Republiková únia zamestnávateľov, Digital Park III, Einsteinova 19, 851 01 Bratislava 5
tel.: +421-2-3301 4280, ruz@ruzsr.sk, www.zamestnavatelia.sk

STANOVISKO REPUBLIKOVEJ ÚNIE ZAMESTNÁVATEĽOV

Stratégia odolnosti kritických subjektov

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/648

Materiál v pripomienkovom konaní do 01.12.2025

Stručný popis podstaty materiálu najmä jeho relevancie z pohľadu RÚZ

Materiál predkladá do medzirezortného pripomienkového konania Ministerstvo vnútra SR na základe § 5 písm. a) zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov

Cieľom a obsahom materiálu je najmä:
Stratégia analyzuje súčasný stav a zraniteľnosť kritických subjektov, vymedzuje strategické ciele a opatrenia do roku 2030, určuje rámec koordinácie medzi ústrednými orgánmi, samosprávou a kritickými subjektmi , obsahuje súbor úloh s určením zodpovedných a súčinných subjektov, navrhuje Ministerstvu vnútra Slovenskej republiky zriadiť stálu medzirezortnú skupinu pre kritickú infraštruktúru ako koordinačného a metodického orgánu na vrcholovej úrovni, navrhuje Ministerstvu financií Slovenskej republiky zriadenie medzirezortnej pracovnej skupiny pre sektor „Financie". Príloha č. 1 obsahuje posúdenie rizika v sektoroch kritickej infraštruktúry Slovenskej republiky. Obsahom prílohy č. 2 je zoznam strategických dokumentov podľa sektorov a príloha č. 3 zahŕňa opis procesu, ktorým sa identifikujú kritické subjekty.

Postoj RÚZ k materiálu

Stratégia analyzuje súčasný stav a zraniteľnosť kritických subjektov, vymedzuje strategické ciele a opatrenia do roku 2030. RÚZ k návrhu predkladá nižšie uvedené pripomienky.

Pripomienky RÚZ k predkladanému materiálu

1. Všeobecná zásadná pripomienka k materiálu ako celku

Dokument opakovane zdôrazňuje potrebu spolupráce so súkromným sektorom (najmä v častiach 4, 8 a 9), avšak nikde explicitne neustanovuje Asociáciu kritickej infraštruktúry Slovenskej republiky (AKI SR) ako konzultačný a odborný orgán, hoci združuje najvýznamnejších prevádzkovateľov, technologické firmy a výskumné subjekty pôsobiace v oblasti kritickej a strategickej infraštruktúry. Navrhujeme preto vložiť Asociáciu kritickej infraštruktúry Slovenskej republiky (AKI SR) ako stáleho partnera MV SR a ostatných ÚOŠS pri tvorbe metodík, cvičení, zdieľaní informácií a konzultácií.

2. Všeobecná zásadná pripomienka k materiálu ako celku

Stratégia obsahuje podľa nášho názoru rizikový pojem „najmenej raz ročne" v oblasti komunikácie s prevádzkovateľmi Raz ročne je pre CER/NIS2 ekosystém nedostatočné – hrozby sú dynamické.

Navrhujeme zmeniť periodicitu na minimálne štvrťročne + v krízových situáciách ad hoc. Asociácia kritickej infraštruktúry Slovenskej republiky (AKI SR) je pripravená tieto stretnutia spolumoderovať.

3. Zásadná pripomienka k Kapitola č. 3, 4 a 6

Návrh úpravy textu:

„Stratégia explicitne ustanovuje, že implementácia opatrení bude prebiehať v úzkej spolupráci so súkromným sektorom ako hlavným prevádzkovateľom kritickej infraštruktúry. Verejno-súkromná spolupráca bude založená na pravidelných konzultáciách, spoločných pracovných skupinách, cvičeniach a koordinovanom zdieľaní informácií o rizikách a incidentoch."

Odôvodnenie:

V SR prevádzkuje viac ako cca 70 % kritickej infraštruktúry súkromný sektor.

Smernica CER jasne stanovuje, že:
- prevádzkovatelia kritických subjektov musia byť aktívne zapojení do procesu budovania odolnosti,
- musia sa podieľať na posúdení rizík, spoločných cvičeniach, výmene informácií a vytváraní bezpečnostných štandardov,
- členské štáty musia podporovať partnerstvá medzi verejným a súkromným sektorom (Public–Private Partnerships).

Stratégia SR však súkromný sektor spomína len okrajovo a nemá definované jeho formálne postavenie.

4. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1 a Cieľ č. 3

Návrh doplnenia:
„Stratégia doplní rámec pre implementáciu povinností podľa smernice CER v súkromných prevádzkovateľoch kritickej infraštruktúry vrátane metodiky posúdenia rizík, bezpečnostných štandardov a odporúčaní pre plánovanie kontinuity a obnovy."

