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

Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/679

Materiál v pripomienkovom konaní do 15.12.2025

Stručný popis podstaty materiálu najmä jeho relevancie z pohľadu RÚZ

Materiál predkladá do medzirezortného pripomienkového konania Národný bezpečnostný úrad SR na základe § 7 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

Cieľom a obsahom materiálu je najmä:
Návrh stratégie je východiskovým strategickým dokumentom, ktorý nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti a je vypracovaný v súlade s vyvíjajúcim sa právnym rámcom Európskej únie, tzn. priamo zohľadňuje povinnosti vyplývajúce z kľúčových právnych aktov – smernice NIS 2, aktu o kybernetickej odolnosti (Cyber Resilience Act), aktu o umelej inteligencii (AI Act) a smernice o odolnosti kritických subjektov.

Návrh stratégie obsahuje päť pilierov: 1, Ochrana národného kybernetického priestoru, 2. Budovanie národných kapacít v oblasti kybernetickej bezpečnosti, 3. Bezpečné a inovatívne digitálne produkty a služby, 4. Vzdelávanie, zručnosti a povedomie, 5. Strategické partnerstvá a medzinárodná spolupráca Jednotlivé piliere obsahujú charakteristiku východiskového stavu, opis cieľového stavu a návrh opatrení, ktorými sa cieľový stav má dosiahnuť.

Postoj RÚZ k materiálu

Návrh stratégie je východiskovým strategickým dokumentom, ktorý nadväzuje na predchádzajúce strategické dokumenty v oblasti kybernetickej bezpečnosti. RÚZ k návrhu predkladá nižšie uvedené pripomienky.

Pripomienky RÚZ k predkladanému materiálu

1. Zásadná pripomienka k materiálu ako celku

Navrhujeme doplniť záväzný finančný rámec stratégie, ktorý bude obsahovať:
- minimálne ročné investičné potreby podľa jednotlivých pilierov,
- mechanizmus spolufinancovania investícií prevádzkovateľov KI (granty, dotácie, daňové nástroje, úvery),
- záväzok vyčlenenia stabilného rozpočtu štátu na kybernetickú odolnosť,
- prepojenie na európske finančné mechanizmy v období 2026–2030.

Odôvodnenie:
Návrh stratégie definuje množstvo opatrení s významnými investičnými dopadmi na prevádzkovateľov kritickej infraštruktúry (napr. prechod na post-kvantovú kryptografiu, budovanie SOC kapacít, bezpečnostné certifikácie, modernizácia OT/IT prostredí, dodávateľské audity, implementácia AI bezpečnostných mechanizmov). Dokument však neobsahuje žiadny rámcový finančný plán, investičné odhady, časové rozdelenie ani mechanizmy spolufinancovania zo strany štátu či EÚ. Bez finančného rámca nie je možné posúdiť uskutočniteľnosť cieľov ani pripravovať investičné plány prevádzkovateľov KI. Ide o nedostatok, ktorý môže výrazne ohroziť implementáciu stratégie.

2. Zásadná pripomienka k materiálu ako celku

Navrhujeme vytvoriť jednotný model implementácie NIS2 + CER pre kritickú infraštruktúru, ktorý bude obsahovať:
- harmonizované procesy riadenia rizík,
- jednotnú terminológiu,
- spoločné auditné štandardy,

- zjednotený reporting incidentov,
- spoločný rámec pre kontrolnú a dohľadovú činnosť štátu.

Odôvodnenie:
V praxi tvoria opatrenia NIS2 a CER jeden spoločný systém riadenia rizík prevádzkovateľov kritickej infraštruktúry. Stratégia však pristupuje k týmto rámcom izolovane, bez harmonizácie postupov, terminológie, kontrolných mechanizmov a reportingových požiadaviek. To môže viesť k duplicite kontrol, regulačnej neistote a neprimeranému administratívnemu zaťaženiu. Prevádzkovatelia KI potrebujú jednotný ucelený rámec.

3. Zásadná pripomienka k materiálu ako celku

Navrhujeme doplniť záväzné mechanizmy financovania, najmä:
- národný fond kybernetickej odolnosti KI,
- možnosť čerpania z fondov EÚ (DIGITAL EUROPE, CEF2, Horizon Europe),
- daňové stimuly pre investície do kyberbezpečnosti,
- schému spolufinancovania pre povinné opatrenia podľa NIS2/CER,
- cenovú reguláciu v regulovaných odvetviach umožňujúcu premietnutie nákladov.

