Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 1647/2026-NÚKIB-E/210 Brno 3. února 2026

NUKIX005LJ9M

Věc: Odpověď na žádost podle ustanovení § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a Výzva k úhradě nákladů za poskytnutí informací podle ustanovení § 17 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Vážený pane [redacted]

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) obdržel dne 22. prosince 2025 Vaši žádost, č. j. 337/2026-NÚKIB-E/210 (dále jen „žádost“), podle zákona č. 106/1999., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“). Ve Vaší žádosti požadujete poskytnutí objemného množství oddělených a odlišných informací, které se týkají ekonomické a personální oblasti NÚKIB, činnosti NÚKIB a také spolupráce NÚKIB s jinými institucemi. Přípisem ze dne 6. ledna 2026 jste byl vyzván k upřesnění žádosti a informován o tom, že byla prodloužena lhůta pro poskytnutí požadovaných informací a o možnosti NÚKIB požadovat úhradu za mimořádně rozsáhlé vyhledání informací podle § 17 odst. 1 InfZ.

Vzhledem k nutnosti provedení mimořádně rozsáhlého vyhledávání dat je NÚKIB oprávněn na základě ustanovení § 17 odst. 1 InfZ podmínit poskytnutí Vámi požadovaných informací uhrazením nákladů za vyhledání, sběr a pořízení kopií těchto informací a nákladů spojených s jejich odesláním. Výše úhrady je stanovena na základě výpočtu podle sazebníku úhrad za poskytnutí informací, který tvoří přílohu Směrnice S11/2021 ředitele NÚKIB, kterou se stanoví jednotný postup při zajišťování práva svobodného přístupu k informacím v podmínkách NÚKIB (dále jen jako „Inf Směrnice“).

Ve Vaší žádosti požadujete poskytnutí mimořádně rozsáhlého množství informací, které je NÚKIB povinen vyhledat a shromáždit. Toto vyhledávání je časově náročné a vymyká se běžnému poskytování informací ze strany NÚKIB. Podle ustanovení § 17 odst. 1 InfZ, v souladu s přílohou č. 1 Inf Směrnice je NÚKIB oprávněn požadovat úhradu nákladů spojených s mimořádně rozsáhlým vyhledáváním informací – a to v celkové výši 150 Kč za každou započatou půlhodinu.

Ve Vaší žádosti požadujete poskytnutí následujících informací:

„Uveďte aktuální organizační strukturu NÚKIB k datu odpovědi na žádost, včetně popisu působnosti jednotlivých odborů a oddělení.“

„Jaký byl celkový rozpočet NÚKIB v letech 2019–2024, včetně jeho rozdělení na: mzdové náklady, provozní výdaje, investiční výdaje“

V tomto rozsahu NÚKIB poskytuje požadované informace, které jsou připojeny ve formě příloh.

[redacted]

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.cz, datová schránka: zzfnkp3, www.nukib.cz

[redacted]

S pozdravem

Elektronický podpis: 3.2.2026
Certifikát autora podpisu:
Jméno: Mgr. Vít Hrazdíra
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 19.11.2026 19:15 +01:00

Mgr. Vít Hrazdíra

vedoucí oddělení právního

Přílohy:

Příloha 1 – Organizační struktura

Příloha 2 – Rozpočet NÚKIB v letech 2019–2024

Obdrží:

[redacted] datovou schránkou

Vypraveno dne:

viz otisk razítka na poštovní obálce nebo časový údaj na obálce datové zprávy

Brno 3. února 2026

Příloha I – Organizační struktura

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Ředitel: Ing. Lukáš Kintr

Sekce personalistiky, práva a provozu

- Odbor právní

Zajišťuje kompletní právní servis pro provozní činnosti Úřadu a zabezpečuje plnění rozličných povinností vyplývajících z postavení Úřadu jakožto ústředního správního orgánu. Odbor právní je zároveň administrátorem výběrových a zadávacích řízení na veřejné zakázky, což zahrnuje mimo jiné i tvorbu a evidenci smluvní dokumentace. V neposlední řadě odbor právní zodpovídá za řízení o přestupcích v rozsahu působnosti svěřené Úřadu, resp. zastřešuje i další správní řízení vedená Úřadem.

