Kontrolní závěr z kontrolní akce

19/26

Budování kybernetické bezpečnosti České republiky

Kontrolní akce byla zařazena do plánu kontrolní činnosti Nejvyššího kontrolního úřadu (dále také „NKÚ“) na rok 2019 pod číslem 19/26. Kontrolní akci řídil a kontrolní závěr vypracoval člen NKÚ Ing. Roman Procházka.

Cílem kontroly bylo prověřit, zda činnosti hlavních subjektů podílejících se na zajištění kybernetické bezpečnosti ČR a míra efektivity jejich vzájemné spolupráce vedou k jejímu zvyšování ve smyslu cílů a aktivit definovaných *Národní strategií kybernetické bezpečnosti České republiky 2015–2020* a *Akčního plánu ke strategii 2015–2020*.

Kontrolované osoby:
Národní úřad pro kybernetickou a informační bezpečnost, Brno (dále také „NÚKIB“),
Ministerstvo vnitra (dále také „MV“).

Kontrola byla prováděna u kontrolovaných osob v období od října 2019 do června 2020.

Kontrolováno bylo období od roku 2015 do roku 2020.

Pozn.: Právní předpisy uvedené v tomto kontrolním závěru jsou aplikovány ve znění účinném pro kontrolované období.

K o l e g i u m N K Ú na svém XIV. jednání, které se konalo dne 14. září 2020,

s c h v á l i l o usnesením č. 8/XIV/2020

k o n t r o l n í z á v ě r v tomto znění:

Kybernetická bezpečnost České republiky v číslech

Česká republika

348 informačních systémů[1]

111 systémů kritické informační infrastruktury (KII)
179 významných informačních systémů (VIS)
58 informačních systémů základních služeb (ISZS)

2 787 mil. Kč[2]

Odhad celkových peněžních prostředků vynaložených ministerstvy a Úřadem vlády ČR na zajištění kybernetické bezpečnosti v letech 2015 až 2019

Národní úřad pro kybernetickou a informační bezpečnost

916

Počet kybernetických incidentů hlášených vládnímu CERT od roku 2017 do poloviny roku 2020, z toho 31% připadalo na incidenty za první polovinu roku 2020.

884 mil. Kč

Výdaje v kapitole NÚKIB od jeho vzniku do konce roku 2019

112 mil. Kč

Peněžní prostředky Výzvy č. 10, které NÚKIB využil v rámci 2 projektů zaměřených na kybernetickou bezpečnost

Ministerstvo vnitra

19 informačních systémů[3]

12 KII
7 VIS

750 mil. Kč[2]

Odhad peněžních prostředků vynaložených MV na zajištění kybernetické bezpečnosti v letech 2015 až 2019

0 Kč

MV nečerpalo v rámci Výzvy č. 10 žádné peněžní prostředky.

---

[1] **KII** – systém, u kterého by narušení funkce mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu, **VIS** – systém, u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci, **ISZS** – systém, na jehož fungování je závislé poskytování základní služby a narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura, chemický průmysl.

[2] Jedná se o odhad peněžních prostředků získaný NÚKIB prostřednictvím dotazníkových šetření v letech 2018 a 2019 u vybraných organizačních složek státu.

[3] Údaj se týká pouze organizační složky státu Ministerstvo vnitra. Kybernetická bezpečnost je však na Ministerstvu vnitra řešena z resortního pohledu. V případě resortu Ministerstva vnitra se tak jedná celkem o 30 informačních systémů (19 KII a 11 VIS). Podrobnější informace jsou k tomuto uvedeny v části II. tohoto kontrolního závěru.

I. SHRNUTÍ A VYHODNOCENÍ

Kontrolovanými osobami byly NÚKIB, který dozoruje kybernetickou a informační bezpečnost státu, a dále MV, které je mj. ústředním orgánem pro oblast informačních systémů státní správy, elektronickou identifikaci a služby vytvářející důvěru. NÚKIB byl zřízen k 1. 8. 2017 a převzal agendu kybernetické bezpečnosti (dále také „KB“) státu od NBÚ. Celkové výdaje, které NÚKIB vynaložil v souvislosti s výkonem svých činností v letech 2017 až 2019, činily přibližně 884 mil. Kč. V kontrole byly prověřeny zejm. činnosti NÚKIB a MV v oblastech nastavení a následného zajišťování kybernetické bezpečnosti České republiky (dále také „ČR“) a plnění cílů a aktivit *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* a *Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020* (dále také „AP NSKB“). Podle výsledků dotazníkových šetření provedených NÚKIB v letech 2018 a 2019 vynaložila ministerstva a Úřad vlády ČR na zajištění KB státu mezi lety 2015 až 2019, dle jejich odhadu, téměř 2,8 mld. Kč.

NKÚ kontrolou ověřil, že činnosti hlavních subjektů podílejících se na zajištění KB ČR a míra efektivity jejich vzájemné spolupráce vedou k jejímu zvyšování. Zvyšování KB státu a míru efektivity spolupráce NÚKIB a MV vyhodnocoval NKÚ na základě plnění 57 vybraných úkolů AP NSKB[4]. NÚKIB a MV se dařilo v kontrolovaném období 2015 až 2020 plnit většinu těchto úkolů. Z 57 prověřovaných úkolů zjistil NKÚ nedostatky u osmi z nich.

MV je ústředním orgánem státní správy mj. pro oblast informačních systémů (dále také „IS“) veřejné správy. Resort MV[5] je z pohledu počtu spravovaných systémů kritické informační infrastruktury a významných informačních systémů nejvýznamnějším resortem státní správy. MV uvedlo, že pro naplnění požadavků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, dále také „ZKB“), chybělo resortu MV k roku 2020[6], podle výsledků dotazníkového šetření provedeného NÚKIB, přibližně 309 mil. Kč. I přes uváděný nedostatek finančních prostředků ze státního rozpočtu se MV nepodařilo využít výzvy č. 10 – *Kybernetická bezpečnost* (dále také „Výzva č. 10“) a nečerpalo jejím prostřednictvím prostředky z fondů EU alokovaných v programovém období 2014+ ve prospěch zvyšování KB. Na nastavení Výzvy č. 10 se přitom MV podílelo ve spolupráci s MMR a dalšími subjekty. Zároveň NKÚ zjistil, že MV nerealizovalo každoročně část opatření, která byla navržena v jednotlivých plánech zvládání rizik[7], což představuje zvýšené bezpečnostní riziko z pohledu KB.