Odôvodnenie:
Prevádzkovatelia KI budú musieť investovať do rozsiahlych bezpečnostných úprav (sieťová segmentácia, monitoring, detekčné systémy, penetračné testovanie, audity, implementácia PQC, certifikácie, školenia). Bez definovaného mechanizmu spolufinancovania, grantových schém, daňových úľav alebo európskych finančných nástrojov môže byť implementácia pre niektoré odvetvia ekonomicky neudržateľná, najmä pre regulované sektory (energia, voda, doprava, zdravotníctvo).

4. Zásadná pripomienka k materiálu ako celku

Doplniť Republikovú únie zamestnávateľov (RÚZ) ako:
- povinného konzultačného partnera,
- člena pracovných skupín pre PQC, SCRM, NIS2/CER implementáciu a architektúru SOC,
- partnera pri tvorbe akčného plánu,
- partnera Monitorovacieho výboru

Odôvodnenie:
RÚZ a v nej združené sektorové profesijné organizácie zabezpečujú odbornú koordináciu, výmenu informácií a pripomienkovanie opatrení na úrovni jednotlivých odvetví kritickej infraštruktúry. Návrh stratégie však ignoruje ich systémovú úlohu a nezaraďuje ich medzi partnerov implementácie, konzultácií ani do pracovných skupín. Takýto prístup obmedzuje možnosť participácie sektorov na formovaní štátnych opatrení a môže viesť k nízkej akceptácii regulácií zo strany prevádzkovateľov KI.

5. Zásadná pripomienka k materiálu ako celku

Navrhujeme doplniť technickú architektúru národného situačného povedomia, vrátane:
- definície dátových tokov KI ↔ sektorové CSIRT ↔ SK-CERT ↔ štátne orgány,
- jednotných API a bezpečnostných štandardov,
- požiadaviek na PQC-ready komunikáciu
- pravidiel pre integráciu sektorových SOC,
- štandardov pre AI-asistované detekčné mechanizmy.

Odôvodnenie:
Stratégia deklaruje potrebu vybudovania národného systému situačného povedomia, no neobsahuje žiadny opis architektúry, štandardov, rozhraní, požiadaviek na integráciu ani modelu zdieľania údajov. Prevádzkovatelia KI tak nemajú možnosť plánovať integráciu svojich SOC alebo OT systémov. Absencia architektúry hrozí duplicitou investícií, nekompatibilitou systémov a právnou neistotou pri ochrane údajov.

6. Pripomienka k materiálu ako celku

Navrhujeme doplniť sadu kľúčových výkonnostných indikátorov (KPI) pre každý strategický cieľ, vrátane merateľných výsledkov a termínov na roky 2026–2030.

Odôvodnenie:
Stratégia je prevažne deklaratívna a neobsahuje konkrétne merateľné ukazovatele výkonu ani termíny realizácie. Bez KPI nie je možné vyhodnocovať priebeh implementácie ani riadiť verejné investície.

7. Pripomienka k materiálu ako celku

Navrhujeme doplniť do stratégie explicitnú úlohu SC-KI-SR ako súčasti národného ekosystému monitoringu a reakcie.

Odôvodnenie:
SC-KI-SR predstavuje už existujúci projekt s významným dopadom na monitoring a ochranu kritickej infraštruktúry. Jeho úplné vynechanie zo stratégie môže viesť k duplicite národných kapacít a k neefektívnemu riadeniu zdrojov.

8. Pripomienka k materiálu ako celku

Navrhujeme doplniť mechanizmy pre:
- diplomatickú podporu pri útokoch na KI,
- technickú a politickú atribúciu s priamym zapojením KI sektorov,
- zdieľanie informácií s európskymi partnermi.

Odôvodnenie:
Prevádzkovatelia KI sú častými cieľmi štátom podporovaných útokov. Strategické dokumenty EÚ v oblasti kyberdiplomacie zdôrazňujú potrebu prepojenia atribúcie, sankčných mechanizmov a ochrany infraštruktúry. Návrh stratégie tieto väzby ignoruje.