  - Oddělení právní
  - Oddělení veřejných zakázek

- Odbor provozně ekonomický (OPE)
  - Oddělení investic

  Zadává a vede tvorbu investičních projektů a zajišťuje jejich realizaci. Předkládá návrhy na stavební činnost a opravy investičního charakteru majetku Úřadu a tyto navrhuje do rozpočtu příslušného roku. Připravuje a zajišťuje projektovou dokumentaci včetně projednání pro jednotlivé akce a to v rámci předprojektové, projektové a realizační činnosti. Podává jménem Úřadu žádosti o územní rozhodnutí a stavební povolení a ostatní nutná povolení související s realizací projektů. Připravuje a realizuje stavby a opravy majetku města investičního charakteru, které budou realizovány na základě stavebního povolení. Vykonává funkci investora na stavbách všeho druhu, které připravil a které realizuje. Zajišťuje všechny náležitosti spojené s uvedením staveb do provozu.

  - Oddělení rozpočtu

  Oddělení rozpočtu zajišťuje přípravu návrhu rozpočtu kapitoly rozpočtu 378-NÚKIB, příprava návrhu střednědobého výhledu a návrhu závěrečného účtu této kapitoly, včetně zpracování podkladů dodávaných od věcně příslušných organizačních celků a sledování jeho čerpání.

Dále je to podílení se na plnění úkolů funkce finančního manažera při financování projektů Úřadu, provádění rozpisu rozpočtu Úřadu na daný rozpočtový rok a v souladu se zákonem č. 320/2001 Sb., o finanční kontrole, v platném znění, plní funkci správce rozpočtu kapitoly 378-NÚKIB. Do náplně oddělení rozpočtu také náleží funkce zastupování Úřadu před Ministerstvem financí a odpovědnost za ekonomické výstupy Úřadu předávané ISSP a na Ministerstvo financí.

- Oddělení účetnictví

Oddělení účetnictví zajišťuje pro věcně příslušné organizační celky účtování správních poplatků a pokut v působnosti Úřadu, organizuje a metodicky usměrňuje inventarizaci majetku. V souladu se zákonem č. 320/2001 Sb., o finanční kontrole, plní funkci hlavní účetní kapitoly 378-NÚKIB. Dále zabezpečuje provádění účetní uzávěrky za daná účetní období, odpovědnost za účetní výstupy Úřadu, zajišťuje chod pokladny Úřadu, agendu tuzemských i zahraničních pracovních cest (ZPC) v rozsahu daném interními normativními akty, agendy související se ZPC a zajišťuje platební styk – bezhotovostní, hotovostní, zprostředkovává styk s bankami a agendu platebních karet ve spolupráci s ČNB.

- Oddělení provozu a služeb

Koordinuje a zabezpečuje materiálně technické zabezpečení Úřadu vyjma prostředků informační a komunikační techniky, vede evidenci movitého a nemovitého majetku Úřadu a provádí jeho inventarizaci. Dále koordinuje a zabezpečuje služby spojené se správou nemovitého majetku, podílí se na koordinaci provozu v objektech Úřadu, zajišťuje styk s vnějšími organizacemi ve správě budov (dodávky energií, vody, plynu, tepla atd.) a zajišťuje revizní zprávy na technologická zařízení. Dozoruje nad údržbou veškerého majetku. Zajišťuje provoz a servis služebních automobilů.

    - Pracovní skupina autoprovozu

- Oddělení personálních věcí a vzdělávání

Vykonává činnosti v oblasti personalistiky, vzdělávání, platové a sociální politiky v souladu se zákoníkem práce a prováděcích předpisů. Kontroluje dodržování pracovněprávních předpisů a zajišťuje evidenci zaměstnanců. Vede přijímací řízení s uchazeči o zaměstnání. Zabezpečuje stáže pro studenty vysokých škol. Podílí se na vytváření pracovně právních předpisů a interních aktů řízení.