Na projekty KB mohli oprávnění žadatelé[8] čerpat prostředky z Výzvy č. 10, a to až do výše 1,3 mld. Kč. Výzvu č. 10 vyhlásilo MMR dne 21. 10. 2015. NÚKIB z Výzvy č. 10 vyčerpal

---

4 NKÚ prověřil 57 z celkového počtu 141 úkolů AP NSKB. Ke kontrole NKÚ vybral primárně ty úkoly AP NSKB, jejichž plnění vyžadovalo spolupráci MV a NÚKIB nebo ve kterých figuroval NÚKIB či MV jako gestor. Nejednalo se o všechny úkoly v gesci NÚKIB a MV.

5 KB je na MV řešena z resortního pohledu skrze jednotný systém řízení bezpečnosti informací.

6 Cílem dotazníkového šetření NÚKIB v letech 2018 a 2019 bylo zjistit rozdíl mezi stavem prostředků na oblast KB a jejich potřebou v roce 2020.

7 Jedná se o základní dokumenty MV upravující jeho směřování v oblasti KB.

8 Tj. organizační složky státu, příspěvkové organizace OSS, státní organizace, státní podniky, kraje, organizace zřizované nebo zakládané kraji, obce (kromě Prahy), organizace zřizované nebo zakládané obcemi (kromě Prahy).

celkem 112 mil. Kč na dva projekty. Největší objem finančních prostředků Výzvy č. 10 (přibližně 903 mil. Kč) připadl na projekty KB u zdravotnických zařízení, z nichž velká část na základě platných kritérií nespadá mezi subjekty spravující KII, VIS nebo ISZS. Ve vztahu k pokračující elektronizaci zdravotnictví byla potřeba investic do KB informačních a komunikačních systémů zdravotnických zařízení prostřednictvím Výzvy č. 10 opodstatněná.

Kybernetické útoky z přelomu let 2019 a 2020 na zdravotnická zařízení však ukázaly, že ač se nejednalo o povinné subjekty podle ZKB, měla by série kybernetických útoků na tato zařízení významný dopad na funkčnost zdravotnického systému ČR.

Schopnost NÚKIB a MV naplňovat klíčové aktivity KB byla závislá na odborných a vysoce specializovaných personálních kapacitách, jejichž zajištění a udržení zůstává pro státní správu dlouhodobě problematické.

Spolupráce mezi NÚKIB a MV nebyla do doby ukončení kontroly formálně nastavena, k čemuž mělo dojít i prostřednictvím naplnění vybraných úkolů AP NSKB. Mimo jiné měl být vytvořen podrobný model a schéma fungování spolupráce v oblasti KB. Spolupráce tak funguje zejm. na neformální úrovni a ad hoc v závislosti na aktuálních potřebách, což NKÚ ověřil na příkladu řešení aktuálních kybernetických útoků. Tento stav však podle názoru NKÚ představuje z dlouhodobého hlediska riziko pro udržení kontinuity spolupráce a potřebnou akceschopnost v případě personálních změn u obou nebo i jen jedné z kontrolovaných institucí.

Celkové vyhodnocení vyplývá z následujících skutečností:

Plnění úkolů AP NSKB

NÚKIB a MV se podařilo většinu z 57 NKÚ prověřovaných úkolů AP NSKB úspěšně naplnit. Dílčí nedostatky NKÚ vyhodnotil u osmi úkolů. Zejména pak ve vtahu k nastavení spolupráce klíčových aktérů KB. Efektivita spolupráce NÚKIB, MV a dalších subjektů může být do budoucna negativně ovlivněna tím, že doposud nedošlo k jejímu formálnímu nastavení a ukotvení mezi těmito orgány. K tomu mělo dojít i v rámci NKÚ prověřovaných vybraných úkolů AP NSKB. Spolupráce však spočívá na osobních vazbách a řešení problémů ad hoc dle potřeb.

Spolupráce NÚKIB a MV při řešení mimořádných kybernetických událostí i přes výše uvedené fungovala. Obě kontrolované instituce se na přelomu let 2019-2020 společně podílely na řešení kybernetických útoků na zdravotnická zařízení[9]. Personální kapacity NÚKIB i MV jsou však při souběhu několika mimořádných událostí velmi omezené.

Financování kybernetické bezpečnosti státu

I přes avizované vynaložení 2,8 mld. Kč za období let 2015 až 2019 chyběly ministerstvům a Úřadu vlády ČR, podle jejich odhadu[10], řádově stovky milionů korun na plné zajištění KB podle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících

[9] A to i v případě, že se jednalo o subjekty, na které se nevztahovaly povinnosti vyplývající ze ZKB.

[10] Jedná se o odhad peněžních prostředků získaný NÚKIB prostřednictvím dotazníkových šetření v letech 2018 a 2019. NKÚ tento odhad neověřoval.

zákonů (zákon o kybernetické bezpečnosti). Odhad vyčíslený MV představoval 309 mil. Kč. Resort MV je z pohledu počtu spravovaných systémů kritické informační infrastruktury (dále také „KII“)[11] a významných IS (dále také „VIS“) státu nejvýznamnějším resortem. Celkově resort MV spravoval k roku 2020 19 KII a 11 VIS. Vývoj počtu kybernetických útoků na IS vykazuje rostoucí trend. U MV v posledních letech došlo k jejich nárůstu nejméně o 220 %.

Ve vztahu k financování KB shledal NKÚ nedostatky v systému sledování vynakládaných peněžních prostředků. NÚKIB neměl v průběhu kontrolovaného období informace o celkové výši vynakládaných peněžních prostředků jednotlivých kapitol státního rozpočtu či celého státu na KB, přičemž pro zjištění jejich výše realizoval v letech 2018 a 2019 celkem čtyři dotazníková šetření u ministerstev a Úřadu vlády ČR. V případě MV nebyly peněžní prostředky vynakládané na KB systematicky a pravidelně sledovány, což představuje omezení pro plnění stanovené povinnosti, aby správce kapitoly soustavně sledoval a vyhodnocoval hospodárnost, efektivnost a účelnost vynakládání výdajů ve své kapitole.[12]

S oblastí peněžních prostředků se úzce pojí také oblast lidských zdrojů. Získání a udržení odborných kapacit je pro obě instituce trvající výzvou. NÚKIB se dlouhodobě potýkal s fluktuací odborných zaměstnanců na úrovni 10 %. MV se taktéž dlouhodobě potýkalo s vysokou fluktuací na příslušných pracovních pozicích a některé klíčové bezpečnostní role zajišťovalo externě, a to i přes skutečnost, že může využívat institutu klíčového služebního místa, neboť se na něj vztahuje zákon č. 234/2014 Sb., o státní službě.