9. Pripomienka k materiálu ako celku

Navrhujeme doplniť opatrenia na podporu odborníkov v KI sektoroch, najmä:
- národné programy certifikácií,
- podporné schémy pre odborníkov pracujúcich v KI,
- finančné a kariérne stimuly,
- spoločné vzdelávacie programy s priemyslom

Odôvodnenie:
Na trhu práce pretrváva nedostatok kvalifikovaných odborníkov v oblasti kybernetickej a infraštruktúrnej bezpečnosti. Stratégia neobsahuje systémové opatrenia na stabilizáciu personálnych kapacít v kritických odvetviach (napr. podpora certifikácií, kariérne programy, štátne stimuly, sektorové školenia). Bez riešenia tejto oblasti nie je možné zabezpečiť dlhodobú udržateľnosť implementácie.

10. Zásadná pripomienka k časti II, odsek Kvantové technológie, strana 6

V druhom odseku navrhujeme za druhú vetu doplniť novú vetu v znení: „Pre súkromný sektor má prípadná realizácia opatrení prechodu na PQC dobrovoľný charakter.“.

Odôvodnenie:
Odporúčanie Európskej komisie o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu ako aj následne vypracovaný Koordinovaný plán vykonávania prechodu na postkvantovú kryptografiu, majú nezáväzný, odporúčací charakter a nepredstavujú právne záväzné akty EÚ. Cieľom navrhovaného doplnenia je predísť výkladovým nejasnostiam, podľa ktorých by mohli byť tieto dokumenty vnímané ako implicitne záväzné pre súkromný sektor. Zároveň sa tým sleduje snaha zabrániť vzniku neprimeranej alebo predčasnej finančnej a administratívnej záťaže pre súkromné subjekty, najmä v situácii, keď prechod na PQC môže vyžadovať významné investície do technológií, systémov a odborných kapacít.

11. Zásadná pripomienka k časti III, str. 12

V časti III. str. 12 navrhujeme doplniť 2. ods. takto:
Popri vysokoškolskom vzdelávaní je potrebné venovať pozornosť aj stredným odborným školám alebo gymnáziám, ktoré môžu pripraviť kvalifikovaných pracovníkov pre niektoré typy profesií už na tejto úrovni. Rozšírenie odborných programov alebo dopĺňanie odborných predmetov by mohlo prispieť k rýchlejšiemu dopĺňaniu pracovných síl na základe potrieb pracovného trhu v oblasti kybernetickej bezpečnosti.

12. Zásadná pripomienka k časti IV, str. 13

V časti IV. str. 13 Záväzný právny rámec chýba zohľadnenie aj právnych rámcov, ktoré buď priamo alebo aj nepriamo majú vplyv na oblasť kybernetickej bezpečnosti, napr.:

1. V oblasti odolnosti kritickej infraštruktúry: nariadenie DORA-2022/2554
2. V oblasti identity, dôvernosti a ochrany údajov: nariadenie eIDAS-910/2014 GDPR, + chýba zohľadnenie aktuálnych trendov - výmeny, zdieľania a interoperability dát užívateľov- Nariadenie Data Governance act a Nariadenie Data Act
3. v oblasti digitálnych služieb: Nariadenie DSA 2022/2065

Odôvodnenie:
Domnievame sa, že NBU by malo aj v stratégii KB jasne definovať pozíciu hlavného gestora kybernetickej bezpečnosti SR, ktorý zastrešuje všetky oblasti kybernetickej bezpečnosti.

13. Zásadná pripomienka k časti VI, cieľ 2.1 Cieľový stav

V 2. vete je nevyhnutne skonštatovať, kto je hlavný garant kybernetickej bezpečnosti SR.

14. Zásadná pripomienka k časti VI. Cieľ 3.1 predposledný ods. str. 25

VI. Cieľ 3.1 predposledný ods. str. 25, prvá veta znie:

„Digitálne produkty a služby sú vyvíjané a uvádzané na trh v súlade s požiadavkami aktu o kybernetickej odolnosti, aktu o umelej inteligencii a ďalšími legislatívnymi požiadavkami."