- **Odbor bezpečnosti**
    - Oddělení spisové a archivní služby

Zajišťuje v rámci Úřadu činnosti podatelny a spisovny, registru utajovaných informací, specializovaného a bezpečnostního archivu. Dále v rámci Úřadu metodicky řídí spisovou službu, podílí se na vytváření interních aktů řízení a dalších dokumentů v oblasti spisové služby a ochrany

utajovaných informací, podílí se na provádění kontrol spisové služby a dodržování zásad ochrany utajovaných informací.

- Oddělení fyzické bezpečnosti

Zajišťuje v rámci Úřadu zabezpečení ochrany utajovaných informací z pohledu fyzické bezpečnosti v souladu s podmínkami stanovenými legislativními předpisy, zvláště pak zákona č. 412/2005 Sb., o ochraně ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a Vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Podílí se na tvorbě projektů fyzické bezpečnosti, vytváří bezpečnostní interní dokumenty a vyjadřuje se k bezpečnostní a projektové dokumentaci při rekonstrukčních a stavebních realizacích objektů Úřadu. Řídí a zabezpečuje činnosti při mimořádných bezpečnostních událostech. Spravuje systémy technické ochrany, přístupové a klíčové systémy. Řeší bezpečnostní incidenty a provádí kontrolní činnost v oblasti fyzické bezpečnosti. Spolupracuje s Ochrannou službou Policie České republiky při výkonu ochrany objektů Úřadu.

- Oddělení informační bezpečnosti

Vykonává bezpečnostní správu informačních a komunikačních systémů nakládajících s utajovanými informacemi Úřadu, vede jejich dokumentaci a evidenci dle příslušné legislativy. Zajišťuje plánování a rozvoj informačních a komunikačních systémů Úřadu nakládajících s utajovanými informacemi a ověřuje podmínky pro provoz a soulad s požadavky na jejich certifikaci. Spolupracuje s manažerem a architektem kybernetické bezpečnosti, kterým poskytuje součinnost v oblasti kybernetické bezpečnosti.

- Oddělení personální bezpečnosti a krizového řízení

Vykonává a zajišťuje připravenost Úřadu na řešení krizových situací ve spolupráci s ostatními organizačními celky Úřadu. Reaguje na aktuální krizové stavy a podílí se na tvorbě legislativy v oblasti krizového řízení v rámci Úřadu. Účastní se meziresortních jednání a iniciativ v oblasti krizového řízení a podílí se na jejich implementaci do praxe. Zajišťuje a provádí činnosti na úseku personální bezpečnosti v rozsahu stanoveném zákonem a interními akty.

- Architekt kybernetické bezpečnosti
- Manažer kybernetické bezpečnosti

Sekce strategických agend a spolupráce

- Odbor mezinárodní spolupráce a Evropské unie
  - Oddělení multilaterální spolupráce I a II

  Zajišťují v působnosti Úřadu agendy EU a NATO, agendu jiných mezinárodních organizacích jako OSN, OECD, OBSE nebo ITU, rozvojovou spolupráci a řešení otázek mezinárodního práva

veřejného. Připravují, koordinují a prosazují pozice ČR k návrhům právních úprav EU a při klíčových jednáních v EU. Dále koordinují úkoly Úřadu při sjednávání mezinárodních smluv a právně nezávazných dokumentů o spolupráci a v souvislosti s jejich prováděním.

- Oddělení bilaterální spolupráce

Udržuje a rozvíjí bilaterální spolupráci s partnery Úřadu a stanovuje priority pro tato jednání. Vede evidenci o jednáních se zahraničními partnery a vyhodnocuje je. Připravuje a koordinuje přípravu podkladů pro ředitele Úřadu a poskytuje mu podporu při jednáních. Ve spolupráci s ostatními organizačními celky se podílí na přípravách a organizaci mezinárodních akcí.

- Odbor cvičení a vzdělávání

  - Oddělení cvičení

  Zabývá se koordinací a přípravou širokého spektra technických a netechnických cvičení kybernetické bezpečnosti na národní i mezinárodní úrovni (např. Cyber Czech, Cyber Coalition, Locked Shields, CMX). Velkou část agendy tvoří příprava cvičení kybernetické bezpečnosti, která jsou zaměřená na regulované subjekty a partnerské instituce, včetně cvičení zaměřených na celé sektory a odvětví. Stejně tak se oddělení podílí na dalších aktivitách jako například přednáškové činnosti či konzultacích cvičení pro výše zmíněné subjekty.

