Příloha č. 6 zadávací dokumentace

Zadavatel:

Nemocnice Strakonice, a.s.
Radomyšlská 336, Strakonice 1, 386 01 Strakonice
IČO: 26095181

k podlimitní veřejné zakázce s názvem:

FULL SERVICE – RTG zařízení; po dobu 3 let

zadávané v podlimitním řízení dle ust. § 26 a § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“)

Bezpečnostní požadavky a kybernetická bezpečnost

1. Status zadavatele a právní rámec

Zadavatel konstatuje, že je poskytovatelem regulované služby podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**ZKB“**). Z tohoto titulu je zadavatel povinen při výběru dodávek a služeb a smluvních partnerů, resp. při výběru nejvhodnějšího uchazeče dodržovat povinnosti poskytovatele regulované služby stanovené příslušnými právními předpisy a dále zohledňovat veškerá aktuální bezpečnostní opatření, informace, upozornění a varování publikovaná Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) ve smyslu § 12 a násl. ZKB.

2. Průběžné vyhodnocování rizik

Poskytovatel bere na vědomí, že zadavatel musí reflektovat veškerá varování NÚKIB vydaná před zahájením, v průběhu i po skončení výběrového řízení. Jakýkoliv seznam rizik či varování přiložený k dokumentaci je pouze demonstrativní a slouží k základní orientaci. Rozhodující je vždy aktuální stav hrozeb v čase plnění.

3. Povinná součinnost

V souladu s příslušnými právními předpisy a metodikami NÚKIB provede zadavatel u předložené nabídky individuální analýzu rizik. Poskytovatel se zavazuje k plné součinnosti nezbytné pro toto posouzení, a to zejména formou dodání:

- kompletní technické specifikace nabízeného zboží nebo služeb, jejich prvků a komponentů,
- údajů o struktuře subdodavatelského řetězce,
- přehledu implementovaných bezpečnostních mechanismů, certifikátů a postupů pro řešení kybernetických incidentů.

4. Důsledky neposkytnutí součinnosti

Odmítnutí součinnosti nebo neschopnost doložit údaje vyžadované analýzou rizik může vést k vyřazení nabídky pro nesplnění podmínek zadávací dokumentace.

5. Transparentnost a nediskriminace

Zadavatel prohlašuje, že definované bezpečnostní standardy jsou formulovány neutrálně. Nejsou namířeny proti konkrétním dodavatelům, značkám nebo státům, nýbrž striktně sledují naplnění zákonných povinností zadavatele pro zajištění kybernetické a informační bezpečnosti. Veškeré požadavky jsou aplikovány jednotně v souladu se zásadami ZZVZ.

6. Bezpečnostní pravidla

Příloha č. 6 zadávací dokumentace

Poskytovatel podáním nabídky potvrzuje, že se seznámil s aktuálními BEZPEČNOSTNÍMI PRAVIDLY

1. PRO DODAVATELE, která je dostupná v záložce ,,Pro významné dodavatele‘‘ zde: https://www.nemst.cz/document/dokumentace/BP_vyznamni_dodavatele.pdf

