Karta projektového okruhu

Číslo a název projektového okruhu: 7. Kybernetická bezpečnost

Garant karty projektového okruhu: Národní bezpečnostní úřad

Spolupracující subjekty: Ministerstvo vnitra, Rada pro kybernetickou bezpečnost, Národní centrum kybernetické bezpečnosti

Výčet strategií a cílů, na jejichž plnění se projektový okruh podílí:

Strategický dokument	Strategický/Specifický cíl
Národní strategie kybernetické bezpečnosti České republiky na období let 2015 - 2020 a návazný Akční plán	Ochrana kritických informačních infrastruktur Posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy Používání spolehlivých a důvěryhodných informačních technologií
Strategický rámec rozvoje veřejné správy České republiky pro období 2014 - 2020	Strategický cíl 3: Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu Specifický cíl 3.1: Dobudování funkčního rámce eGovernmentu
Digitální Česko (DIGIC)	Strategický cíl 1: Zajištění bezpečnosti a odolnosti ICT infrastruktur cestou zaměření na prevenci, připravenost a informovanost Strategický cíl 2: Bezpečnost služeb a sítí elektronických komunikací
Digitální agenda pro Evropu (DAEVR)	Strategický cíl 1: Důvěra a bezpečnost IKT Strategický cíl 2: Opatření na ochranu sítí a informací, boj proti kyberkriminalitě

Zdůvodnění potřebnosti projektového okruhu včetně popisu výchozího stavu:

Výchozí stav:

V současné době organizace veřejné správy provozují v rámci výkonu veřejné moci značné množství informačních systémů veřejné správy (ISVS). Z bezpečnostního hlediska se na tyto systémy již po delší dobu vztahují požadavky vyplývající ze zákonů č. 101/2000 Sb., o ochraně osobních údajů, a č. 365/2000 Sb., o informačních systémech veřejné správy, které jsou však poměrně obecné, tudíž ISVS, jichž se týkají, nemusí mít konzistentní úroveň zabezpečení. V návaznosti na přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti, dochází v této oblasti k výrazné změně. Tento zákon pro vybrané typy důležitých ISVS (tzv. významných informačních systémů a systémů kritické informační infrastruktury) předepisuje konkrétní bezpečnostní požadavky. Jedná se převážně o zavedení metodiky řízení bezpečnosti informací v intencích ČSN ISO/IEC 27001 a následné zavedení technických opatření na základě zhodnocení bezpečnostních rizik. Dalším důležitým dopadem zákona č. 181/2014 Sb. je povinnost hlášení bezpečnostních incidentů na národní centrum kybernetické bezpečnosti (NCKB) a implementace opatření požadovaných NBÚ (NCKB).

Současný stav jednotlivých ISVS z hlediska kybernetické bezpečnosti je velmi různorodý. Pro zajištění odolnosti systémů veřejné správy vůči kybernetickým útokům, kyberkriminalitě a ztrátám z toho plynoucím, je nutné povýšit jak jejich organizační, tak i procesní a technickou odolnost.

Zdůvodnění potřebnosti projektového okruhu:

Bez ohledu na zákonné požadavky na ISVS, narůstající počty kybernetických útoků v posledních několika letech poukazují na nutnost soustředit se na bezpečnost informačních systémů zpracovávajících libovolné hodnotné

nebo jinak zajímavé informace. Studie prováděné v posledních letech v Nizozemsku a v USA odhadují ztráty způsobené v těchto státech kyberkriminalitou na 1-1.5% HDP. Jedná se tedy o extrémně závažnou hrozbu, která může mít i velmi výrazné hospodářsko-ekonomické důsledky. I systémy neobsahující data s výraznou ekonomickou hodnotou se mohou stát cílem útoku, a to buď jako vedlejší důsledek útoku na jiné systémy nebo jako cíl vandalismu.

Projektový okruh bude zajišťovat výrazné zvýšení bezpečnosti informačních systémů veřejné správy, a to jak v oblasti technických opatření, tak i v oblasti organizační a procesní. Díky značné provázanosti jednotlivých ISVS dojde při implementaci lepších bezpečnostních opatření u méně bezpečnostně zralých systémů k vylepšení bezpečnostní situace i u připojených systémů bezpečnostně zralejších. Obzvláště výrazné toto je u zajištění integrity a důvěrnosti dat, které musí být předávány do méně zabezpečených systémů.