  - Oddělení vzdělávání

  Zajišťuje vzdělávací a osvětové aktivity, pořádá konference a školení na téma kybernetické bezpečnosti, připravuje a provozuje tematické e-learningové kurzy. Primární cílovou skupinou vzdělávání jsou zaměstnanci veřejné správy a další osoby, které zastávají role podle Zákona o kybernetické bezpečnosti. Sekundární cílovou skupinu tvoří osoby identifikované jako „zranitelné v kyberprostoru“. Jsou jimi žáci a studenti všech stupňů vzdělávání a senioři. Oddělení ve velké míře spolupracuje s dalšími rezorty a klíčovými hráči v oblasti vzdělávání, kdy je podporuje při šíření osvěty v oblasti kybernetické bezpečnosti a podílí se na společných aktivitách. Oddělení rovněž plní roli autorizačního orgánu pro povolání v oblasti kybernetické bezpečnosti (v souladu se zákonem č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů).

- Odbor centrální analytiky

  - Oddělení strategických analýz

  Provádí analýzu a monitoring kybernetických hrozeb, rizik a aktuálních trendů v kybernetické bezpečnosti. Posuzuje jejich politický a bezpečnostní kontext či dopady incidentů. V návaznosti na to poskytuje analytickou podporu v rámci NÚKIB, rozhodujícím činitelům v české státní správě a zahraničním partnerům. Ve spolupráci s CERT rozvíjí pokročilou analytickou kapacitu v podobě Cyber Threat Intelligence (CTI).

- Oddělení informačního šetření

Na základě zpravodajství z otevřených zdrojů (OSINT) poskytuje analytickou podporu příslušným organizačním celkům. Dále též poskytuje analytickou podporu externím partnerům v rámci úzce vymezených agend.

- Pracovní skupina správy a analýzy dat

Poskytuje dalším organizačním celkům podporu v podobě datové analýzy nebo vývoje, správy a poskytování datových a analytických nástrojů.

- Oddělení národních strategií a politik

Zabývá se přípravou dlouhodobé strategie a poskytuje analýzu, a potřebnou expertízu, včetně věcných i právních doporučení k zajištění, aby NÚKIB, potažmo ČR plnila všechny stanovené cíle v oblasti zajišťování kybernetické bezpečnosti, a to co nejefektivnějším způsobem. Podílí se na tvorbě kybernetických bezpečnostních politik a zajišťuje jejich efektivní koordinaci a harmonizaci napříč veřejnou sférou a dalšími subjekty. Mimo jiné usiluje o budování koherentní národní komunity kybernetické bezpečnosti v ČR a intenzivně spolupracuje s partnery ze státní i soukromé sféry na národní i mezinárodní úrovni.

- Oddělení vědy, výzkumu a inovací

Zabývá se koordinací výzkumných a inovačních aktivit v oblasti kybernetické a informační bezpečnosti. Vytváří Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti a ve spolupráci s partnery realizuje kroky k jeho naplňování. Provozuje Národní koordinační centrum dle Nařízení Evropského parlamentu a Rady 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. Zapojuje se do řešení výzkumných projektů a podněcuje účast výzkumné komunity na přeshraničních projektech.

Sekce informačních systémů

- Odbor bezpečnosti informačních a komunikačních technologií

  - Oddělení vývoje kryptografických prostředků

Provádí a zabezpečuje základní a aplikovaný výzkum a vývoj v oblasti kryptografie, kryptoanalýzy a kryptografických prostředků, vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany. Dále zabezpečuje vývoj kryptografických schémat pro použití v kryptografických prostředcích ochrany utajovaných informací (UI), provádí analýzy a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně UI a podílí se na zajišťování veřejných zakázek Úřadu v oblasti výzkumu, vývoje a výroby kryptografických prostředků.

