Ministerstvo zahraničních věcí
České republiky

ČESKÁ REPUBLIKA
POMÁHÁ

Program budování kapacit partnerských zemí v oblasti kybernetické bezpečnosti

Program budování kapacit partnerských zemí v oblasti kybernetické bezpečnosti (dále jen „Program“) je rozvojovým nástrojem, který vychází z Cílů udržitelného rozvoje OSN (SDG) 2030, zejména z cíle č. 9 c) tj., „Zvýšit přístup k informačním a komunikačním technologiím“, dále ze Strategie zahraniční rozvojové spolupráce ČR na léta 2018 – 2030 a z Národní strategie kybernetické bezpečnosti ČR. Program odráží dosavadní zkušenosti z této oblasti na základě realizovaných aktivit v Gruzii, Bosně a Hercegovině a v Ghaně.

Program dále přispívá k naplňování příslibů vyplývajících z Evropského konsensu o rozvoji a dále napomáhá naplňovat závazky plynoucí z Akční agendy z Addis Abeby.

Rozvoj digitálních a kybernetických kapacit je nedílnou součástí pokroku a rozvoje každé země v ekonomické, politické a sociální oblasti. Sdílení odborných znalostí o kybernetické bezpečnosti se zahraničními partnery zvyšuje kolektivní schopnost porozumět společným protivníkům a bránit se proti nim, což v důsledku posiluje globální kybernetickou odolnost. Jedná se o nedílnou součást mezinárodní spolupráce, jež tak může podpořit mezinárodní solidaritu se společnou vizí a cílem: zabezpečit svobodný, otevřený, bezpečný a interoperabilní kybernetický prostor pro všechny a zároveň zajistit dodržování lidských práv a v souladu s příslušnými mezinárodními závazky.

Česká republika má v oblasti kybernetické bezpečnosti řadu dovedností, které může sdílet s dalšími partnerskými zeměmi. Je připravena nabídnout své zkušenosti z oblasti legislativy, budování kapacit, předat své technologie, software a hardware státním institucím, firmám i vysokým školám v partnerských zemích. Program budování kapacit partnerských zemí v oblasti kybernetické bezpečnosti obsahuje portfolio projektů a návazných aktivit s cílem zvýšit odolnost třetích zemí vůči kybernetickým hrozbám. Součásti programu může být i podpora projektů mezinárodních vládních organizací, kterých je ČR členem.

Cíl programu

Hlavním cílem programu je pomáhat partnerským zemím posilovat jejich kapacity v oblasti kybernetické bezpečnosti, a to zejména podporou fungujících a odpovědných institucí s cílem zvýšit kybernetickou odolnost a schopnost účinně reagovat na počítačovou kriminalitu.

Cílem programu je i výměna informací a užší spolupráce s jednotlivými zeměmi v rámci multilaterálních jednání o kybernetické bezpečnosti a boji proti kybernetické kriminalitě (zodpovědné chování států v kyberprostoru, opatření pro budování důvěry, aplikace mezinárodního práva na kyberprostor, budování kapacit, diskuse o nových technologických hrozbách apod.). V důsledku toho může program rovněž přispět ke snížení kybernetických hrozeb globálně i vůči České republice.

Cíle programu jsou zaměřeny na posílení veřejného, akademického i soukromého sektoru v partnerských zemích.

Předávání odborných zkušeností je doplněno nabídkou produktů českých firem v oblasti kybernetické bezpečnosti, díky čemuž program přispívá i ke zvýšení exportního potenciálu ČR.

Hlavní tematické oblasti programu

Projekty a návazné aktivity programu podporují strategická partnerství, která zemím pomáhají posilovat národní kybernetickou bezpečnost a související úsilí v oblasti vymáhání práva. Zaměříme se na pomoc zejména v těchto oblastech:

- rozvíjení a provádění národní kybernetické strategie a politiky
- předávání zkušenosti z oblasti legislativy a budování kapacit (institucí);
- ochrana instituce před kybernetickými útoky;
- zřizování a posílení týmů pro reakci na kybernetické incidenty (CSIRT);
- účinná reakce na počítačovou kriminalitu;
- účinná spolupráce v multilaterálních jednáních o kybernetické bezpečnosti a boji proti kybernetické kriminalitě.

Program je doplněn o nástroje ekonomické diplomacie, které mohou dále posílit kapacity partnerských zemí.

Teritoriální zaměření programu

Teritoriální zaměření programu odpovídá prioritám stanoveným v Koncepci zahraniční politiky ČR a ve Strategii zahraniční rozvojové spolupráce ČR (2018 – 2030). Je součásti „Team Europe Initiative“ a vychází ze zásad „Global Gateway“. Projekty v rámci programu jsou určeny pro rozvojové země (dle OECD/DAC) při zohlednění zahraničně-politických priorit ČR mimo jiné i s cílem posílení spolupráce s partnerskými zeměmi na multilaterálním poli (OSN). Program cílí zejména na země těchto regionů:

Afrika
Západní Balkán
Východní partnerství
Indo-Pacifik

Nástroje programu

Program má celkem 4 nástroje, přičemž nástroje č. 1 – 3 jsou součástí zahraniční rozvojové spolupráce a jsou započitatelné do ODA, nástroj č. 4 je nástrojem ekonomické diplomacie.