Odôvodnenie:
Vid komentár v časti IV.-Záväzný právny rámec

15. Pripomienka k časti VI. Cieľ 4.1 posledný ods. str. 27

Aké centrum, na čo sa zameriava a samotnú formuláciu je potrebne doplniť.

16. Zásadná pripomienka k časti VI. Cieľ 4.2:

VI. Cieľ 4.2: Zvyšovanie digitálnej gramotnosti občanov a bezpečnostného povedomia
V rámci tohto bodu chýba, že NBU zároveň na národnej úrovni podporuje cielenú a systematickú digitalizáciu verejných služieb a ich bezpečné využívanie, pretože získané zručnosti a znalosti v oblasti digitálnej gramotnosti je nevyhnutné každodenne využívať a rozvíjať praxou.

17. Zásadná pripomienka k časti VI. Cieľ 5.1.

VI. Cieľ 5.1 posledná veta na str. 30 znie:

„V úzkej spolupráci medzi Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky a ďalšími relevantnými orgánmi Slovensko aktívne pôsobí v medzinárodných organizáciách, svetových a európskych fórach, ktoré formujú normy, štandardy a politiky v oblasti kybernetickej bezpečnosti s cieľom zvyšovať diplomatickú angažovanosť Slovenska, posilňovať jeho viditeľnosť a budovať tzv. image modernej a bezpečnej krajiny a prispievať k utváraniu medzinárodného prostredia založeného na zodpovednom správaní štátov v kybernetickom priestore."

18. Zásadná pripomienka k časti VII, str. 32, odsek Akčný plán

Časť VI. má byť označená „VII."

Na konci navrhujeme doplniť poslednú vetu v znení: „Navrhované úlohy však nesmú neprimeraným spôsobom finančne a administratívne zaťažovať podnikateľské subjekty, ktoré boli určené ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb.

Odôvodnenie:
Podnikateľské subjekty identifikované ako prevádzkovatelia základných služieb alebo ako prevádzkovatelia kritických základných služieb budú povinné plniť rozsiahle povinnosti a znášať finančné náklady spojené s implementáciou povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti v znení jeho poslednej novely, a preto je potrebné,

aby nové procesy, formy spolupráce, výmena informácií a ostatné povinnosti, ktoré môžu vyplynúť z navrhovaných úloh boli realizované spôsobom, ktorý rešpektuje primeranosť, minimalizuje administratívnu a finančnú záťaž a nevytvára dodatočné povinnosti nad rámec zákonných požiadaviek. Uvedené opatrenia by preto mali byť vykonávané s dôrazom na efektívnosť, minimálne finančné a administratívne zaťaženie podnikateľských subjektov a na zachovanie rovnováhy medzi verejným záujmom a ochranou podnikateľského prostredia.

19. Zásadná pripomienka k časti VII, str. 32

Časť VI. má byť označená „VII."

Na strane 32 Implementačný rámec navrhujeme úpravy v 2. a 4. vete:
„Akčný plán musí byť v súlade s prioritami stratégie a zároveň dostatočne flexibilný, aby mohol reagovať na trendy, meniace sa podmienky a potreby spoločnosti. ..."

„...Po prijatí národnej stratégie, Slovenská republika notifikuje o národnej stratégii kybernetickej bezpečnosti SR Európsku komisiu do troch mesiacov od jej prijatia."

20. Zásadná pripomienka k časti VII, str. 33

Strana 33 Implementačný rámec navrhujeme doplnenia:

Kybernetická bezpečnosť priamo súvisí alebo úzko interaguje s inými oblasťami práva a správy veci verejných. Ide predovšetkým o oblasti súvisiace s:
- informatizáciou a digitalizáciou verejnej správy,
- ochranou kritickej infraštruktúry,
- krízovým riadením štátu,
- obranou štátu,
- ochranou osobných údajov
- „interoperabilitu údajov a"
- reguláciou umelej inteligencie.

„... Dôraz sa bude klásť na pravidelnú vzájomnú komunikáciu, výmenu informácií, interoperabilitu procesov a konzistentnosť odporúčaní tak, aby sa opatrenia v oblasti kybernetickej bezpečnosti prirodzene dopĺňali s opatreniami v iných oblastiach."

Zdroj:

https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/679