Seznam varování Národního úřadu pro kybernetickou a informační bezpečnost

23.04.2025	Upozorňujeme na metodu „harvest now, decrypt later“
14.04.2025	Upozornění na možnou zvýšenou aktivitu kyberútočníků v souvislosti s EXPO 2025
24.10.2024	Upozorňujeme na zneužívání identit Amazon, Microsoft a státních institucí
07.06.2024	Upozornění na zvýšené riziko DDoS útoků během voleb do Evropského parlamentu
16.02.2024	Upozornění na kompromitaci routerů Ubiquity Edge OS aktérem sponzorovaným ruským státem
09.02.2024	Upozorňujeme na dvě kritické zranitelnosti v operačním systému FortiOS
05.01.2024	Upozorňujeme na hrozbu Terrapin útoku mířícího na SSH protokol
30.11.2023	NÚKIB upozorňuje na hrozbu spojenou s aplikací WeChat společnosti Tencent
24.10.2023	Upozorňujeme na zranitelnost CVE-2023-20273 v Cisco IOS XE (CVSS 7.2)
18.10.2023	Upozorňujeme na kritickou zranitelnost CVE-2023-20198 v Cisco IOS XE (CVSS 10.0)
29.09.2023	Upozorňujeme na kritické zranitelnosti v knihovnách webových prohlížečů
28.07.2023	Upozornění na zranitelnost MikroTik RouterOS CVE-2023-30799
20.06.2023	Upozorňujeme na zvýšené riziko ransomwarových útoků
12.06.2023	Upozorňujeme na kritickou zranitelnost FortiOS CVE-2023-27997
15.03.2023	NÚKIB upozorňuje na zranitelnost CVE-2023-23397
08.03.2023	Aplikace TikTok představuje bezpečnostní hrozbu
13.02.2023	Upozorňujeme na zneužití dokumentů OneNote ke stahování malware
15.12.2022	Upozorňujeme na kritickou zranitelnost FortiOS CVE-2022-42475
02.11.2022	Upozorňujeme na zranitelnosti knihovny OpenSSL ve verzi 3
01.11.2022	Upozorňujeme na zvýšené riziko DDoS útoků
17.10.2022	Upozorňujeme na závažnou zranitelnost Wi-Fi v linuxovém jádru
10.10.2022	Upozorňujeme na kritickou zranitelnost FortiGate CVE-2022-40684 (CVSS 9.6)
30.09.2022	Upozorňujeme na zranitelnost Microsoft Exchange Server CVE-2022-41040 (CVSSv3 6.3) CVE-2022-41082 (CVSSv3 8.8)
01.09.2022	Upozorňujeme na závažnou zranitelnost CVE-2022-26113 (CVSS 7.5) ve FortiClient
30.08.2022	Upozorňujeme na phishingovou kampaň s cílem zneužít bankovní identitu

Příloha č. 6 zadávací dokumentace

15.08.2022	Upozornění na sadu zranitelností týkající se softwaru VMware a platformy VMware vRealize Operations
31.05.2022	Upozornění na zranitelnost CVE-2022-30190
31.05.2022	Doplnění informací k varování NÚKIB v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací
30.05.2022	NÚKIB vydal Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím
14.04.2022	Upozorňujeme na stále trvající kampaň podvodných vishingových telefonátů
21.03.2022	NÚKIB vydal Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací
25.02.2022	NÚKIB v rámci preventivních kroků vydal v souvislosti s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou Varování
25.02.2022	Upozornění na výskyt nového destruktivního malware typu wiper
11.02.2022	Upozorňujeme na novou vlnu podvodných vishingových telefonátů
02.02.2022	Upozornění na kritickou zranitelnost Samba - CVE-2021-44142
28.01.2022	Upozornění na zvýšené riziko kyberšpionáží či ransomwarových útoků proti České republice
17.01.2022	Komentář GovCERT.CZ k napadení webů ukrajinské vlády a doporučení k zabezpečení
15.12.2021	NÚKIB vydává reaktivní opatření v souvislosti se zranitelností Log4Shell
10.12.2021	Upozornění na zranitelnost Apache Log4j - Log4Shell
18.11.2021	Situační přehled o zneužívání zranitelnosti ProxyShell pro potřeby doručování malwaru.
10.11.2021	Upozornění na zranitelnost MS Exchange Server a MS Excel
05.11.2021	Upozornění na kampaň zneužívající zranitelnosti Exchange Server
27.09.2021	Upozornění na aktivní zneužívání zranitelnosti vCenter serverů
17.09.2021	Upozornění na závažné zranitelnosti ohrožující systémy Linux v Azure
17.09.2021	Zveřejnění dešifrovacího nástroje pro ransomware REvil
13.08.2021	Upozornění na aktivní zneužívání zranitelnosti Microsoft Exchange Server - ProxyShell
21.07.2021	Upozornění na zranitelnost HiveNightmare
01.07.2021	AKTUALIZACE 07.07.: Upozornění na zranitelnost PrintNightmare
01.07.2021	Upozornění na aktivní zneužívání zranitelnosti Cisco ASA
16.06.2021	Upozornění na další vlnu vyděračské kampaně
27.05.2021	Upozornění na kritickou zranitelnost v produktu VMware vCenter
25.05.2021	Upozornění na probíhající kampaň ransomwaru Avaddon
21.05.2021	Upozornění na zranitelnost Windows HTTP Protocol Stack
06.05.2021	Upozornění na zranitelnost v systémovém ovladači od výrobců Dell a Alienware