Využití peněžních prostředků ESIF na zajištění kybernetické bezpečnosti

Ministerstva a další subjekty měly v kontrolovaném období možnost čerpat peněžní prostředky evropských strukturálních a investičních fondů (dále také „ESIF“) na projekty v oblasti KB z výzvy *Integrovaného regionálního operačního programu* (dále také „IROP“) č. 10 – *Kybernetická bezpečnost*, a to až do výše 1 340 mil. Kč. Na projekty realizované subjekty státního sektoru připadlo po posouzení řídicím orgánem 799,6 mil. Kč, z toho na projekty ústředních orgánů státní správy pouze 121 mil[13]. Kč. Z této částky navíc představovaly 112 mil. Kč projekty NÚKIB. MV i přes svoji pozici v rámci státní správy peněžní prostředky z Výzvy č. 10 nečerpalo. MV podalo celkem dvě žádosti o podporu v listopadu 2017, tedy více než 2 roky po vyhlášení Výzvy č. 10. Pro převis žádostí nad alokací výzvy však byly tyto žádosti ze strany řídicího orgánu zamítnuty. Největší objem finančních prostředků z celkové alokace Výzvy č. 10 (přibližně 903 mil. Kč) připadl na projekty zdravotnických zařízení, z nichž některá mohla podávat žádosti na své projekty až po rozšíření okruhu podporovaných aktivit Výzvy č. 10, tj. po 19 měsících od jejího vyhlášení.

NKÚ na základě skutečností zjištěných kontrolou doporučuje NÚKIB v rámci výkonu svěřené koordinační role prověřit nastavení kritérií pro určení poskytovatelů základních služeb v odvětví zdravotnictví a příp. provést jejich revizi.

[11] Podle ZKB se jedná o informační a komunikační systémy kritické informační infrastruktury. Pro zjednodušení je však užíván v kontrolním závěru pojem „systémy kritické informační infrastruktury“ a zkratka „KII“.

[12] Ustanovení § 39 zákona č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla).

[13] Zdroj dat: informační systém *MS2014+*, podrobněji viz kapitola IV. tohoto kontrolního závěru.

II. INFORMACE O KONTROLOVANÉ OBLASTI

NÚKIB je ústředním správním úřadem pro oblast KB. Vznikl na základě zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některých dalších zákonů. NÚKIB byl zřízen k 1. 8. 2017 a převzal agendu KB státu od NBÚ. NÚKIB má mj. zajišťovat prevenci, vzdělávání a metodickou podporu v oblasti KB a ve vybraných oblastech ochrany utajovaných informací, vydávat opatření a působit jako koordinační orgán ve stavu kybernetického nebezpečí. Dále provádí analýzu a monitoring kybernetických hrozeb a rizik. NÚKIB také provádí příslušnou kontrolu dle ZKB. Celkové výdaje na zajištění činností NÚKIB v letech 2017 až 2019 činily přibližně 884 mil. Kč.

MV plní podle zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, mj. koordinační úlohu pro informační a komunikační technologie. K 31. 1. 2020 spravovalo MV celkem 12 KII, což představovalo 22 % ze všech KII ve správě OSS. Z pohledu resortu MV, tj. po započtení dalších 7 KII, pak tento podíl představoval cca 35 %. K 31. 1. 2020 dále MV spravovalo 7 VIS, resp. 11 z resortního pohledu, tj. při započtení VIS ve správě Policie České republiky (dále také „PČR“) a Správy základních registrů.

Kybernetická bezpečnost

KB je specifickou oblastí výpočetní techniky. Jejím cílem je zajistit ochranu informací a majetku před krádeží, zneužitím, korupcí či přírodní katastrofou s tím, že chráněné informace musí zůstat přístupné svým uživatelům. Právní rámec KB státu a práva a povinnosti subjektů veřejné správy vymezuje ZKB a jeho prováděcí předpisy.

Vládní CERT (GovCERT)

Součástí NÚKIB je i odbor vládní CERT. Úlohou tohoto odboru je působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Je klíčový při ochraně KII a VIS podle ZKB a jeho prováděcích předpisů. Neméně důležitou roli hraje také při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

***Národní strategie kybernetické bezpečnosti na období let 2015–2020* a AP NSKB**

NÚKIB a MV se významně podílejí na rozvoji informačních a komunikačních technologií (dále také „ICT“) ve veřejné správě ČR a jejím zabezpečení. K problematice KB vydal NBÚ *Národní strategii kybernetické bezpečnosti na období let 2015–2020*. Ta byla schválena usnesením vlády ČR ze dne 16. února 2015 č. 105. Dne 25. května 2015 byl pak usnesením vlády ČR č. 382 schválen AP NSKB. Ten obsahoval celkem 141 úkolů rozdělených mezi jednotlivá ministerstva a další orgány veřejné správy. Výše zmíněná strategie a AP NSKB přesahují v některých oblastech ustanovení ZKB.

III. ROZSAH KONTROLY

Cílem kontroly bylo prověřit, zda činnosti hlavních subjektů podílejících se na zajištění kybernetické bezpečnosti ČR a míra efektivity jejich vzájemné spolupráce vedou k jejímu zvyšování ve smyslu cílů a aktivit definovaných *Národní strategií kybernetické bezpečnosti České republiky 2015–2020* a *Akčního plánu ke strategii 2015–2020*. V souvislosti s výše uvedeným prověřil NKÚ také realizaci tří projektů v oblasti KB. Dva z těchto projektů realizoval NÚKIB a jeden projekt realizovalo MV.

NÚKIB dozoruje kybernetickou a informační bezpečnost státu a plnění povinností dle ZKB. MV je mj. ústředním orgánem státní správy pro oblast informačních systémů veřejné správy, elektronickou identifikaci a služby vytvářející důvěru. Zároveň MV, resp. resort MV, spravuje 30 IS (19 KII, 11 VIS) spadajících pod ZKB. Zvyšování kybernetické bezpečnosti státu a míru efektivity spolupráce NÚKIB a MV vyhodnocoval NKÚ na základě vybraných úkolů AP NSKB. Z celkového počtu 141 úkolů AP NSKB NKÚ vybral 57 úkolů s ohledem na jejich gestory a spolugestory a zároveň s cílem prověřit primárně úkoly vyžadující spolupráci NÚKIB a MV.