Odôvodnenie:
Stratégia neuvádza podrobnosti implementácie CER na úrovni súkromných prevádzkovateľov (najväčších držiteľov KI)

CER stanovuje povinnosti kritickým subjektom – nie štátu. To znamená, že implementácia prebieha primárne v súkromných firmách, nie na ministerstvách.
Stratégia sa sústreďuje najmä na štátne orgány a informačné systémy verejnej správy a neobsahuje:
- odporúčané opatrenia pre súkromný sektor,
- modely implementácie,
- odporúčané štandardy pre súkromné subjekty,
- metodiku pre risk management v podnikoch,
- mechanizmy, ako budú súkromné subjekty vyhodnocovať odolnosť.

5. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1

Návrh doplnenia:

„Zavedie sa povinné alebo odporúčané mapovanie kritických dodávateľov, hodnotenie závislostí, minimálne požiadavky pre third-party risk management. Hodnotenie rizík bude obsahovať povinnosť analyzovať dodávateľské reťazce, rizikových dodávateľov a závislosti od tretích strán s osobitným dôrazom na súkromné prevádzkovateľské siete."

Odôvodnenie:
Dokument nezohľadňuje dodávateľské reťazce súkromného sektora. Neobsahuje požiadavky na testovanie odolnosti dodávateľských reťazcov. Hybridné a supply-chain útoky sú v dokumente spomenuté, ale bez praktických opatrení.

6. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1 a úloha č. 1

Návrh:
Doplniť požiadavku na povinné konzultácie so zástupcami kritických subjektov, najmä prostredníctvom Asociácie kritickej infraštruktúry Slovenskej republiky (AKI SR).

Odôvodnenie:
Dokument predpokladá tvorbu posúdení rizík v réžii ÚOŠS (Úloha č. 1), no nezahŕňa povinné konzultácie s prevádzkovateľmi – čo je v rozpore s filozofiou CER, ktorá zdôrazňuje spoluprácu.

7. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1 a úloha č. 2

Pri návrhu a testovaní softvérového nástroja navrhujeme zapojiť aj Asociáciu kritickej infraštruktúry, ktorá môže sprostredkovať spätnú väzbu od kritických a iných dotknutých subjektov a pomôcť prispôsobiť nástroj praktickým potrebám kritických subjektov

8. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1 a úloha č. 3

Návrh doplnenia:
Požadujeme technickú a procesnú mapu interoperability.
Zohľadniť existujúce požiadavky NIS2 a NBÚ.

Odôvodnenie:
Dokument uvádza JISKB, no nepopisuje, ako bude zabezpečená interoperabilita s novým systémom incident reporting (Úloha č. 3). Chýba detail: či má vzniknúť nový systém, alebo či sa má rozšíriť funkčnosť JISKB.

9. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 1 a úloha č. 3

Návrh úpravy:
„Pri návrhu, vývoji a testovaní informačného systému na nahlasovanie incidentov bude od začiatku zapojený súkromný sektor a profesijné združenia (AKI), aby bol systém plne použiteľný pre reálne prevádzkové potreby kritických subjektov."

Odôvodnenie:
Dokument neobsahuje praktický rámec pre zdieľanie spravodajských a taktických informácií
Síce sa uvádza úloha č. 3 – incident reporting systém – ale chýba rámec na taktické varovania, spravodajské zhrnutia, technické IOCs a včasné upozornenia na hybridné hrozby.
Návrh doplnenia:
Vytvoriť mechanizmus „Trusted Operators Channel" so zapojením Asociácie kritickej infraštruktúry Slovenskej republiky (AKI SR), NBÚ, SIS a VS.
Mechanizmus Incident Reportingu
Smernica CER a NIS2 žiadajú, aby:
- incident reporting bol jednotný,
- procesy boli jednoduché,
- povinnosti boli primerané možnostiam subjektov,
- súkromný sektor bol zapojený do testovania.

10. Zásadná pripomienka k Kapitola č. 3, cieľ č. 2, úloha č. 6

Návrh úpravy:

„Medzirezortná skupina pre kritickú infraštruktúru bude doplnená o zástupcov relevantných súkromných prevádzkovateľov a profesijných združení - Asociácie kritickej infraštruktúry Slovenskej republiky, ktorí budú participovať ako odborní členovia a konzultačná platforma pre komunikáciu verejného a súkromného sektora."

Odôvodnenie:
Chýba formálne zastúpenie súkromného sektora v riadiacich štruktúrach implementácie CER
CERG odporúča, aby do národných koordinačných orgánov boli zahrnuté:
- profesijné a sektorové združenia,
- prevádzkovatelia kritickej infraštruktúry,
- expertné komunity z praxe.