V rámci projektů tohoto okruhu by mělo dojít k významnému zvýšení schopnosti monitorovat a vyhodnocovat kybernetické události v důležitých sítích ISVS a k posílení bezpečnostního povědomí zaměstnanců veřejné správy.

Legislativní změny:

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

Vyhláška 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Vyhláška 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

průběžně aktualizovaný Seznam prvků kritické infrastruktury

Cíle projektového okruhu:

1) Zvýšení odolnosti informačních systémů veřejné správy proti kybernetickým hrozbám

Indikátor:

Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti

Vazba na hlavní aktivity Implementačního plánu:

Hlavní aktivity Implementačního plánu	Vazba (ANO/NE)
1. Koncepční zajištění fungování eGovernmentu a realizace projektů ICT (včetně legislativy a řízení investic do ICT)	NE
2. Vzdělávání v oblasti ICT a eGovernmentu včetně kybernetické bezpečnosti	ANO
3. Dobudování eGovernmentu	NE
4. Prosazování principu Open Data	NE
5. Rozšíření, propojení a konsolidace datového fondu veřejné správy a jeho efektivní a bezpečné využívání dle jednotlivých agend	ANO
6. Dobudování infrastruktury a úložišť informačních a komunikačních systémů veřejné správy a eGovernmentu	ANO
7. Zvýšení kybernetické bezpečnosti IKT VS	-
8. Realizace systému elektronické identifikace, autentizace a autorizace a dalších služeb vytvářejících důvěru	NE
9. Elektronizace podpůrných procesů	NE

Návaznost na předchozí projekty a výzvy:

Operační program	Výzva	V čem navazuje
Integrovaný operační program	19	V rámci výzvy zaměřené na rozvoj krajských služeb eGovernmentu byly podporovány aktivity týkající se: • managementu bezpečnostních informací a událostí (SIEM) • systémů pro prevenci a detekci průniku (IPS, IDS) • nástrojů pro zabezpečení rozhraní sítí a provozu aplikací včetně filtrace komunikace různých typů sítí • nástrojů pro sběr a analýzu síťového provozu • zabezpečení uživatelských sítí a přístupů • aktualizace bezpečnostních politik • penetračního testování
Integrovaný operační program	22	V rámci výzvy zaměřené na konsolidaci IT a nové služby TC obcí byly podporovány aktivity týkající se nákupu a implementace bezpečnostních prvků - firewally, loadbalancery, reverzní proxy, aplikační firewally, IDS, IPS, SIEM řešení - sběr logů, událostí, analýza síťového provozu, elektronická autentizace a identifikace uživatele v síti, včetně prvků fyzické bezpečnosti.

Řešené architektonické oblasti (vazba na architekturu):

Projektový okruh kybernetické bezpečnosti může mít z hlediska architektonického dopad do všech vrstev. Na úrovni infrastruktury to může znamenat segmentaci sítě případně zapojení nových aktivních prvků, na úrovni technologie nasazení nových technických opatření, na úrovni aplikační jsou nejpravděpodobnější změny funkcí jako je logování případně identifikace a autentizace. Na úrovni procesní by měly být doplněné procesy spojené s řízením bezpečnosti a procesy, které jsou organizačními bezpečnostními opatřeními.

Vzor: Kybernetická bezpečnost

Předpoklady a podmínky (max. 5 <u>obecných</u> předpokladů a podmínek realizace):

1) Zajištění důvěrnosti - informační systém musí zajistit důvěrnost uložených dat, tedy, že data budou dostupná pouze oprávněným osobám.

2) Zajištění integrity - informační systém musí zajistit integritu uložených dat a informačního systému samotného, tedy, že data a informační systém budou upravované pouze definovaným způsobem oprávněnými osobami.

3) Zajištění dostupnosti - informační systém musí zajistit dostupnost uložených dat a informačního systému samotného, tedy, že oprávněné osoby mohou pracovat s daty a informačním systémem tehdy, když potřebují.