U NÚKIB se kontrola zaměřila na činnosti tohoto úřadu z pohledu gestora KB státu, přičemž celkové výdaje, které NÚKIB vynaložil v souvislosti s výkonem svých činností v letech 2017 až 2019, činily přibližně 884 mil. Kč. Jednalo se mimo jiné o činnosti v oblastech: financování KB státu, personální kapacity NÚKIB pro její zajištění, spolupráce NÚKIB a MV při vybraných činnostech a podíl NÚKIB na nastavení pravidel pro čerpání prostředků na KB z evropských strukturálních a investičních fondů (dále také „ESIF“). Dále se NKÚ zaměřil na hospodárnost a účelnost vynaložení peněžních prostředků na projekty *Systém detekce kybernetických bezpečnostních incidentů ve vybraných informačních systémech veřejné správy* a projekt *Ochrana vnějšího perimetru*.

V případě MV se kontrola zaměřila mimo jiné na plánování a rozvoj KB jím spravovaných IS, zajištění financování rozvoje KB, personální kapacity MV v této oblasti, spolupráci MV a NÚKIB při vybraných činnostech a podíl MV na nastavení pravidel pro čerpání prostředků na KB z ESIF. Dále se NKÚ zaměřil na účelnost vynaložení peněžních prostředků na projekt Dohledového centra eGovernmentu (dále také „DCeGOV“).

V souvislosti s aktuálním děním prověřil NKÚ také činnosti NÚKIB a MV při řešení kybernetických útoků na zdravotnická zařízení a další subjekty, a to zejména v souvislosti s vytížením jejich personálních kapacit.

Kontrolovaný objem peněžních prostředků byl 828 828 806 Kč.

IV. PODROBNÉ SKUTEČNOSTI ZJIŠTĚNÉ KONTROLOU

Plnění úkolů AP NSKB

Zvyšování kybernetické bezpečnosti státu a míru efektivity spolupráce NÚKIB a MV vyhodnocoval NKÚ zejm. na základě naplnění či nenaplnění vybraných úkolů AP NSKB a spolupráce výše uvedených subjektů při plnění těchto úkolů. Z celkového počtu 141 úkolů AP NSKB prověřoval NKÚ naplnění/nenaplnění a spolupráci u 57 vybraných úkolů. NKÚ vybral tyto úkoly s ohledem na jejich gestory a spolugestory a zároveň s cílem prověřit primárně úkoly vyžadující spolupráci NÚKIB a MV. NÚKIB v rámci plnění povinnosti vycházející z usnesení vlády ČR ze dne 25. května 2015 č. 382 vytvořil předpoklady pro spolupráci se zástupci jednotlivých subjektů, které se podílejí na plnění úkolů AP NSKB. Dílčí nedostatky NKÚ vyhodnotil u 8 úkolů, a to zejm. ve vtahu k nastavení a ukotvení spolupráce klíčových aktérů KB.

Tabulka č. 1: Prověřované úkoly AP NSKB se zjištěnými nedostatky

Číslo opatření AP NSKB	Znění	Gestor	Spolugestor	Stav
A.1.01	Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti	NÚKIB	MV	Úkol za NÚKIB nesplněn, MV se na plnění úkolu nepodílelo
A.1.02	Provést analýzu agend v rámci problematiky kybernetické bezpečnosti a na jejím základě definovat národní zájmy a priority v této oblasti	NÚKIB		Úkol nesplněn
A.1.03	Provádět technická i netechnická národní cvičení kybernetické bezpečnosti	NÚKIB	MV	Úkol za NÚKIB splněn, úkol za MV částečně splněn
A.2.02	Vytvořit komunikační matici mezi vrcholovými aktéry kybernetické bezpečnosti (národní aktéři, KII, VIS)	NÚKIB		Úkol částečně splněn
A.4.01	Vytvořit efektivní model pro sdílení informací o zahraničních aktivitách mezi NBÚ a ostatními relevantními subjekty	NÚKIB	MV	Úkol za NÚKIB splněn, MV se na plnění úkolu nepodílelo
C.5.02	Vytvořit na základě dokončení mapování zabezpečovacích prvků u KII a VIS automatizovanou platformu na sdílení informací o kybernetických bezpečnostních hrozbách a incidentech vybraným ohroženým subjektům	NÚKIB		Úkol nesplněn
G.2.03	Společně plánovat jednotlivé nákupy pro výkonná pracoviště OIK a znalecká pracoviště počítačové analýzy s garancí vázanosti plánovaných prostředků v plánovaných rozpočtech pro další údobí	MV (PČR)		Úkol nesplněn
G.5.01	Rozšířit kurzy kvalifikační přípravy o základní znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií a zavést elektronický nebo obdobně plošně nasaditelný systém průběžného vzdělávání	MV (PČR)		Úkol částečně splněn

Zdroj: vypracoval NKÚ.

Cíl A.1.01 nebyl naplněn, protože NÚKIB ani MV nepředložil žádný dokument zachycující schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti. Spolupráce mezi NÚKIB a MV funguje zejména na neformální úrovni a s ohledem na aktuální potřeby.

Cíl A.1.02 nebyl naplněn, protože NÚKIB nepředložil žádné výstupy analýzy agend týkající se problematiky KB ani definici národních zájmů a priorit v této oblasti.

NÚKIB naplnil cíl A.1.03, protože v letech 2015 až 2019 byla provedena řada cvičení kybernetické bezpečnosti technického i netechnického charakteru. MV tento cíl jakožto spolugestor naplnilo pouze částečně, neboť se těchto cvičení mělo účastnit průběžně, avšak zúčastnilo se tří cvičení, a to pouze v letech 2018 a 2019.

Cíl A.2.02 naplnil NÚKIB pouze částečně, neboť vytvořil databázi kontaktů, avšak nevytvořil komunikační matici mezi vrcholovými aktéry KB, která měla vzniknout podle cíle nastaveného v akčním plánu.

Cíl A.4.01 splnilo NBÚ již v roce 2015 (před vznikem NÚKIB) tím, že vytvořilo model sdílení informací o zahraničních aktivitách a nastavilo rámec spolupráce mezi NBÚ/NCKB a ostatními relevantními subjekty. Za tímto účelem byla vytvořena pracovní skupina pro harmonizaci mezinárodních aktivit na národní úrovni. MV se na plnění úkolu jako spolugestor nezapojilo.

NÚKIB nenaplnil cíl C.5.02, neboť ani čtyři roky po termínu nevytvořil na základě dokončení mapování zabezpečovacích prvků u KII a VIS automatizovanou platformu na sdílení informací o kybernetických bezpečnostních hrozbách a incidentech.