V SR však v navrhovanej stálej medzirezortnej skupine pre KI chýba zastúpenie súkromných kritických subjektov.

11. Zásadná pripomienka k Kapitola č. 3, cieľ č. 2 (posilnenie plánovania a reakcie, str. 11)

V prvom odseku navrhujeme za slová „vybrané kritické subjekty" doplniť slová: „zo sektora verejnej správy".

Odôvodnenie:
Testovanie informačného systému má byť podľa nášho názoru zabezpečené výlučne na úrovni štátnych orgánov a nemá vytvárať dodatočné administratívne zaťaženie pre súkromné podniky, ktoré budú identifikované ako kritické subjekty. Súkromné subjekty už budú mať povinnosti a náklady spojené s implementáciou opatrení vyplývajúcich zo

zákona č. 367/2024 Z. z. o kritickej infraštruktúre (ďalej len „zákon"), vrátane povinností v oblasti analýzy rizík, kontinuity činností, vedenia kontaktov a nahlasovania incidentov. Zapojenie súkromných podnikov aj do testovania informačného systému by tento rozsah povinností ďalej rozširovalo, a to ešte pred samotným zavedením systému do ostrej prevádzky. Domnievame sa, že ciele sledované testovaním systému možno plnohodnotne dosiahnuť prostredníctvom subjektov verejnej správy bez nutnosti zaťaženia podnikateľského prostredia.

12. Zásadná pripomienka k Kapitola č. 3, cieľ č. 3 (komplexný prístup k odolnosti, str. 13)

V treťom odseku navrhujeme znenie druhej vety nahradiť nasledovným znením: „Navrhované opatrenia sa realizujú prostredníctvom plnenia úloh, napríklad podľa § 15 ústredný orgán na úseku kritickej infraštruktúry môže uskutočniť po vzájomnej dohode s kritickým subjektom koordinačnú poradu s týmto kritickým subjektom vo svojej pôsobnosti s cieľom výmeny informácií a skúseností.".

Odôvodnenie:
Nesúhlasíme s automatickou ročnou periodicitou stretnutí ústredného orgánu s kritickými subjektmi, keďže takáto povinnosť nie je v § 15 zákona explicitne ustanovená. Ak by stratégia zaviedla pravidelné každoročné porady ako fakticky povinné, vytvorilo by to nad rámec zákona dodatočné administratívne a organizačné zaťaženie pre súkromné kritické subjekty, ktoré už musia plniť významný rozsah nových povinností vyplývajúcich zo zákona. Preto je podľa nášho názoru nevyhnutné, aby koordinačné porady prebiehali len po vzájomnej dohode a so súhlasom kritického subjektu, čo zabezpečí zachovanie účelu spolupráce a výmeny informácií bez neprimeraného dopadu na podnikateľské prostredie.

13. Zásadná pripomienka k Kapitola č. 3, Cieľ č. 3 a úloha č. 11

Návrh doplnenia:
Zaviesť PQC ako súčasť minimálnych štandardov (Úloha č. 11).
Pridať PQC do rizikových scenárov a incident response metodík.

Odôvodnenie:
Stratégia neobsahuje požiadavky na post-kvantovú kryptografiu (PQC). Nie je zmienené odporúčanie EÚ 2024/1101 o koordinovanom prechode na PQC, ktoré je pre CI sektory kritické.

14. Zásadná pripomienka k Kapitola č. 4

Návrh doplnenia:

„Bude vytvorený model finančnej podpory pre súkromné kritické subjekty vrátane dotácií, daňových úľav, výziev z eurofondov, finančných nástrojov a podpory investícií do kybernetickej bezpečnosti, fyzickej bezpečnosti, redundancie a prevádzkovej kontinuity. Bude vytvorená samostatná dotačná schéma pre subjekty CI: kybernetická odolnosť, fyzická bezpečnosť, cvičenia, software, post-kvantová bezpečnosť, kontinuálne plánovanie.

Bude zriadený program obdobný „Resilience Facility" pre CI subjekty s podporou MIRRI SR."

Odôvodnenie:
Stratégia deklaruje úlohu 12 (zapojenie EÚ fondov), ale nejasne definuje mechanizmy čerpania pre súkromné kritické subjekty. Kritická infraštruktúra na Slovensku je vo významnej časti prevádzkovaná súkromným sektorom, ktorý je súčasne vystavený najvyšším nákladom v implementácii CER + NIS2.