- Oddělení certifikací informačních a komunikačních systémů

Plní úkoly Národního střediska pro bezpečnost informačních systémů, provádí certifikaci informačních systémů používaných k nakládání s utajovanými informacemi (UI), schvaluje projekty bezpečnosti komunikačních systémů používaných k nakládání s UI, zajišťuje plnění úlohy Úřadu jako orgánu pro bezpečnostní akreditaci informačních systémů nakládajících s UI pro NATO a EU a jiné mezinárodní organizace, provádí hodnocení informačních systémů nakládajících s UI NATO a EU a jiných mezinárodních organizací, provádí styk s orgány NATO a EU a jiných mezinárodních organizací pro zajištění akreditace informačních systémů a průběžnou kontrolní činnost v akreditovaných systémech podle požadavků NATO a EU a jiných mezinárodních organizací.

- Oddělení certifikací kryptografických prostředků a pracovišť

Zabezpečuje a provádí certifikaci kryptografických prostředků (KP) a stanovuje bezpečnostní standardy v oblasti certifikace KP, provádí certifikaci kryptografických pracovišť (KPr) a stanovuje bezpečnostní standardy v oblasti certifikace KPr. Ověřuje a schvaluje implementaci a zasazení kryptografických prostředků. Schvaluje způsobilost materiálu k zajištění funkce KP, schvaluje projekty zástavby KP do mobilních a dočasně rozmístitelných systémů. Provádí styk s orgány NATO, EU a jiných mezinárodních organizací pro zajištění mezinárodní certifikace (schválení) KP těmito organizacemi. Podílí se na výkonu kontroly ve vybraných oblastech ochrany utajovaných informací v rámci České republiky. Podílí se, případně vykonává inspekce NATO a EU v oblasti kryptografické ochrany utajovaných informací. Podílí se na ověřování a schvalování způsobilosti kryptografických pracovišť pro manipulaci s kryptografickým materiálem EU. Zabezpečuje a provádí ověřování odborné způsobilosti pracovníků kryptografické ochrany (zkoušky zvláštní odborné způsobilosti). Provádí metodickou a poradní činnost v oblasti kryptografické ochrany utajovaných informací.

- Oddělení TEMPEST

Plní úkoly Národního střediska pro měření kompromitujícího elektromagnetického vyzařování, provádí analýzy a hodnocení elektrických a elektronických zařízení z hlediska úniku utajovaných informací (UI) prostřednictvím elektromagnetického vyzařování, provádí zónové hodnocení prostorů určených pro zpracování UI, certifikaci stínících komor určených k ochraně UI, analýzy a hodnocení kryptografických prostředků z hlediska ochrany proti kompromitujícímu vyzařování, kontrolu, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací.

- Oddělení kryptografických analýz
- Oddělení odborné podpory
- Oddělení Národní distribuční středisko

Zajišťuje a plní úkoly Národního střediska pro distribuci kryptografického materiálu (NDA), zabezpečuje a provádí ověřování odborné způsobilosti pracovníků kryptografické ochrany (zkoušky zvláštní odborné způsobilosti) a vydává osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany, zajišťuje a provádí výrobu klíčových materiálů pro provoz kryptografických prostředků distribuci klíčových materiálů a kryptografických prostředků, zajišťuje servis a údržbu speciálních zařízení pro výrobu klíčových materiálů a kryptografických prostředků.

        - Pracovní skupina CDA

- Odbor informačních technologií

    - Oddělení síťové infrastruktury a dohledu

    Zabývá se systémovou podporou aplikací ERP, Personalistiky, mezd a Spisové služby. Zabezpečuje instalaci systémů, uživatelskou podporu, správu, optimalizaci a údržbu databází pro výše uvedené systémy. Řeší strategické a rozvojové záměry v oblasti informačních systémů (JIS, nové lokality, GDPR, atd.). Provozuje Registrační certifikační autoritu pro x509 zaměstnanecké certifikáty. Vydává serverové x509 certifikáty (CESNET) a certifikáty pro FW (sondy). Realizuje a aktualizuje DRP plán klíčových aplikací.