MV (PČR) nenaplnilo cíl G.2.03, neboť plánované nákupy HW a SW nebyly pořizovány z vázaných (garantovaných) plánovaných peněžních prostředků, ale z peněžních prostředků evropských fondů a mimořádné dotace ve výši 30 mil. Kč (jednalo se o přesun finančních prostředků v rámci kapitoly MV). Do doby ukončení kontroly nebyly schváleny finanční prostředky na periodickou obnovu materiálně technického vybavení, což může negativně ovlivnit udržitelnost.

MV (PČR) splnilo úkol G.5.01 částečně, neboť do doby ukončení kontroly nezavedlo elektronický nebo jiný podobně plošně nasaditelný systém průběžného vzdělávání. Kurzy kvalifikační přípravy MV (PČR) rozšířilo o základní znalosti a dovednosti spojené s kriminalitou páchanou prostřednictvím informačních a komunikačních technologií.

Spolupráce NÚKIB, MV a ostatních orgánů zajišťujících KB státu nebyla doposud formálně nastavena a ukotvena. K tomu mělo dojít i v rámci plnění některých výše uvedených úkolů AP NSKB, zejm. úkolu A.1.01 – *Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti*, a spolupráce těchto subjektů tak spočívá zejména na osobních vazbách a dohodách ad hoc.

V souvislosti s nastavením předávání hodnoticích zpráv o plnění jednotlivých úkolů AP NSKB upozorňuje NKÚ, že NÚKIB nastavený systém nevedl k získání zpráv o plnění AP NSKB od všech dotazovaných subjektů. Např. MV v letech 2015, 2016 a 2018 nepředávalo NÚKIB veškeré požadované informace o úkolech, které mělo v gesci nebo spolugesci, a zároveň tak nepostupovalo podle ustanovení § 21 zákona č. 2/1969 Sb., když svým postupem důsledně neposkytovalo součinnost při naplňování AP NSKB podle úkolu III/1b uloženého usnesením vlády ČR ze dne 25. května 2015 č. 382.

NKÚ nad rámec plnění AP NKSB prověřoval také další oblasti KB vyžadující spolupráci NÚKIB a MV. NKÚ ověřil, že NÚKIB v oblasti přípravy právních předpisů aktivně spolupracoval s MV jak na samotných zněních jednotlivých materiálů, tak i na ostatních s tím souvisejících dokumentech. NÚKIB také jakožto gestor KB vydával doporučení směřující k jednotlivým oblastem ZKB a komunikoval s Odborem hlavního architekta eGovernmentu MV (dále také „OHA“) při posuzování ICT projektů týkajících se KB. Tato komunikace probíhala nepravidelně formou oficiálních dopisů, a to zejména v případě vzniku potřeby konzultovat otázky související s KB.

V období od prosince 2019 do doby ukončení kontroly NKÚ došlo na území ČR k řadě významných kybernetických útoků, zejména s dopady na provoz nemocnic. První případ nastal dne 11. 12. 2019 v nemocnici v Benešově. K dalšímu útoku došlo dne 13. 3. 2020, kdy byla napadena počítačová síť brněnské fakultní nemocnice v Bohunicích. NÚKIB a MV se podílely na řešení těchto kybernetických incidentů, a to i v případě, kdy tento incident nastal u subjektu, který nespadal jako tzv. povinný subjekt pod ZKB[14]. V případě výskytu několika incidentů současně však existuje riziko, že NÚKIB a MV nebudou mít dostatek personálních kapacit, které by mohly na jejich řešení využít.

Financování kybernetické bezpečnosti státu

NÚKIB, potažmo stát, neměl v průběhu kontrolovaného období informace o celkové výši vynakládaných peněžních prostředků jednotlivých kapitol státního rozpočtu či celého státu na KB. Vzhledem k výše uvedené absenci informací o vynakládaných peněžních prostředcích a potřebě jejich získání mj. v souvislosti s novou vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), prováděl NÚKIB v letech 2018 a 2019 celkem čtyři dotazníková šetření u ministerstev a Úřadu vlády ČR[15].

Z dotazníkových šetření provedených NÚKIB vyplynulo, že na zajištění KB informačních systémů státu podle ZKB a souvisejících vyhlášek vynaložila ministerstva a Úřad vlády ČR v letech 2015 až 2019 podle jejich odhadu téměř 2,8 mld. Kč. V případě MV činil odhad celkových vynaložených peněžních prostředků na KB v období 2015–2019 cca 750 mil. Kč (pouze za správce kapitoly). K roku 2020 vyčíslili respondenti dotazníkových šetření NÚKIB potřebné (chybějící) finanční prostředky na zajištění KB podle požadavků ZKB v jejich kapitolách řádově ve stovkách milionů korun. Odhad vyčíslený MV představoval 309 mil. Kč. NKÚ prověřil, že MV nerealizovalo v některých oblastech KB veškerá potřebná opatření, která byla navržena v jednotlivých plánech zvládání rizik[16], což představuje zvýšené bezpečnostní riziko pro KB resortu MV. Jednalo se např. o opatření v oblastech: rozvoje DCeGOV, zabezpečení některých KII a VIS podle ZKB nebo rozvoje systému řízení bezpečnosti informací. V kontrolovaném období přitom MV čelilo vzrůstajícímu počtu kybernetických útoků, když ve srovnání let 2016 až 2019 došlo k jejich nárůstu nejméně o 220 %. Například v roce 2019 MV evidovalo 397 kybernetických útoků. I z pohledu celé ČR jako celku narůstal v posledních letech počet kybernetických útoků, s čímž souvisí i rostoucí počet kybernetických incidentů,

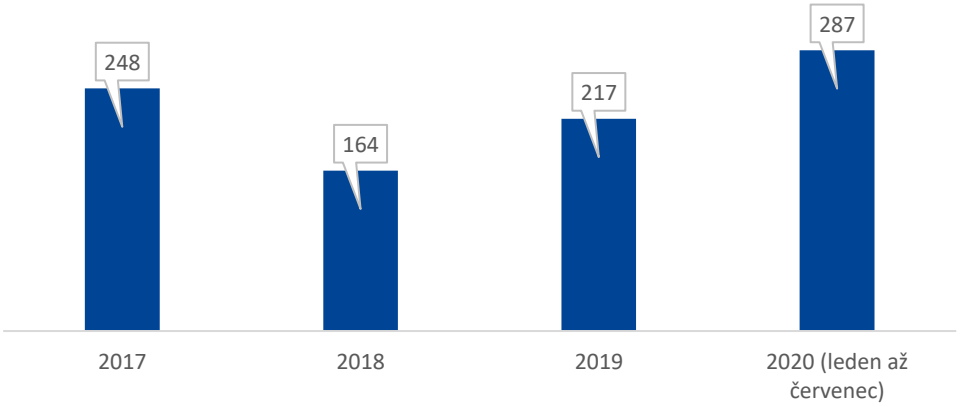
[14] NÚKIB se na řešení incidentů podílel podle ustanovení § 20 písm. l) zákona č. 181/2014 Sb., který mu umožňuje podílet se na řešení kybernetického incidentu i u subjektů, které nejsou uvedeny v ustanovení § 3 ZKB, pokud má vážný dopad a kapacity mu to umožňují. MV se na řešení incidentu v Benešově podílelo na žádost NÚKIB, neboť mělo zkušenosti s podobným typem útoku.

