SPS

Kybernetická bezpečnosť (KPI)

Program "Baseline bezpečnosť" (2026-2027) *45 mil. EUR*

Program zabezpečenie kontinuity prevádzky (2026-2029) *50 mil. EUR*

Program operačná bezpečnosť (2026-2030) *45 mil. EUR*

ID	Kľúčový merateľný ukazovateľ	Východisková hodnota	Cieľ	Termín	Spôsob merania	Ako to dosiahneme	Detail	Čo sa bude merať	Určenie štandardu	Program	Úloha na MIRRI	Termín úloha MIRRI	Úloha na OVM	Termín úloha OVM
1.	Úroveň riadenia v správe ITVS prostredníctvom vybraných kľúčových ukazovateľov	N/A	≥ 30 %	Q4/2030	Monitoring výkonu riadenia	Implementácia baseline bezpečnostných štandardov v súlade s NIS2 bude zahŕňať pravidelné odpočítavanie a hodnotenie bezpečnostných ukazovateľov pomocou, na základe priebežného monitoringu informačného systému Achilles a zavedenia periodických auditov ktoré overia implementáciu a efektívnu bezpečnostných opatrení. Taktiež sa vytvoria plány kontinuálneho zlepšovania vrátane školení pre IT personál, aby sa zabezpečilo dodržiavanie najnovších medzinárodných a európskych smerníc a zvyšovania úrovne kybernetickej odolnosti verejnej správy.		Percento správcov informačných systémov verejnej správy, ktorí splnili základnú úroveň bezpečnosti, v pomere k celkovému počtu správcov.		Program "Baseline bezpečnosť" (2026-2027)	Definovať postupy zavádzania baseline bezpečnosti	Q2/2026	Realizovať overenie zavedenia baseline bezpečnosti	Q4/2027
											Pripraviť vzory bezpečnostnej dokumentácie pre všetky OVM	Q2/2027		
2.	Počet subjektov verejnej správy zapojených do pravidelného vyhľadávania zraniteľností	306 subjektov	800 subjektov	Q4/2030	SKB MIRRI	Vybuduje sa komplexný systém, ktorý zahŕňa identifikáciu a zoznam všetkých relevantných inštitúcií, zavedenie jednotnej metodológie a štandardných postupov pre pravidelné skenovanie a hodnotenie zraniteľností. Súčasťou bude nastavenie monitorovania, reportovania a analytických hlásení a využitím automatizovaného systému Achilles, ako aj zabezpečenie centralizovanej podpory a koordinácie zo strany odborných orgánov. Návrh legislatívneho prípadne regulačného opatrenia pre zabezpečenie povinnosti orgánov zapojiť sa do pravidelných vyhľadávaní zraniteľností.		Počet informačných systémov verejnej správy, v ktorých je vykonávané pravidelné vyhľadávanie zraniteľností, v pomere k celkovému počtu systémov.		Program zabezpečenie kontinuity prevádzky (2026-2029)	Zaviesť centrálne zálohovanie kritickej infraštruktúry (NASES)	Q2/2028	Vytvoriť DR plány pre prioritné informačné systémy	Q4/2027
											Monitoring zapojených subjektov do pravidelného vyhľadávania zraniteľností	priebežne	Pravidelné vyhľadávania zraniteľnosti	priebežne
3.	Priemerný čas reakcie na bezpečnostný incident	13 hodín	8 hodín	Q4/2030	SKB MIRRI	Primárne cez Program Operačná bezpečnosť. Postupné zníženie: 72h → 24h (zmluvena SOC) + 12h (24/7 prevádzka) + 8h (SIEM/SOAR automatizácia) + 0h (AI orchestrácia). Kľúčové míľniky: SOC Q2/2027, SOAR platforma Q4/2027, plná automatizácia Q4/2028.		Priemerný čas reakcie na bezpečnostný incident vyjadrený v hodinách.		Program operačná bezpečnosť (2026-2030)	Zriadiť centrálny CSIRT/SOC pre verejnú správu	Q2/2027	Organizovať sektorové cvičenia kybernetickej bezpečnosti každoročne (NBÚ/OVM)	Q4/2028
											Zaviesť platformu pre threat intelligence zdieľanie	Q2/2028		
											Realizovať celonárodné cvičenia incident response na úrovni kritickej infraštruktúry	Q4/2026		
											Vytvoriť plány obnovy pre informačné systémy, ktoré zabezpečujú kritické základné služby štátu	Q4/2027	Pre informačné systémy, ktoré zabezpečujú kritické základné služby štátu zaviesť distribuované spracovanie odolné voči výpadku v jednej lokalite	Q4/2030
4.	Počet vykonaných osobokliskov v oblasti kybernetickej bezpečnosti	menej ako 1500	10 000 osobokliskov	Q4/2030	Výstupy školiacich aktivít	Kombinácia e-learningu, certifikácií a praktických cvičení.		Počet osobokliskov realizovaných v oblasti kybernetickej bezpečnosti.		Program operačná bezpečnosť (2026-2030)	Vykonať 10 000 osobokliskov v oblasti kybernetickej bezpečnosti (MIRRI/OVM)	Q4/2030	Vykonať 10 000 osobokliskov v oblasti kybernetickej bezpečnosti (MIRRI/OVM)	Q4/2030
5.	Orgány riadenia pripojené na systém včasného varovania (EWS)	7 orgánov	15 orgánov	Q4/2030	SKB MIRRI	Cez program Operačná bezpečnosť. Postupné pripájanie vybraných organizácií. Technické zabezpečenie cez centrálny SOC a Threat Intelligence platformu.		Počet riadiacich orgánov pripojených na systém včasného varovania (EWS), v pomere k celkovému počtu relevantných orgánov.		Program operačná bezpečnosť (2026-2030)	Pripojiť 15 OVM na systém včasného varovania (EWS)	Q4/2030		
6.	Vykonané a otestované plány kontinuity a plány obnovy systémov a záloh raz/rôt raz za rok na informačný systém / raz za pol roka pre kritické informačné systémy verejnej správy	nepravidelné vykonávanie bez dohľadu orgánu riadenia	100% pre kritické informačné systémy	Q4/2030	Monitoring výkonu riadenia	Implementáciou programu Zabezpečenie kontinuity prevádzky.		Počet kritických informačných systémov verejnej správy s vykonanými a otestovanými plánmi kontinuity a plánmi obnovy systémov a záloh minimálne raz za pol roka		Program zabezpečenie kontinuity prevádzky (2026-2029)	Vykonávať a testovať plány kontinuity a plánov obnovy systémov a záloh (NASES)	Každoročne pre každý ISVS a každý pobrok pre kritický ISVS	Vykonávať a testovať plány kontinuity a plánov obnovy systémov a záloh	Každoročne pre každý ISVS a každý pobrok pre kritický ISVS.