        - Pracovní skupina provozního dohledu

    - Oddělení serverové infrastruktury

    Zabývá se instalací, přípravou, správou a optimalizací serverové infrastruktury. Dále se zabývá správou virtualizačního prostředí, poštovních služeb, datových úložišť a též správou fyzického serverového vybavení, udržuje též v provozu interně vyvinuté nástroje pro zabezpečenou komunikaci. Udržuje veškeré možné komunikační cesty úřadu.

    - Oddělení podpory aplikací a rozvoje

    - Oddělení klientské podpory

    Zabývá se podporou uživatelů v oblasti IT. Řeší problémy s hardwarem i softwarem koncových stanic a příslušenství uživatelů. Zabezpečuje nákup potřebného IT vybavení. Předává podklady pro evidenci majetku.

        - Pracovní skupina speciálních prostředků

    - Oddělení plánování, ekonomiky a logistiky v IT

- Oddělení bezpečnosti satelitních služeb

Zodpovídá za implementaci a provoz veřejně regulované služby (PRS) systému Galileo v ČR a koordinuje veškeré aktivity spojené s přístupem k informacím a technologiím PRS. V souladu s platnou evropskou legislativou (1104/2011/EU) plní funkci Příslušného orgánu PRS (Competent

PRS Authority), přičemž zejména zodpovídá za organizaci přístupu a přidělení přístupových práv oprávněným uživatelům, ochranu a distribuci utajovaných informací PRS, zpracování provozních a bezpečnostních předpisů pro využití PRS a vyhodnocení potenciálních rizik pro PRS, včetně definování příslušných nápravných a preventivních opatření. Je kontaktním místem pro trvalé spojení s bezpečnostním střediskem PRS, kterému oznamuje všechny bezpečnostní incidenty narušující bezpečnost PRS a rušivé elektromagnetické interference na frekvencích vyhrazených pro PRS.

Sekce Národního centra kybernetické bezpečnosti (NCKB)

- Odbor vládní CERT (GovCERT)
  - Oddělení reaktivní

Hlavním úkolem reaktivního oddělení je prvotní koordinace, zpracování a řešení kybernetických bezpečnostních incidentů a vedení komunikačních kanálů s ostatními subjekty.

  - Oddělení analýzy síťového provozu

Zabývá se kybernetickou bezpečností z pohledu síťového provozu. Hlavním posláním oddělení je (forenzní) zkoumání útoků, hledání škodlivé aktivity v síťových záznamech a úzká kooperace s incident handlingem při řešení aktivních incidentů. Provozuje i vlastní detekční systémy, kde proaktivně vyhledává útočníky a předchází tím větším škodám.

  - Oddělení analytické

Zabývá se zkoumáním dat. Provádí forenzní zkoumání počítačů a mobilních zařízení a také analýzu artefaktů vzniklých v souvislosti s bezpečnostními incidenty. Také se věnuje analýze malware a reverznímu inženýrství.

  - Oddělení penetračního testování

Specializuje se na identifikaci a zlepšení bezpečnostních aspektů pomocí technik penetračního testování. Hlavním cílem je zajištění odolnosti vůči potenciálním kybernetickým hrozbám a bezpečnostním rizikům. K dosažení těchto cílů odborníci z Oddělení penetračního testování provádí praktické prověření zabezpečení pomocí simulovaných kybernetických útoků). V současné době jsou nabízeny služby externích a interních penetračních testů, wifi sítí, phishingové a vishingové kampaně, fyzické testy, testy zahlcení (dos), a po domluvě také nestandardní testy specifických zařízení nebo konzultace k nasazení nových technologií.

    - Pracovní skupina testování síťových služeb

Zaměřuje se na interní penetrační testy a testování služeb vyskytujících se v síťových infrastrukturách. Hlavním cílem je identifikace možných slabiny, které by mohly být využity útočníky po získání přístupu do vnitřních sítí organizací.

- Oddělení bezpečnosti operačních technologií

Zabývá se problematikou kybernetické bezpečnosti průmyslově orientovaných technologií a řídících systémů, které jsou součástí nejen určené Kritické infrastruktury ČR. Podílí se na procesu regulace a kontroly subjektů provozujících operační technologie. V souvisejících oblastech jsou otevřeni k technickým konzultacím.

