MĚSTO LANŠKROUN

nám. J. M. Marků 12
Lanškroun - Vnitřní Město
563 01 Lanškroun
www.lanskroun.eu

Vyřizuje: Miroslav Krsek
Telefon: 778 888 031
E-mail: Miroslav.krsek@lanskroun.eu
Čj.: MULA 32922/2024
Vaše značka:
Počet listů dokumentu: 21
Počet příloh: 3
Počet listů příloh: 9
Spisový znak: 91.3
Spisová značka:
Skartační lhůta: S10

V Lanškrouně 4. prosince 2024

Zadávací podmínky a Zadávací dokumentace (dále jen „ZD“)
na veřejnou zakázku malého rozsahu na služby dle zákona č. 134/2016 Sb. o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ“).

Zadavatel:

Název zadavatele: Město Lanškroun
Sídlo zadavatele: nám. J. M. Marků 12, Lanškroun-Vnitřní Město, 563 01 Lanškroun
IČ: 00279102
Osoba oprávněná jednat: Mgr. Radim Vetchý, starosta města
Profil zadavatele: https://zakazky.lanskroun.eu/

Zadavatel si Vás dovoluje vyzvat k podání cenové nabídky na akci:

Název zakázky:
„GAP analýza v rámci projektu Kybernetická bezpečnost ICT MĚSTSKÉHO ÚŘADU LANŠKROUN“

Preambule:
Jedná se o zadání veřejné zakázky malého rozsahu podle ustanovení §27 písm.a) a § 31 ZZVZ při dodržení zásad uvedených v §6 odst.1 až 3 ZZVZ a §4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „zákon o střet zájmů“).
Tyto zadávací podmínky a Zadávací dokumentace jsou vypracovány ve smyslu „Směrnice pro zadávání veřejných zakázek malého rozsahu Městem Lanškroun“ schválené usnesením rady města č. 199/RM/2023 ze dne 03.05.2023 jako podklad pro podání nabídek vyzvaných účastníků v rámci zadání zakázky malého rozsahu

na služby (dále jen veřejná zakázka). Při zadání veřejné zakázky malého rozsahu není zadavatel povinen použít ustanovení ZZVZ. Pokud se dále v textu vyskytne odkaz na zákon nebo jsou použity zákonné pojmy, jde jen o podpůrný krok a zadavatel se bude citovanými ustanoveními zákona nebo pojmy řídit pouze přiměřeně.

1. Vymezení předmětu plnění veřejné zakázky

Předmětem plnění veřejné zakázky je zpracování GAP analýzy.

Zadavatel požaduje zpracování GAP analýzy vůči:

- stávajícímu zákonu o kybernetické bezpečnosti – zákon o o kybernetické bezpečnosti 181/214 Sb. v aktuálním znění a prováděcí vyhláškou 82/2018 Sb.
- návrhu nového zákona o kybernetické bezpečnosti (Implementace NIS2 do české legislativy) - dle aktuálního návrhu ke dni podpisu smlouvy, uveřejněné v elektronické knihovně VeKLEP (https://odok.cz/portal/veklep/materialy) .

CÍLE GAP ANALÝZY

1. **Komplexní zmapování a analýza**:
   - Procesních postupů organizace z hlediska řízení kybernetické bezpečnosti.
   - Veškerých technologií používaných v ICT a OT prostředí, včetně zařízení úředníků.
2. **Identifikace nedostatků**:
   - Posouzení souladu aktuálního stavu s požadavky ZKB a směrnice NIS2 s ohledem na procesní, faktické fungování organizace včetně technického zajištění fungování organizace (ICT, IO, fyzického zabezpečení apod.).
   - Vyhodnocení bezpečnostních rizik z pohledu organizace i rizik a zranitelností v ICT a OT prostředí.
3. **Návrh konkrétních opatření**:
   - Konkrétní procesní i technická doporučení, která zajistí dodržení legislativních požadavků.
   - Podrobné návrhy na tvorbu nebo aktualizaci interní dokumentace potřebné pro zajištění souladu s legislativou.

SPECIFIKACE PŘEDMĚTU PLNĚNÍ

1. Analýza prostředí

1. **ICT infrastruktura**:
   - **Servery**: Posouzení konfigurací, verzí operačních systémů, aplikací, bezpečnostních záplat apod.
   - **Síťové prvky a Firewall**: Analýza firewall politik, segmentace sítě, směrovačů, přepínačů a bezpečnostní politik content filteringu, veřejně dostupných služeb apod.
   - **VPN:** Posouzení nastavení VPN tunelů, autentizace uživatelů a šifrování přenosu dat.

     Hodnocení politik pro vzdálený přístup a ochranu přístupových bodů.

- **Wi-Fi sítě**: Posouzení šifrování komunikace, autentizace uživatelů a izolace přístupových bodů.
- **Uživatelské zařízení**: Posouzení bezpečnostních politik na počítačích a noteboocích úředníků, včetně ochrany proti virovým nákazám, správy přístupů a šifrování dat.

2. **OT prostředí**:
   - Identifikace zařízení používaných v provozních systémech. Doporučení na jejich bezpečné začlenění do stávající ICT infrastruktury.
   - