečnosti** *(čl. 35)*
- **Usmernenie k používaniu európskych systémov certifikácie kybernetickej bezpečnosti produktov, služieb a procesov IKT** *(čl. 36)*

Zdroj: ENTSOE.eu

KYBERNETICKÁ ODOLNOSŤ V SEKTORE DOPRAVA

CUSEC

PLÁN OBNOVY

Civilné letectvo

- Agentúra Európskej únie pre bezpečnosť letectva („EASA“)
- **Nariadenie (EÚ) 2022/1645 a vykonávacie nariadenie (EÚ) 2023/203,** súhrnne známe ako **Part-IS,** ktorými sa zavádzajú záväzné požiadavky na informačnú bezpečnosť v celom sektore civilného letectva EÚ a nariaďuje sa **štruktúrovaný systém riadenia informačnej bezpečnosti („ISMS“)** v súlade s cieľmi bezpečnosti letectva.
- Medzi subjekty (nariadenie Komisie (EÚ) 2022/1645), patria najmä prevádzkovatelia letísk, projekčné a výrobné organizácie a poskytovatelia služieb riadenia prevádzky na odbavovacej ploche. Pre tieto subjekty sa časť IS uplatňuje **od 16. októbra 2025.**
- Subjekty (nariadenie Komisie (EÚ) 2023/203), zahŕňajú organizácie údržby a organizácie riadenia zachovania letovej spôsobilosti, komerčných aj nekomerčných leteckých prevádzkovateľov, schválené výcvikové organizácie a prevádzkovateľov výcvikových zariadení na simuláciu letu, poskytovateľov leteckých navigačných služieb, výcvikové strediská riadiacich letovej prevádzky a príslušné orgány vrátane samotnej agentúry EASA. Pre tieto subjekty sa časť IS uplatňuje o**d 22. februára 2026.**

Part-IS.I.OR (nariadenie 2023/203)

PRÍLOHA II INFORMAČNÁ BEZPEČNOSŤ – ORGANIZAČNÉ POŽIADAVKY [ČASŤ IS.I.OR]

IS.I.OR.100. Rozsah pôsobnosti

IS.I.OR.200. Systém riadenia informačnej bezpečnosti (ISMS)

IS.I.OR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

IS.I.OR.210. Riešenie rizika v oblasti informačnej bezpečnosti

IS.I.OR.215. Systém interného nahlasovania informačnej bezpečnosti

IS.I.OR.220. Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a obnova

IS.I.OR.225. Reakcia na zistenia oznámené príslušným orgánom

IS.I.OR.230. Systém externého nahlasovania informačnej bezpečnosti

IS.I.OR.235. Zadávanie činností riadenia informačnej bezpečnosti

IS.I.OR.240. Požiadavky na personál

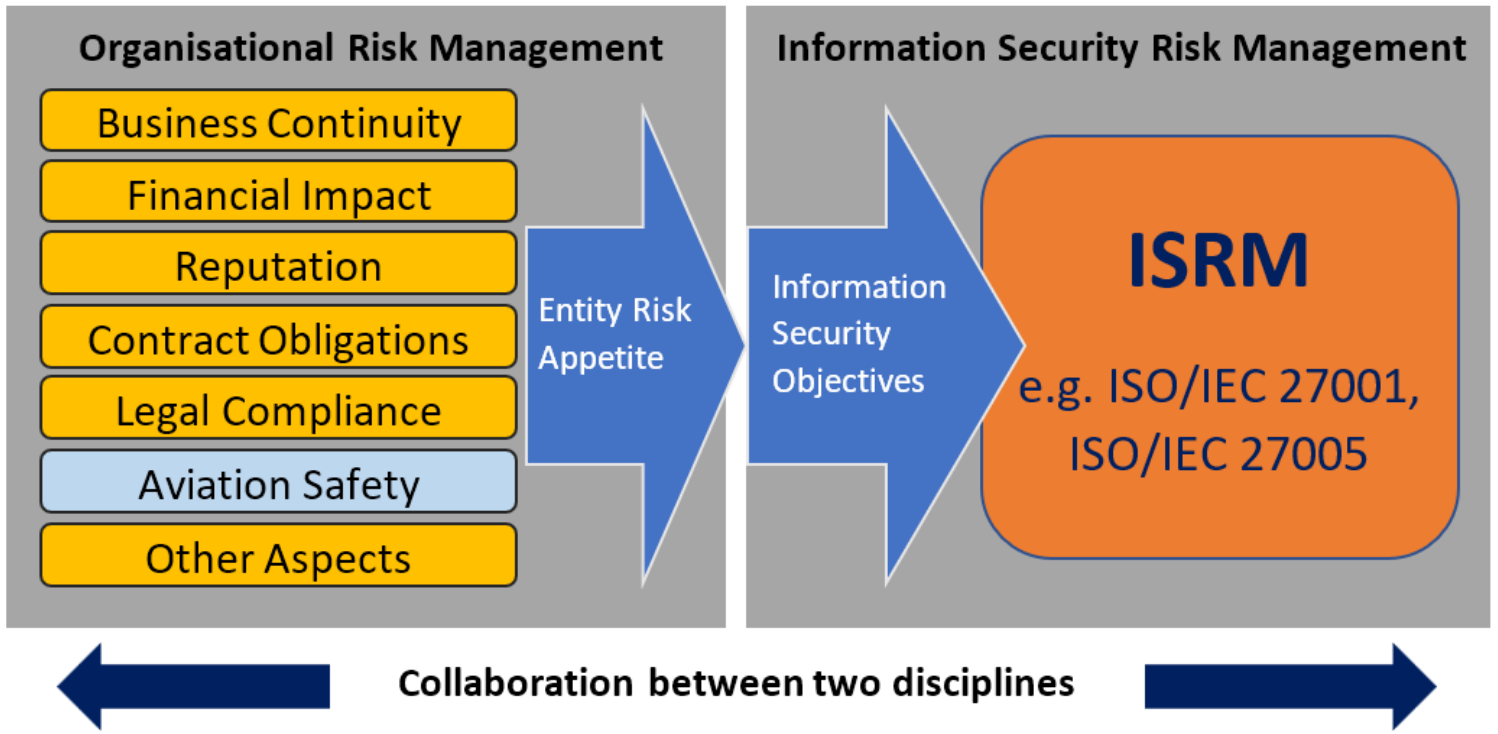
IS.I.OR.245. Vedenie záznamov

IS.I.OR.250. Príručka riadenia informačnej bezpečnosti (ISMM)

IS.I.OR.255. Zmeny systému riadenia informačnej bezpečnosti

IS.I.OR.260. Neustále zlepšovanie

ISO27001 vs. Part-IS



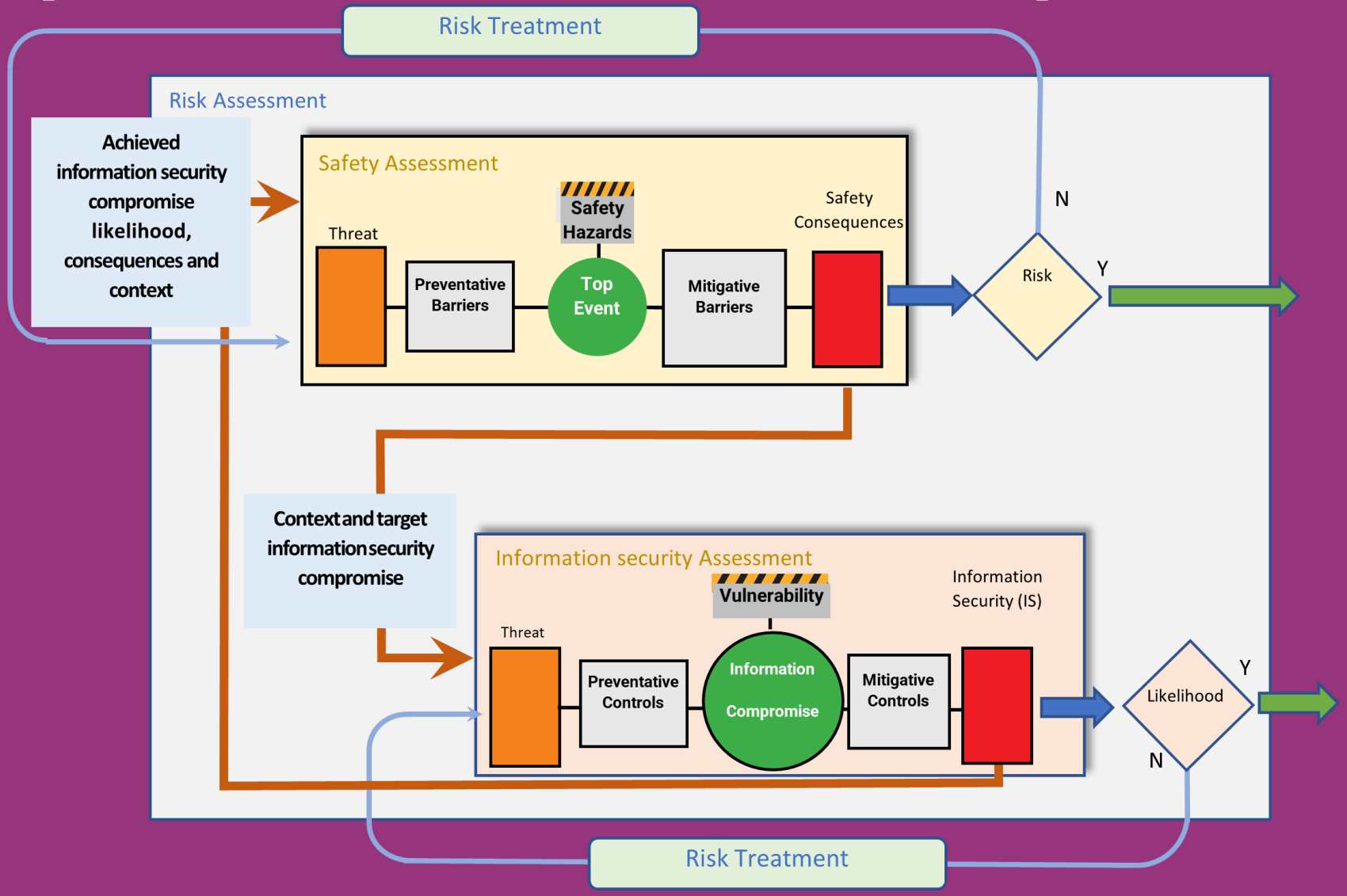
Zdroj: EASA

Safety + Security

V letectve sa bezpečnosť tradične zameriavala na fyzické riziká – výkon lietadla, ľudský faktor a prevádzkové postupy. Dnes však môžu mať zraniteľnosti priame bezpečnostné dôsledky. Kybernetický útok na softvér na plánovanie letov by napríklad mohol viesť k meškaniam, nesprávnemu smerovaniu a iným závažným následkom.

Použitie pojmu „informačná bezpečnosť" v časti IS na rozdiel od pojmu „kybernetická bezpečnosť" je zámerné. Táto terminológia je zvolená tak, aby zahŕňala širšiu škálu rizík spojených s informačnými systémami, nad rámec digitálnej sféry a zahŕňa aj analógové hrozby.

Bezpečnosť letectva a hrozby IB



Zdroj: EASA

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CUSEC

Part-IS vs NIS2

- Časť IS agentúry EASA predstavuje zásadný posun tým, že vyžaduje, aby sa informačná bezpečnosť považovala za základnú súčasť bezpečnosti (safety) letectva. Regulované subjekty by sa mali posunúť od vnímania kybernetickej bezpečnosti ako samostatného IT problému k integrácii štruktúrovaného systému ISMS do existujúcich protokolov prevádzkovej bezpečnosti.
- Part_IS je nariadenie priamo uplatniteľné v celej EÚ bez potreby národnej transpozície.
- Part-IS však **nie je lex specialis k NIS2/ZoKB,** podľa Európskej komisie nespadá do kategórie „lex specialis". Je to spôsobené najmä **špecifickým rozsahom pôsobnosti právnych predpisov o systémoch riadenia informačnej bezpečnosti (ISMS) v porovnaní so širším prístupom smernice NIS 2/ZoKB**.
- Súlad s časťou IS nezbavuje subjekty kľúčové alebo dôležité podľa smernice NIS2/ZokB od povinnosti dodržiavať požiadavky smernice NIS 2/ZoKB.

Ransomvérový útok na letiská (2025)

- V septembri 2025, kybernetický incident zasiahol check-in a boarding systémy dodávané spoločnosťou Collins Aerospace – podľa Reuters išlo o útok na tretí subjekt, ktorý spôsobil návrat k manuálnym check-inom, dlhé rady, meškania a aj rušenie letov (napr. Brussels, Heathrow, Berlin). ENISA to potvrdila ransomvérový útok.

https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/