- Oddělení SecOps

Hlavní agendou oddělení SecOps (Security Operations) je vývoj, nasazení a zabezpečení aplikací, přičemž je kladen důraz na použití nejmodernějších technologií. Tyto činnosti jsou vykonávány jak pro vnitřní potřebu odboru Vládní CERT, tak i pro potřeby spolupráce s externími subjekty. Odborníci oddělení SecOps také ve velké míře zajišťují technickou část kontrol povinných subjektů dle Zákona o kybernetické bezpečnosti. Dále aktivně participují na tvorbě nových metodik a standardů a posuzování bezpečnosti cloudových služeb a poskytovatelů.

- Odbor regulace

Zabývá se problematikou upravenou zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a zároveň oblastí EU certifikací kybernetické bezpečnosti obsažené v nařízení (EU) č. 2019/881, aktu o kybernetické bezpečnosti. Na každodenní bázi komunikuje s regulovanými subjekty, ať už ve věci regulace, EU certifikací nebo poskytování metodické podpory. Podílí se na přípravě legislativy v oblasti kybernetické bezpečnosti, včetně návrhu certifikačních schémat. Hraje klíčovou roli při určování a ochraně kritické informační infrastruktury, významných informačních systémů a systémů základních služeb v rámci České republiky. V oblasti EU certifikací kybernetické bezpečnosti (dále jen EU certifikace KB) pak v souladu s aktem o kybernetické bezpečnosti plní úlohu vnitrostátního orgánu certifikace kybernetické bezpečnosti.

- Oddělení regulace soukromého sektoru

Zajišťuje určování provozovatelů základních služeb. Aplikuje, udržuje a vykládá vyhlášku č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. Zajišťuje určování kritické informační infrastruktury v soukromém sektoru. Poskytuje výklad a podporu v oblasti regulace soukromého sektoru. Komunikuje s příslušnými regulátory.

- Oddělení regulace veřejného sektoru

Zajišťuje identifikaci významných informačních systémů. Aplikuje, udržuje a vykládá vyhlášku č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Zajišťuje určování kritické informační infrastruktury ve veřejném sektoru. Poskytuje výklad a podporu v oblasti regulace veřejného sektoru. Komunikuje s příslušnými regulátory.

- Oddělení regulace dodavatelů informačních technologií

Zajišťuje posuzování nabídek cloud computingu podle zákona o informačních systémech veřejné správy a zákona o kybernetické bezpečnosti. Aplikuje, udržuje a vykládá tzv. cloudové vyhlášky. Konzultuje posuzování dopadů narušení systémů pro účely procesů cloud computingu u orgánů veřejné moci. Poskytuje výklad a podporu v oblasti regulace využívání cloud computingových služeb orgány veřejné moci. Komunikuje s příslušnými regulátory.

    - Pracovní skupina bezpečnosti dodavatelského řetězce

  - Pracovní skupina Evropských certifikací

V roli vnitrostátního orgánu certifikace kybernetické bezpečnosti dohlíží na dodržování pravidel zahrnutých v evropských schématech certifikace KB a tato pravidla vymáhá. Má za úkol v příslušných případech autorizovat subjekty posuzování shody a delegovat vydávání EU certifikátů KB. Řeší stížnosti související s EU certifikáty KB. Zastupuje ČR v rámci Evropské skupiny pro certifikaci KB. Poskytuje výklad a podporu v oblasti EU certifikací KB. Komunikuje s příslušnými stakeholdery.

- Odbor kontroly

Provádí kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných subjektů. Současně s odborem regulace se podílí na přípravě legislativy v oblasti kybernetické bezpečnosti a poskytuje metodickou podporu regulovaným subjektům. Dále na kontrolní činnosti spolupracuje s dalšími kontrolními orgány, jejichž kontrolní činnost má přesah do oblasti kybernetické bezpečnosti.

