

SP5**Kybernetická bezpečnosť (KPI)**

ID	Kľúčový merateľný ukazovateľ	Východisková hodnota
1.	Úroveň riadenia v správe ITVS prostredníctvom vybraných kľúčových ukazovateľov	N/A
2.	Počet subjektov verejnej správy zapojených do pravidelného vyhľadávania zraniteľností	306 subjektov
3.	Priemerný čas reakcie na bezpečnostný incident	13 hodín
4.	Počet vykonaných osoboškolení v oblasti kybernetickej bezpečnosti	menej ako 1500
5.	Orgány riadenia pripojené na systém včasného varovania (EWS)	7 orgánov

6.	Vykonané a otestované plány kontinuity a plány obnovy systémov a záloh aspoň raz za rok na informačný systém / raz za pol roka pre kritické informačné systémy verejnej správy	nepravidelné vykonávanie bez dohľadu orgánu riadenia
----	--	---

Cieľ	Termín
o 30 %	Q4/2030
800 subjektov	Q4/2030
8 hodín	Q4/2030
10 000 osoboškolení	Q4/2030
15 orgánov	Q4/2030

100% pre kritické informačné systémy

Q4/2030

Program "Baseline bezpečnosti" (2026-2027)

Program zabezpečenie kontinuity prevádzky (2026-2029)

Program operačná bezpečnosť (2026-2028)

Spôsob merania	Ako to dosiahneme
Monitoring výkonu riadenia	Implementácia baseline bezpečnostných štandardov v súlade s NIS2 bude zahŕňať pravidelné odpočtovanie a hodnotenie bezpečnostných ukazovateľov pomocou, na základe plošného monitoringu informačného systému Achilles a zavedenia periodických auditov ktoré overia implementáciu a efektivitu bezpečnostných opatrení. Taktiež sa vytvoria plány kontinuálneho zlepšovania vrátane školení pre IT personál, aby sa zabezpečilo dodržiavanie najnovších medzinárodných a európskych smerníc a zvyšovanie úrovne kybernetickej odolnosti verejnej správy.
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 s 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.
SKB MIRRI	Primárne cez Program Operačná bezpečnosť. Postupné zníženie: 72h → 24h (zriadenie SOC) → 12h (24/7 prevádzka) → 8h (SIEM/SOAR automatizácia) → 5h (AI orchestrácia). Kľúčové míľniky: SOC Q2/2027, SOAR platforma Q4/2027, plná automatizácia Q4/2028.
Výstupy školiacich aktivít	Kombinácia e-learningu, certifikácií a praktických cvičení.
SKB MIRRI	Cez program Operačná bezpečnosť. Postupné pripájanie vybraných organizácií. Technické zabezpečenie cez centrálny SOC s Threat Intelligence platformou.

Monitoring výkonu riadenia

Implementáciou programu Zabezpečenie kontinuity prevádzky.

45 mil. EUR

50 mil. EUR

45 mil. EUR

Detail	Čo sa bude merať
	Percento správcov informačných systémov verejnej správy, ktorí splnili základnú úroveň bezpečnosti, v pomere k celkovému počtu správcu.
	Počet informačných systémov verejnej správy, v ktorých je vykonávané pravidelné vyhľadávanie zraniteľností, v pomere k celkovému počtu systémov.
	Priemerný čas reakcie na bezpečnostný incident vyjadrený v hodinách.
	Počet osoboškolení realizovaných v oblasti kybernetickej bezpečnosti.
	Počet riadiacich orgánov pripojených na systém včasného varovania (EWS), v pomere k celkovému počtu relevantných orgánov.

Počet kritických informačných systémov verejnej správy
s vykonanými a otestovanými plánmi kontinuity a
plánmi obnovy systémov a záloh minimálne raz za pol
roka

Určenie štandardu	Program
	Program "Baseline bezpečnosti" (2026-2027)
	Program zabezpečenie kontinuity prevádzky (2026-2029)
	Program operačná bezpečnosť (2026-2030)
	Program operačná bezpečnosť (2026-2030)
	Program operačná bezpečnosť (2026-2030)

Program zabezpečenie kontinuity prevádzky (2026-2029)

Úloha na MIRRI

Definovať postupy zavádzania baseline bezpečnosti

Pripraviť vzory bezpečnostnej dokumentácie pre všetky OVM

Zaviesť centrálné zálohovanie kritickej infraštruktúry (NASES)

Monitoring zapojených subjektov do pravidelného vyhľadávania zraniteľnosti

Zriadiť centrálny CSIRT/SOC pre verejnú správu

Zaviesť platformu pre threat intelligence zdieľanie

Realizovať celonárodné cvičenia incident response na úrovni kritickej infraštruktúry

Vytvoriť plány obnovy pre informačné systémy, ktoré zabezpečujú kritické základné služby štátu

Vykonať 10 000 osoboškolení v oblasti kybernetickej bezpečnosti (MIRRI/OVM)

Pripojiť 15 OVM na systém včasného varovania (EWS)

Vykonávat a testovat plány kontinuity a plánů obnovy systémů a záloh (NASES)

Termín úloha MIRRI	Úloha na OVM
Q2/2026	Realizovať overenie zavedenia baseline bezpečnosti
Q2/2027	
Q2/2028	Vytvoriť DR plány pre prioritné informačné systémy
priebežne	Pravidelné vyhľadávania zraniteľnosti
Q2/2027	Organizovať sektorové cvičenia kybernetickej bezpečnosti každoročne (NBÚ/OVM)
Q2/2028	
Q4/2026	
Q4/2027	Pre informačné systémy, ktoré zabezpečujú kritické základné služby štátu zaviesť distribuované spracovanie odolné voči výpadku v jednej lokalite
Q4/2030	Vykonať 10 000 osoboškolení v oblasti kybernetickej bezpečnosti (MIRRI/OVM)
Q4/2030	

Každoročne pre každý
ISVS a každý polrok pre
kritický ISVS

Vykonávať a testovať plány kontinuity a plánov obnovy systémov a záloh

Termín úloha OVM
Q4/2027
Q4/2027
priebežne
Q4/2028
Q4/2030
Q4/2030

Každoročne pre
každý ISVS a každý
polrok pre kritický
ISVS.