[15] Před průzkumy realizovanými NÚKIB v letech 2018 a 2019 provádělo podobné šetření i MV.

[16] Jedná se o základní dokumenty resortu MV upravující jeho směřování v oblasti KB.

které byly hlášeny vládnímu CERT, resp. NÚKIB. Jen za prvních 6 měsíců bylo NÚKIB nahlášeno více incidentů než za celý rok 2019, což ilustruje následující graf.

Graf č. 1: Vývoj počtu kybernetických incidentů hlášených vládnímu CERT



Zdroj: vypracoval NKÚ na základě dat od NÚKIB.

S oblastí peněžních prostředků se pojí také oblast lidských zdrojů. Fluktuace zaměstnanců NÚKIB – specialistů vykonávajících odbornou činnost – se pohybovala na úrovni 10 %, což z dlouhodobého pohledu představuje riziko snížení schopnosti zabezpečovat KB státu. V případě MV za zajišťování implementace ZKB a za nastavení, provoz, rozvoj a kontrolu systému zajištění KB[17] zodpovídalo oddělení KB. MV se však dlouhodobě potýkalo s nedostatkem personálních kapacit pro jeho obsazení. Obsazenost 12 systemizovaných míst oddělení KB se v kontrolovaném období pohybovala mezi 66 % až 83 %, přičemž ale v době ukončení kontroly bylo pouze 25 % pozic obsazeno zaměstnanci, kteří v oddělení KB působili déle než 3 roky, a to i přes využívání institutu klíčového služebního místa. NÚKIB nemůže využívat institutu klíčového služebního místa, neboť zákon č. 234/2014 Sb., o státní službě, se na jeho zaměstnance nevztahuje, na rozdíl od MV. MV navíc v období let 2016–2020 zajišťovalo externě dvě klíčové bezpečnostní role, tzn. architekta KB a auditora KB, a to na základě smluv o poskytování konzultačních služeb v celkové výši 2,25 mil. Kč. Zjištěná skutečnost představuje riziko z hlediska dlouhodobého rozvoje a uchování znalostí v oblasti KB uvnitř MV.

Využití peněžních prostředků ESIF na zajištění kybernetické bezpečnosti

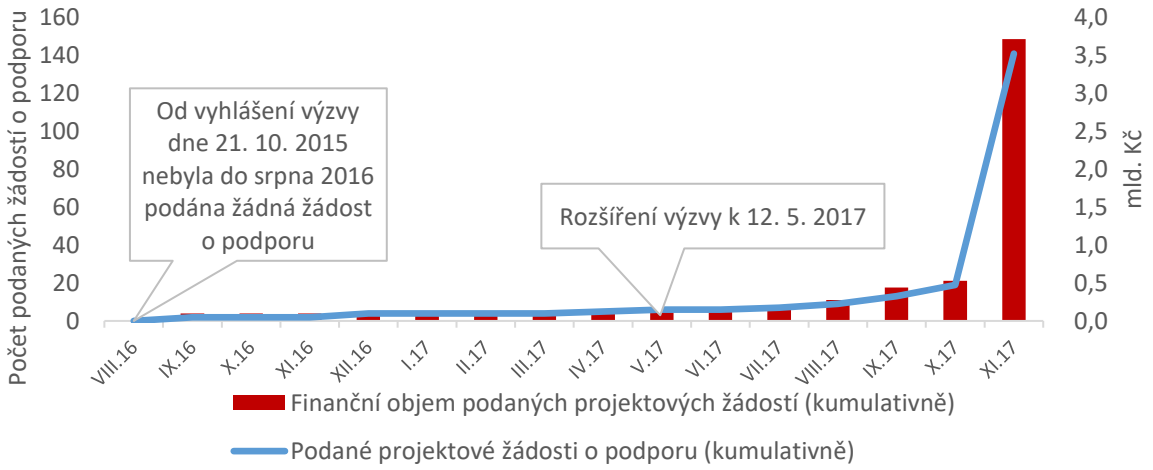
Ministerstva, Úřad vlády ČR a další subjekty měly v kontrolovaném období možnost čerpat peněžní prostředky na projekty v oblasti KB v rámci průběžné Výzvy č. 10[18]. Ta byla MMR vyhlášena dne 21. 10. 2015. Při vyhlášení byla hlavní podporovaná aktivita zaměřena pouze na zabezpečení KII a VIS dle ZKB. Od svého vyhlášení však prošla Výzva č. 10 celkem sedmi změnami, přičemž změnou ze dne 12. 5. 2017 došlo mj. k úpravě hlavní podporované aktivity. Oprávnění žadatelé mohli následně žádat o peněžní prostředky na zabezpečení nejen KII a VIS, ale i ISZS a ostatních IS a KS, které nespadají pod dříve uvedené kategorie systémů. Celková alokace výzvy dosahovala výše cca 1 340 mil. Kč (dotace z EFRR). Podmínkou poskytnutí dotace

[17] KB je na MV řešena z resortního pohledu. Z pohledu resortu MV se jednalo o zajišťování KB u 19 KII a 11 VIS.

[18] Ve vztahu k nastavení pravidel pro čerpání prostředků na KB z ESIF NKÚ ověřil, že MV se podílelo na nastavení Výzvy č. 10. NÚKIB a MV se také podílejí na přípravě čerpání prostředků ESIF na KB v následujícím programovém období.

bylo dodržení souladu se standardy KB podle ZKB. Průběh podávání žádostí znázorňuje následující graf.

Graf č. 2: Vývoj podaných žádostí o podporu do Výzvy č. 10 od srpna 2016 do listopadu 2017



Zdroj: informační systém *MS2014+* (údaje k 24. 3. 2020).