1. <u>Projekty pro rozvoj odpovědných institucí a přenos zkušeností v oblasti legislativy.</u>

Základním prvkem programu jsou projekty zaměřené na budování kybernetických kapacit, které pomáhají při rozvoji fungujících a odpovědných institucí, účinně reagují na počítačovou kriminalitu a posilují kybernetickou odolnost země. Tyto projekty mají mnoho podob, například poradenství vládním týmům, jak reagovat na národní incidenty kybernetické bezpečnosti, školení pro policisty a vyšetřovatele zaměřená na vyšetřování činů kybernetické kriminality, pomoc s tvorbou strategických a koncepčních dokumentů, výměna informací o dodržování norem odpovědného chování států v kybernetickém prostoru apod. Projekty mohou být realizovány institucemi státní správy, justice a policie České republiky.

Aktivity podpořené v rámci programu jsou realizovány zejména ve formě odborných seminářů, workshopů a školení pořádaných týmy pracovníků státní správy, justice a policie z oblasti kybernetické bezpečnosti a kriminality se zaměřením na legislativu, justici, bezpečnostní složky apod.

Tato složka programu je financována z rozpočtu na zahraniční rozvojovou spolupráci v gesci MZV ČR, položky Technická expertní spolupráce a je realizována v gesci ORS. Plán ZRS na rok 2022 (UV č. 535/2021) počítá pro uvedenou položku s částkou 5 mil. Kč, se stejným objemem finančních prostředků se počítá i pro roky 023 a 2024.

2. Předávání technologií a softwaru formou darů, případně formou vázaných peněžních darů

Dalším prvkem programu je předávání technologií a softwaru formou darů, s preferencí využití nástroje vázaných peněžních darů, které umožňují dodávku českého materiálu a zařízení vybraným příjemcům v cílových zemích. Vázané peněžní dary jsou realizovány v souladu s Metodickým postupem pro poskytování vázaných peněžních darů a financovány z příslušné položky rozpočtu MZV.

Tato složka programu je financována z rozpočtu na zahraniční rozvojovou spolupráci v gesci MZV ČR, položky Technická expertní spolupráce a je realizována v gesci ORS. Plán ZRS na rok 2022 (UV č. 535/2021) počítá pro uvedenou položku s částkou 5 mil. Kč, se stejným objemem finančních prostředků se počítá i pro roky 2023 a 2024.

3. Spolupráce akademického sektoru

Tato část programu je komplementární s cíli programu „Posilování kapacit veřejných vysokých škol v rozvojových zemích“, tj. zvyšovat kvalitu a odbornost vysokoškolského vzdělávání, vědy a výzkumu v rozvojových zemích v oblasti kybernetické bezpečnosti. Cílem je vytvořit síť absolventů, lektorů a expertů se znalostí technické stránky kybernetické bezpečnosti, ale také seznámených s mezinárodními výzvami a procesy v oblasti kybernetické bezpečnosti a připravených podporovat implementaci a všeobecnou informovanost o kybernetické bezpečnosti, mimo jiné pokyny OSN o normách a opatřeních k budování důvěry.

Aktivity podpořené v rámci programu zahrnují zejména odborné výměny pedagogů z českých a partnerských veřejných vysokých škol, realizaci společných pedagogických aktivit v rámci meziuniverzitní spolupráce, realizaci specializovaných krátkodobých studijních pobytů učitelů i studentů z rozvojových zemí na českých veřejných vysokých školách, včetně předávání českého know-how v oblasti managementu vysokého školství či v odborné publikační činnosti, apod. Uvedené aktivity mohou být provázány s projekty pro rozvoj odpovědných institucí (viz bod 1).

Realizaci výše uvedených aktivit může zajišťovat koordinační centrum na půdě některé z českých vysokých škol

Tato část programu je realizována formou dotačních výzev vyhlašovaných MZV. Oprávněnými příjemci dotace jsou české veřejné vysoké školy v partnerství či konsorciu s veřejnými vysokými školami z příslušné rozvojové země a případně s dalšími aktéry (české či místní neziskové či komerční subjekty, výzkumné instituce, kraje či obce apod.).

Projekty předkládané v rámci dotační výzvy mohou být jednorázové (jednoleté) i víceleté, přičemž dotace je vždy přidělena na příslušný kalendářní rok na základě splnění stanovených podmínek (zejména včasné předložení průběžného vyúčtování a zprávy o realizaci projektu).

