Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
210-1414/2026-E
Číslo jednací:
14643/2026-NÚKIB-E/210

Brno, 20. dubna 2026

Veřejná vyhláška

Vyhlášení řízení o výběru žádosti o uzavření veřejnoprávní smlouvy s provozovatelem Národního CERT

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) jako věcně příslušný správní orgán podle ustanovení § 53 odst. 1 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve spojení s § 163 odst. 4 zákona č. 500/2004 Sb., správní řád (dále jen „správní řád“)

oznamuje

podle ustanovení § 146 odst. 2 správního řádu **vyhlášení řízení o výběru žádosti o uzavření veřejnoprávní smlouvy s provozovatelem Národního CERT.**

Účel a právní rámec

Úřad v souladu s ustanovením § 146 odst. 2 správního řádu vyhlašuje řízení formou výběru žádosti o uzavření veřejnoprávní smlouvy dle § 53 odst. 1 zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“). Cílem tohoto řízení je vybrat uchazeče pro provozování Národního CERT, jehož žádost nejlépe odpovídá stanoveným požadavkům. Vybraný uchazeč následně uzavře s Úřadem veřejnoprávní smlouvu o výkonu činnosti Národního CERT podle § 53 odst. 1 zákona o kybernetické bezpečnosti.

Toto vyhlášení určuje zákonem stanovenou minimální lhůtu pro podávání žádostí (30 dnů) a kritéria hodnocení podaných žádostí. Řízení bude vedeno jako společné řízení o všech podaných žádostech podle § 146 odst. 1 správního řádu.

Vymezení činností Národního CERT

Podle § 43 odst. 1 zákona o kybernetické bezpečnosti vykonává Národní CERT tyto činnosti:

a) zajišťuje v rozsahu zákona o kybernetické bezpečnosti sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti a působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu nižších povinností dle zákona o kybernetické bezpečnosti,

b) přijímá hlášení o kybernetických bezpečnostních incidentech, kybernetických bezpečnostních událostech, hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti a tyto údaje zaznamenává, vyhodnocuje, uchovává a chrání,

c) poskytuje poskytovatelům regulovaných služeb v režimu nižších povinností zákona o kybernetické bezpečnosti metodickou podporu, pomoc a součinnost při výskytu a zvládání kybernetického bezpečnostního incidentu s významným dopadem a při zveřejňování informací o zranitelnostech v oblasti kybernetické bezpečnosti,

d) provádí vyhledávání a hodnocení zranitelností v oblasti kybernetické bezpečnosti,

e) předává Úřadu údaje o nahlášených hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech podle § 15 zákona o kybernetické bezpečnosti a zranitelnostech v oblasti kybernetické bezpečnosti,

f) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování regulované služby v tomto jiném členském státu a zároveň o tom informuje Úřad, přičemž dbá na bezpečnost a jiné oprávněné zájmy ohlašovatele,

g) přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti,

h) plní roli CSIRT týmu a podílí se na fungování mezinárodních uskupení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,

i) se v případě potřeby podílí na procesu vzájemného hodnocení a

j) upřednostňuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných zdrojích.

Provozovatel Národního CERT vykonává činnosti podle písm. a), b) a e) až h) bezúplatně a je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v odstavci 1 nezbytné náklady.

Výše popsané činnosti Národního CERT vykonává provozovatel Národního CERT, který přitom postupuje nestranně.

Podmínky účasti (požadavky na uchazeče) a kritéria hodnocení

Provozovatelem Národního CERT se může stát pouze právnická osoba, která splňuje **podmínky** uvedené v § 43 odst. 4 zákona o kybernetické bezpečnosti.

K posouzení a výběru nejvhodnější žádosti stanovuje Úřad následující **kritéria hodnocení** (níže uvedené oblasti budou posuzovány prioritně):

- **Technické zajištění provozu:** Úroveň a kvalita technického zabezpečení navrhovaného provozu Národního CERT. Posuzuje se infrastruktura, vybavení a schopnost zajistit nepřetržitý dohled, sběr a vyhodnocování kybernetických hrozeb a incidentů.

- **Nástroje pro analýzu hrozeb a malwaru:** Schopnost uchazeče využívat pokročilé nástroje a technologie pro analýzu kybernetických hrozeb, malwaru a zranitelností. Hodnotí se existence vlastních či sdílených analytických platforem, sandboxů, systémů pro indikátory kompromitace apod.

- **Technologie bezpečné komunikace:** Úroveň implementace a používání technologií pro bezpečnou komunikaci při řešení incidentů. Například schopnost bezpečně sdílet citlivé informace s ohlašovateli incidentů a s partnery (šifrované komunikační kanály, zabezpečené úložiště dat apod.).