  - Oddělení kontroly 1
  - Oddělení kontroly 2
  - Oddělení kontroly 3

- **Odbor Kabinet ředitele (OKŘ)**
  - Oddělení komunikace
  - Oddělení vládní agendy a legislativy

Koordinuje a realizuje pravomoci Úřadu v legislativním procesu a poskytuje výkladová stanoviska k právním předpisům v působnosti Úřadu. Zastřešuje přípravu nelegislativních materiálů předkládaných vládě, Bezpečnostní radě státu, Výboru pro kybernetickou bezpečnost nebo jiným orgánům státu, popřípadě tyto materiály zpracovává samostatně. Dále zajišťuje vládní agendu a strategickou komunikaci s ministerstvy a ostatními ústředními orgány státní správy.

  - Oddělení plánování a řízení
  - Oddělení Projektová kancelář

Zajišťuje efektivní řízení širokého portfolia projektů NÚKIB v průběhu celého životního cyklu. Naplňuje tyto funkce: podílí se přímo na realizaci a řízení projektů, popř. projektům asistuje metodicky. Vydává závazné pokyny i metodické materiály pro organizaci, pomáhá ověřovat kvalitu řízení projektů. Zajišťuje a podporuje vzdělávání v oblasti projektového řízení. Podílí se na tvorbě politiky ČR v oblasti spolufinancování kybernetické bezpečnosti z EU-fondů. Asistuje také ve využití příležitostí čerpání prostředků z EU – vlastní organizaci i za její hranice.

- **Oddělení strategické komunikace a rozvoje**
- Bezpečnostní ředitel
- Auditor kybernetické bezpečnosti
- Interní auditor
- Pověřenec pro ochranu osobních údajů
- **Rozkladová komise ředitele NÚKIB**
  - JUDr. Barbora Schrötterová (*Předsedkyně RK, zaměstnankyně NÚKIB)*
  - prof. JUDr. Radim Polčák, Ph.D. (*Externista)*
  - JUDr. Ing. Jiří Nováček (*Externista)*
  - JUDr. Bc. Petr Kadlec (*Externista)*
  - RNDr. Radim Ošťádal, Ph.D. (*Externista)*
  - Mgr. Iveta Pospíšilíková (*Externistka)*
  - Mgr. Marcela Káňová, Ph.D. (*Externistka)*
  - Ing. Martin Konečný (*Externista)*
  - Mgr. Pavel Štěpáník, LL.M. (*Zaměstnanec NÚKIB)*

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 3. února 2026

Příloha II – Rozpočet NÚKIB v letech 2019–2024

Rozpočet NÚKIB v letech 2019-2024

Kapitola 378 - NÚKIB

(v tis Kč)

	2019		2020		2021		2022		2023		2024	
	Schválený rozpočet	**Konečný rozpočet**	**Schválený rozpočet**	**Konečný rozpočet**	**Schválený rozpočet**	**Konečný rozpočet**	**Schválený rozpočet**	**Konečný rozpočet**	**Schválený rozpočet**	**Konečný rozpočet**	**Schválený rozpočet**	**Konečný rozpočet**
Výdaje celkem	**352 460,73**	**538 446,70**	**425 317,71**	**572 300,13**	**427 932,11**	**634 679,54**	**529 141,43**	**645 103,15**	**616 610,01**	**683 273,49**	**610 947,41**	**820 999,11**
Běžné výdaje	275 759,27	348 957,80	327 566,24	397 826,17	364 180,84	426 490,97	399 738,54	470 392,20	498 073,91	541 553,41	520 207,17	551 081,06
:z toho Platy vč. příslušenství	*138 407,48*	*168 591,52*	*189 491,87*	*195 698,00*	*231 106,28*	*230 503,87*	*261 133,81*	*268 824,82*	*316 431,90*	*315 842,76*	*322 794,78*	*325 420,78*
:z toho běžné výdaje bez platů a příslušenství	*137 351,78*	*180 366,27*	*138 074,37*	*202 128,18*	*133 074,57*	*195 987,10*	*138 604,74*	*201 567,38*	*181 642,00*	*225 710,66*	*197 412,39*	*225 660,28*
Kapitálové výdaje	76 701,47	189 488,91	97 751,47	174 473,96	63 751,27	208 188,56	129 402,89	174 710,95	118 536,11	141 720,08	90 740,24	269 918,05

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.cz, datová schránka: zzfnkp3, www.nukib.cz