Tato složka programu je financována z rozpočtu na zahraniční rozvojovou spolupráci v gesci MZV ČR, položky Technická expertní spolupráce a je realizována v gesci ORS. Plán ZRS na rok 2022 (UV č. 535/2021) počítá pro uvedenou položku s částkou 5 mil. Kč, se stejným objemem finančních prostředků se počítá i pro roky 2023 a 2024.

4. Následné projekty na podporu ekonomické diplomacie

Program počítá se zapojením soukromého sektoru zejména z okruhu firem zabývajících se zaváděním metod ochrany před kybernetickými útoky. Jedná se především o cíleně zaměřené akce na podporu obchodních aktivit českých firem, které partnerským zemím nabídnou softwarové či hardwarové produkty a vybavení na posílení odolnosti proti kybernetickým hrozbám. Projekty jsou realizovány primárně zastupitelskými úřady ČR v různých podobách (oborové prezentace, business fóra, semináře, účasti na výstavách, kulaté stoly, podnikatelské mise apod.) ve spolupráci s českými firmami.

Projekty na podporu ekonomické diplomacie (PROPED) jsou financovány ze Společného nástroje financování ekonomické diplomacie, do kterého jsou kromě Ministerstva zahraničních věcí ČR zapojena i další ministerstva a NÚKIB. Návrhy na projekty předkládají v souladu s Metodikou projektů ekonomické diplomacie zastupitelské úřady v partnerské zemi a jsou v gesci MZV ČR (OED).

Návrhy projektů podávaných v rámci PROPED pro realizaci programu budování kapacit partnerských zemí v oblasti kybernetické bezpečnosti jsou v databázi PROPED označeny příznakem „cybervac“. Před samotným předložením jsou návrhy předjednány v úzké součinnosti mezi OKB a ZÚ. Předložené návrhy jsou v rámci komise pro výběr projektů PROPED schvalovány formou per-rollam.

Účastníci programu

Do programu jsou zapojeny české instituce napříč státní správou, dále subjekty z akademické sféry a soukromého sektoru a zahraniční partnerské instituce. Jedná se zejména o tyto subjekty:

- Státní správa (Ministerstvo zahraničních věcí, Ministerstvo spravedlnosti, Ministerstvo vnitra, NÚKIB ad.);
- Policie ČR (zejména Národní centrála proti organizovanému zločinu);

- Justice (zejména Nejvyšší státní zastupitelství);
- Soukromý sektor – české firmy nabízejí řešení v oblasti kybernetické bezpečnosti
- Akademický sektor – české vysoké školy a univerzity (Masarykova univerzita, ČVUT apod.).
- nevládní a neziskové organizace zabývající se problematikou kybernetické bezpečnosti
- Zahraniční partnerské instituce

Zajištění realizace programu a rozdělení gescí

OKB – politické a obsahové zastřešení programu, stanovení obsahových priorit, spolupráce s institucemi státní správy, akademickým sektorem a ZÚ;

ORS – propojení s nástroji ZRS v souladu s příslušnými metodickými pokyny, správa prostředků na projekty pro rozvoj odpovědných institucí (bod č. 1), na vázané peněžní dary (bod č. 2.), na projekty spolupráce v akademickém sektoru (bod č. 3),

OED – následné projekty na podporu ekonomické diplomacie (bod č. 4)

Teritoriální odbory – spolupráce při stanovování geografických priorit;

Zastupitelské úřady – spolupráce při přípravě projektů (body č. 1, 2, 3, 4) a návazných aktivit, komunikace se zahraničními subjekty.

Intervenční logika Programu

Cíl	Nástroj	Aktivita
rozvíjení a provádění národní kybernetické strategie a politiky	č. 1) Projekty pro rozvoj odpovědných institucí	odborné semináře, workshopy a školení
předávání zkušenosti z oblasti legislativy a budování kapacit (institucí);	č. 1) Projekty pro rozvoj odpovědných institucí č. 3) Spolupráce akademického sektoru	odborné semináře, workshopy a školení krátkodobé studijní pobyty
účinná reakce na počítačovou kriminalitu	č. 2) Předávání technologií formou darů, případně vázaných peněžních darů	Nabídka softwarových a hardwarových produktů českých firem
účinná spolupráce v multilaterálních jednáních o kybernetické bezpečnosti a boji proti kybernetické kriminalitě.	č. 1) Projekty pro rozvoj odpovědných institucí č. 3) Spolupráce akademického sektoru	odborné semináře, workshopy a školení krátkodobé studijní pobyty,
zřizování a posílení týmů pro reakci na kybernetické incidenty (CSIRT);	č. 1) Projekty pro rozvoj odpovědných institucí č. 4) Následné projekty na podporu ekonomické diplomacie	odborné semináře, workshopy a školení Nabídka softwarových a hardwarových produktů českých firem
ochrana instituce před kybernetickými útoky;	č. 2) Předávání technologií formou darů, případně vázaných peněžních darů č. 4) Následné projekty na podporu ekonomické diplomacie	Nabídka softwarových a hardwarových produktů českých firem