- **Dlouhodobé působení a zapojení v komunitě:** Délka a kvalita dosavadního působení uchazeče v oblasti kybernetické bezpečnosti na národní i mezinárodní úrovni. Zohledňuje se účast v mezinárodních platformách či organizacích (např. FIRST, TF-CSIRT), úroveň spolupráce s jinými CSIRT týmy a reputace uchazeče v komunitě.

- **Zkušenost s řešením incidentů:** Praktické zkušenosti uchazeče s řešením incidentů, včetně pravidelných účastí na kybernetických cvičeních.

- **Implementované procesy pro řešení incidentů:** Připravenost uchazeče efektivně řešit hlášené kybernetické bezpečnostní incidenty. Posuzuje se existence a úroveň interních procesů, metodik či schémat pro příjem, kategorizaci, řešení a vyhodnocování kybernetických bezpečnostních incidentů a událostí. Důraz je kladen na zavedené postupy pro komunikaci s postiženými subjekty a následná preventivní opatření.

- **Osvětová a publikační činnost:** Míra angažovanosti uchazeče ve zvyšování povědomí o kybernetické bezpečnosti. Hodnotí se dosavadní osvětové aktivity (např. školení, workshopy, veřejná upozornění na hrozby) a publikační činnost (odborné články, analýzy, reporty o incidentech či hrozbách), kterými uchazeč přispívá k celkové bezpečnostní komunitě.

- **Zkušenosti s provozem týmu CERT/CSIRT:** Relevantní zkušenosti uchazeče s provozem bezpečnostního týmu typu CERT/CSIRT. Přednostně bude hodnoceno, zda uchazeč již provozuje či provozoval tým řešící kybernetické incidenty (např. sektorový CERT, akademický CSIRT apod.), včetně dosažených výsledků a referencí.

Každá podaná žádost bude posouzena hodnotící komisí jmenovanou ředitelem Úřadu v souladu s § 146 odst. 6 správního řádu. Komise provede hodnocení podle výše uvedených kritérií a doporučí Úřadu nejvhodnějšího uchazeče k uzavření smlouvy.

Podání žádosti a požadované dokumenty

Způsob podání

Žádost o účast v řízení a o výběru žádosti na uzavření veřejnoprávní smlouvy musí být podána písemně. Uchazeči mohou žádost zaslat na adresu NÚKIB elektronicky prostřednictvím datové schránky nebo e-mailem s využitím elektronického podpisu, poštou nebo ji doručit osobně.

Náležitosti žádosti

Každá žádost musí obsahovat alespoň:

- identifikační údaje uchazeče,
- doklady prokazující splnění podmínek účasti,
- popis zajištění činností Národního CERT: dokument popisující, jak uchazeč hodlá zabezpečit výkon požadovaných činností Národního CERT podle § 43 odst. 1 zákona o kybernetické bezpečnosti. Měl by zahrnovat například organizační zajištění týmu, technické vybavení, způsob

kooperace s Úřadem a zapojení do mezinárodních struktur, návrh procesů pro přijímání a řešení kybernetických bezpečnostních incidentů atd.

- reference a přílohy k hodnotícím kritériím: důkazy podporující splnění hodnoticích kritérií; např. ukázky publikačních výstupů, potvrzení o členství v nadnárodních organizacích, případové studie řešených incidentů apod.

Lhůta pro podání žádostí

Lhůta pro podávání žádostí činí **30 dnů a počíná běžet patnáctým dnem po zveřejnění tohoto vyhlášení** na úřední desce NÚKIB. V souladu s § 146 odst. 2 správního řádu nelze zmeškání úkonu prominout.

Řízení je zahájeno patnáctým dnem po vyvěšení tohoto vyhlášení na úřední desce Úřadu, za předpokladu současného zveřejnění informací alespoň ve dvou celostátních hromadných sdělovacích prostředcích, v souladu s § 146 odst. 2 správního řádu.

Další informace

Oznámení výsledků

Po vyhodnocení všech žádostí bude výsledné rozhodnutí o výběru provozovatele Národního CERT oznámeno formou rozhodnutí vydaného Úřadem. Následně Úřad uzavře s vybraným uchazečem veřejnoprávní smlouvu podle § 53 odst. 1 zákona o kybernetické bezpečnosti, upravující konkrétní podmínky provozování Národního CERT. Konkrétní podoba smlouvy bude s vybraným uchazečem projednána. Vybraný uchazeč má právo veřejnoprávní smlouvu s Úřadem neuzavřít.

Vyvěšeno dne:

Sejmuto dne:

Elektronický podpis: 20.4.2026
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
Národní úřad pro kybernetickou
a informační bezpečnost