15. Zásadná pripomienka k Kapitola č. 6

Do textu kapitoly 6 po odseku, kde sa spomína zapojenie akademického sektora a výskumných inštitúcií, navrhujeme doplniť nový odsek:

„Významným partnerom pri implementácii stratégie je Asociácia kritickej infraštruktúry Slovenskej republiky (ďalej len „AKI"), ktorá združuje kritické subjekty súkromného sektora a ďalšie subjekty pôsobiace v tejto oblasti. AKI predstavuje platformu pre odborný dialóg medzi verejným a súkromným sektorom, umožňuje agregovať návrhy a potreby kritických subjektov a zohráva dôležitú úlohu pri prenose informácií o rizikách, hrozbách a osvedčených postupoch."

V kapitole 6, kde sú vymenované subjekty ako SIS, Policajný zbor, akademická obec atď., doplniť medzi „ďalšie zainteresované subjekty" Asociáciu kritickej infraštruktúry Slovenskej republiky (AKI) ako reprezentatívneho zástupcu kritických subjektov a ďalších dotknutých subjektov súkromného sektora.

16. Zásadná pripomienka k Kapitola č. 7

Návrh doplnenia textu:

„Pri uplatňovaní odporúčaných minimálnych opatrení bude vždy uplatňovaný princíp primeranosti podľa veľkosti subjektu, dostupných zdrojov a typu prevádzkovanej infraštruktúry. Pre MSP bude vytvorený zjednodušený režim posúdenia rizík a incident reportingu."

Odôvodnenie:

Dokument predpokladá rovnaké povinnosti pre štátne a súkromné subjekty čo je nereálne pre MSP. MSP tvoria väčšinu prevádzkovateľov napr. v sektore dopravy, zdravotníctva (laboratóriá), waste management, digitálne služby. CER vyžaduje, aby MSP mali primerané povinnosti.

17. Zásadná pripomienka k Kapitola č. 8 (spolupráca a medzinárodní partneri, časť Zapojenie súkromného sektora, str. 21)

Na konci navrhujeme doplniť poslednú vetu v znení: „Realizácia navrhovaných opatrení však nesmie neprimeraným spôsobom zaťažovať podnikateľské subjekty, ktoré budú identifikované ako kritické subjekty.".

Odôvodnenie:

Podnikateľské subjekty identifikované ako kritické subjekty budú povinné plniť rozsiahle povinnosti a znášať finančné náklady spojené s implementáciou zákona, a preto je potrebné, aby nové procesy, formy spolupráce a výmena informácií boli realizované spôsobom, ktorý rešpektuje primeranosť, minimalizuje administratívnu záťaž a nevytvára dodatočné povinnosti nad rámec zákonných požiadaviek. Uvedené opatrenia by preto mali byť vykonávané s dôrazom na efektívnosť, dobrovoľnú participáciu súkromných kritických subjektov a na zachovanie rovnováhy medzi verejným záujmom a ochranou podnikateľského prostredia.

18. Zásadná pripomienka k prílohe č. 1 ,časti Odporúčané opatrenia na zvýšenie odolnosti kritických subjektov

Slová: „najvyššie vedenie organizácie sa bude podieľať" navrhujeme nahradiť slovami: "štatutárny orgán alebo ním určené zodpovedné osoby a osoby zodpovedné za riadenie subjektu verejnej správy sa budú podieľať".

Odôvodnenie:

Pojem „najvyššie vedenie organizácie" nie je ustáleným právnym pojmom, ktorý by bol výslovne zakotvený ako v súkromnoprávnej legislatíve (Obchodný zákonník), tak ani vo verejnoprávnych predpisoch (zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy). Pre odstránenie interpretačných nejasností je preto potrebné jednoznačne uviesť, koho možno považovať za najvyššie vedenie organizácie. V podmienkach Slovenskej republiky je vrcholovým riadiacim orgánom súkromnej právnickej osoby štatutárny orgán, resp. jeho členovia a v prípade subjektov verejnej správy je týmto orgánom minister v prípade ministerstiev alebo v prípade ostatných ústredných orgánov štátnej správy vedúci, predseda alebo riaditeľ. Zároveň je potrebné pôvodné znenie preformulovať aj z dôvodu, že z pôvodného znenia implicitne vyplýva, že povinnosť podieľať sa na procesoch posúdenia rizík a bezpečnosti v rôznych oblastiach sa má automaticky vzťahovať len najvyššie vedenie organizácie, t. j. štatutárny orgán (resp. jeho členov) - v prípade súkromných spoločností. V praxi je bežné, aby štatutárny orgán delegoval odborné a operatívne úlohy na zodpovedné osoby, ktoré majú na tieto činnosti potrebnú odbornú kvalifikáciu. Umožnenie delegácie je štandardom aj v iných regulovaných oblastiach a zabraňuje tomu, aby boli štatutárne orgány neprimerane zaťažované operatívnymi povinnosťami.

Zdroj:

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/648