Příloha č. 6 zadávací dokumentace

06.05.2021	Upozornění na zranitelnosti Exim
20.04.2021	Upozornění na vishing zneužívající identitu bankovních institucí
20.04.2021	Upozornění na zranitelnost Pulse Connect Secure
18.03.2021	Kritická zranitelnost v systému GitLab
12.03.2021	Upozornění na zranitelnosti zařízení BIG-IP a BIG-IQ společnosti F5
05.03.2021	Vyjádření k aktuální situaci
03.03.2021	Upozornění na zranitelnosti Exchange Server
25.02.2021	Upozornění na kritickou zranitelnost produktu VMWare vCenter Server
11.02.2021	Upozornění na kritické zranitelnosti v systémech Windows
04.02.2021	Upozornění na zranitelnost v programu sudo v operačních systémech Unix, Linux a MacOS
21.01.2021	Upozorňujeme na novou vlnu phishingových mailů
04.01.2021	Upozornění na zranitelnost firewallů a přístupových prvků Zyxel
04.01.2021	Upozornění na novou vlnu podvodných vyděračských emailů
18.12.2020	Doplnění informací k reaktivnímu opatření – software společnosti SolarWinds
14.12.2020	Upozornění na rizika softwaru firmy SolarWinds
01.10.2020	Upozornění na zvýšenou aktivitu malwaru Emotet
24.09.2020	Upozornění na zranitelnost Zerologon
15.07.2020	Upozornění na zranitelnost Windows DNS server
15.07.2020	Upozornění na zranitelnost SAP NetWeaver
22.05.2020	NXNSAttack - zranitelnost protokolu DNS
27.04.2020	Nová vlna vyděračských e-mailů
18.04.2020	NÚKIB vydal Varování před hrozbou a doporučil opatření
07.04.2020	Upozornění na hrozbu ransomware útoků
03.04.2020	Upozornění na rizika online konferenčních služeb
25.03.2020	Zranitelnost Adobe Type Manager v Microsoft Windows
12.03.2020	Upozornění na zranitelnost SMBv3
03.03.2020	Zranitelnost Microsoft Exchange Server
19.02.2020	Upozornění na podvodné emaily zneužívající epidemie Koronaviru
17.02.2020	Pozor na šířící se podvodný e-mail se zavirovanou přílohou!
29.01.2020	Aktualizace zranitelnosti systémů Citrix
24.01.2020	Aktualizace informací o hrozbě Emotet-Trickbot-Ryuk
22.01.2020	Upozornění na zranitelnost Internet Explorer
17.01.2020	Upozornění na zranitelnost systémů Citrix
15.01.2020	Kritické zranitelnosti operačního systému Windows
14.01.2020	Upozornění na zranitelnost Cable Haunt
23.12.2019	Varování o hrozbě Emotet-Trickbot-Ryuk
30.05.2019	Upozornění na závažné bezpečnostní aktualizace ve Fortinet VPN/Firewall produktech
04.04.2019	Varování před novým podvodným vyderačským e-mailem
20.12.2018	NÚKIB opakuje podstatné informace týkající se varování ze dne 17. 12. 2018
17.12.2018	Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou

Příloha č. 6 zadávací dokumentace

25.09.2018	Nebezpečná aplikace QRecorder
24.09.2018	Varování před podvodným vyderačským e-mailem
18.09.2018	Varování před cílenými phishingovými útoky na akademickou sféru
29.06.2018	Ransomware je stále aktuální hrozbou
14.05.2018	Efail - kritická zranitelnost postihující PGP a S/MIME
05.01.2018	Meltdown - chyba v moderních procesorech
04.01.2018	Spectre - chyba v moderních procesorech
25.10.2017	Nový ransomware Bad Rabbit
17.10.2017	ROCA - zranitelnost v generování RSA klíčů
16.10.2017	KRACK - zranitelnost protokolu WPA2 umožňuje čtení šifrovaných dat
27.06.2017	Petya/Petrwrap/NotPetya - nová hrozba ransomwaru
13.06.2017	Crash Override - Win32/Industroyer - nová hrozba pro průmyslové řídicí systémy
23.05.2017	EternalRocks - vážnější hrozba než WannaCry
15.05.2017	Ransomware WannaCry
10.05.2017	Nová vlna podvodných e-mailových zpráv cílí na klienty bank
02.02.2017	JScript Ransomware RPG