NÚKIB a MV byly oprávněnými žadateli spravujícími prvky KII, VIS a další IS a KS. NÚKIB využil možnosti financování v rámci Výzvy č. 10, když podal dvě žádosti o podporu v celkové výši cca 112 mil. Kč, které byly následně schváleny MMR. Oba projekty realizované NÚKIB byly již finančně ukončeny ze strany MMR. MV podalo v rámci Výzvy č. 10 dvě žádosti o podporu s požadovanými prostředky na jejich realizaci ve výši cca 368 mil. Kč. Obě žádosti podalo MV v listopadu 2017, tedy až po rozšíření okruhu podporovaných aktivit v rámci Výzvy č. 10. Obě žádosti byly ze strany MMR vyřazeny z administrace z důvodu vysokého převisu žádostí o podporu nad alokací. MV tak nečerpalo v rámci Výzvy č. 10 žádné peněžní prostředky, a nevyužilo tak možnosti financovat zajištění KB z prostředků alokace. MV bylo přitom z pohledu spravovaných KII a VIS jednou z nejvýznamnější OSS. Souhrnně byly na projekty realizované subjekty státního sektoru v rámci Výzvy č. 10 ze strany řídicího orgánu schváleny prostředky ve výši cca 800 mil. Kč. Podrobnější údaje jsou uvedeny v následující tabulce.

Tabulka č. 2: Výzva č. 10 – projekty se schválenými prostředky na realizaci

Žadatelé	Podrobnější klasifikace žadatele	Počet projektů	Finanční objem schválených žádostí o podporu (EFRR)
Státní sektor	OSS	5	156,1 mil. Kč***
	státní příspěvkové organizace	7	589,5 mil. Kč*
	státní podniky	2	53,9 mil. Kč
Mezisoučet – státní sektor		**14**	**799,5 mil. Kč**
Samospráva	kraje	7	158 mil. Kč
	obce	6	66,6 mil Kč
	organizace zřizované nebo zakládané kraji/obcemi	27	344 mil. Kč**
Mezisoučet – samospráva		**40**	**568,6 mil. Kč**
Celkem státní sektor + samospráva		**54**	**1 368,1 mil. Kč**

Zdroj: informační systém *MS2014+* (údaje k 24. 3. 2020).

* Z toho 6 projektů zdravotnických zařízení v hodnotě 579,1 mil. Kč.

** Z toho 23 projektů zdravotnických zařízení v hodnotě 324,1 mil. Kč.

*** Z toho 121 mil. Kč představovaly projekty ústředních orgánů státní správy, z čehož 112 mil. Kč připadlo na projekty NÚKIB.

NKÚ považuje za účelné, že došlo k úpravě podporované aktivity, po které mohli oprávnění žadatelé čerpat prostředky z Výzvy č. 10 na zajištění KB nejen KII a VIS, ale i ISZS a dalších IS a KS, které nespadají pod KII, příp. VIS. Podmínkou bylo dodržení souladu se standardy KB podle ZKB. Velká část schválených projektů tak byla podána zdravotnickými zařízeními, která na základě platných kritérií ve vyhlášce č. 437/2017 Sb. nespadají mezi subjekty spravující KII, VIS nebo ISZS. Kritéria pro určení ISZS v odvětví zdravotnictví uvádí následující tabulka č. 3. Podle těchto kritérií je v ČR pouze šestnáct zdravotnických zařízení, na které se vztahují povinnosti vyplývající ze zákona č. 181/2014 Sb. (ve všech případech se jedná o zařízení spravující ISZS). Kybernetické útoky na zdravotnická zařízení z přelomu let 2019 a 2020 ukázaly, že ač se nejednalo o povinné subjekty podle ZKB, měla by série kybernetických útoků na tato zařízení významný dopad na funkčnost zdravotnického systému ČR.

Tabulka č. 3: Kritéria pro určení ISZS v odvětví zdravotnictví

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
5.1. Poskytování zdravotních služeb	Poskytovatel zdravotních služeb podle zákona o zdravotních službách	a) celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800 nebo b) statut centra vysoce specializované traumatologické péče podle zákona o zdravotních službách	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení druhu služby postihující více než 50 000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1 000 zraněných osob vyžadujících lékařské ošetření, V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo VI. kompromitaci citlivých osobních údajů o více než 200 000 osobách.

Zdroj: převzato z vyhlášky č. 437/2017 Sb.

NKÚ v kontrole také prověřoval následující tři projekty:

- *Ochrana vnějšího perimetru* (NÚKIB) – prověřována byla hospodárnost a účelnost vynaložených prostředků,
- *Systém detekce kybernetických bezpečnostních incidentů ve vybraných informačních systémech veřejné správy* (NÚKIB) – prověřována byla hospodárnost a účelnost vynaložených prostředků,
- DCeGOV (MV) – prověřována byla účelnost vynaložených prostředků a v rámci tohoto projektu byly dále prověřovány:
  - dohledové centrum MV pro provoz ICT systémů a kybernetickou bezpečnost (SOCCR),
  - vybudování první etapy dohledového centra NOC,
  - kontinuální rozvoj DCeGOV.

Hospodárnost vynaložených prostředků byla u vybraných projektů, realizovaných NÚKIB a financovaných ze SR a ESIF, posouzena v souvislosti s naplňováním úkolů stanovených AP NSKB. Kontrolou bylo ověřeno, zda NÚKIB postupoval při realizaci vybraných projektů v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek. Účelnost projektů byla u MV a NÚKIB posouzena ve vztahu plnění ke schváleným cílům projektů a cílům AP NSKB. Při kontrole výše uvedených projektů neshledal NKÚ nedostatky, které by měly závažný vliv na jejich hospodárnost a účelnost.

NKÚ v rámci kontrolní akce č. 19/26 provedl mezinárodní srovnání v oblasti KB. Více informací k tomu srovnání je uvedeno v příloze č. 1.

Seznam zkratek

AP NSKB	*Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*
CERT	Computer Emergency Response Team
ČR	Česká republika
DCeGOV	Dohledové centrum eGovernmentu
EFRR	*Evropský fond pro regionální rozvoj*
ESIF	evropské strukturální a investiční fondy
HW	hardware
ICT	informační a komunikační technologie
IROP	*Integrovaný regionální operační program*
IS	informační systémy
ISZS	*Informační systém základní služby*
KB	kybernetická bezpečnost
KII	kritická informační infrastruktura
KS	komunikační systémy
MMR	Ministerstvo pro místní rozvoj
MV	Ministerstvo vnitra
NBÚ	Národní bezpečnostní úřad
NKÚ	Nejvyšší kontrolní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OHA	Odbor hlavního architekta eGovernmentu
OIK	pracoviště kybernetické kriminality
OSS	organizační složky státu
PČR	Policie České republiky
SW	software
VIS	významné informační systémy
Výzva č. 10	výzva IROP č. 10 – *Kybernetická bezpečnost*
ZKB	zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Příloha č. 1

Mezinárodní srovnání

NKÚ oslovil nejvyšší kontrolní instituce ostatních zemí Evropské unie s cílem získat informace týkající se zajištění KB v jiných zemích a srovnat problematiku KB na systémové úrovni. Z odpovědí oslovených zemí mimo jiné vyplynulo, že:

- peněžní prostředky vynakládané na KB jsou na úrovni státního rozpočtu sledovány pouze ve Velké Británii,
- seznam VIS a KII je považován za citlivou informaci.

Souhrnné výsledky dotazníkového šetření uvádí následující tabulka. Z tabulky je patrné, že ČR má systém zajištění KB nastaven podobně jako ostatní srovnávané země. Ve všech sledovaných zemích existuje subjekt zodpovědný za oblast KB, ať již v podobě zvláštního státního orgánu či v podobě některého z ministerstev, pod které je problematika zařazena. Tento subjekt stanovuje kritéria pro určení klíčových informačních systémů, která jsou v případě většiny zemí součástí zákona. Posouzení, zda daný informační systém naplňuje kritéria klíčového systému, provádí buď správce daného informačního systému (tj. ministerstvo, instituce) nebo zvláštní orgán KB. Všechny sledované země za účelem dalšího rozvoje KB státních IS přijaly příslušnou strategii.

Výše v kontrolním závěru bylo popsáno, že NÚKIB, potažmo stát, neměl v průběhu kontrolovaného období informace o celkové výši peněžních prostředků vynakládaných jednotlivými kapitolami státního rozpočtu na KB. Většina srovnávaných zemí má nastaven systém zajištění KB a jejího rozvoje podobně jako ČR. Za zmínku stojí rozdílný přístup k vykazování peněžních prostředků na zajištění a rozvoj KB v případě Velké Británie. Ta vykazuje peněžní prostředky na zajištění a rozvoj KB státu na úrovni zvláštní položky rozpočtu. Díky tomu může Velká Británie lépe monitorovat výši prostředků, které jsou na KB vynakládány na úrovni celého státu.

Souhrn výsledků dotazníkového šetření

	Česká republika	Lotyšsko	Německo	Velká Británie	Kypr	Finsko
Existence kritérií pro určení klíčových IS	**ANO**	**ANO**	**ANO**	**NE**	**ANO**	**ANO**
Legislativní úprava kritérií	**Zákon** (o KB), **vyhláška**	**Zákon**	**Zákon** (o KB), **vyhláška**	**Jiný metodický materiál**	**Zákon** (obecná kritéria), **jiný metodický materiál** (detailní kritéria)	**Zákon, jiný metodický materiál**
Orgán odpovědný za kybernetickou bezpečnost	**Zvláštní orgán KB** (NÚKIB)	**Ministerstvo** (obrany, které zodpovídá za KB)	**Ministerstvo** (Spolkové ministerstvo vnitra, výstavby a domova)	**Ministerstvo** (Úřad vlády, Centrum pro ochranu národní infrastruktury)	**Zvláštní orgán KB** (Úřad digitální bezpečnosti)	**Ministerstvo** (financí, které zodpovídá za KB)
Orgán posuzující naplnění kritérií kritických IS	**Správce IS,** výsledky předává NÚKIB (ten dá významné IS a základní služby na příslušný seznam a u kritických IS dá požadavek na zařazení do seznamu kritické infrastruktury	**Správce IS**, u kritických IS správce nebo úřad bezpečnosti (návrh posoudí meziresortní komise pro národní bezpečnost a předloží ke schválení vládě)	**Správce IS** (pokud vyhodnotí jako kritický IS, kontaktuje Úřad pro informační bezpečnost)	Respondentovi není známo	**Zvláštní orgán KB** (Úřad digitální bezpečnosti)	**Zvláštní orgán KB** (Národní centrum pro KB)
Počet veřejných IS, z toho kritických	8 000 • 45 kritických, • 178 významných, • 30 poskytovatelů základních služeb	Celkový počet IS není znám, počet kritických je vyhrazená informace	Celkový počet IS nelze kvantifikovat, 1 500 kritických IS, 600 operátorů kritické infrastruktury	Informace není veřejně dostupná	Údaj o celkovém počtu IS neuveden, 50 kritických IS + další v polostátním sektoru (organizace vlastněné vládou)	4 000 IS ve veřejném sektoru
Financování zajištění kybernetické bezpečnosti	**Na úrovni správce IS** (není zvláštní rozpočtová položka, proto nelze kvantifikovat plánované náklady na KB)	**Na úrovni správce IS** (není zvláštní rozpočtová položka, proto nelze kvantifikovat plánované náklady na KB); **na úrovni zvláštního orgánu KB**	**Na úrovni správce IS** (**<u>většinou</u>** není zvláštní rozpočtová položka, proto **<u>většinou</u>** nelze kvantifikovat plánované náklady na KB)	**Na úrovni státního rozpočtu** (zvláštní rozpočtová položka)	**Na úrovni správce IS** (respondent neuvádí detaily, ale vzhledem k nemožnosti vyčíslit náklady v následující otázce lze předpokládat, že ani zde není zvláštní rozpočtová položka)	**Na úrovni správce IS** (není zvláštní rozpočtová položka, proto nelze kvantifikovat plánované náklady na KB)
Náklady na KB IS 2015–2020	**Není možné stanovit** (vzhledem ke způsobu plánování nákladů viz výše)	**Není možné** stanovit (vzhledem ke způsobu plánování nákladů viz výše)	**Není možné stanovit** (vzhledem ke způsobu plánování nákladů viz výše)	1,3 mld. GBP (2016–21)	**Není možné stanovit** (vzhledem ke způsobu plánování nákladů viz výše)	**Není možné stanovit** (vzhledem ke způsobu plánování nákladů viz výše). Řeší se. Možné zlepšení do budoucna
Strategie rozvoje kybernetické bezpečnosti	**ANO** (2015–20), vydal zvláštní orgán KB + akční plán	**ANO** (2019–22), připravilo MO odpovědné za KB, schválila vláda + akční plán	**ANO** (2016)	**ANO** (2016–21)	**ANO** (2012), vydal zvláštní orgán KB	**ANO** (2019), bude detailnější implementační plán

Zdroj: vypracoval NKÚ dle odpovědí kontrolních institucí.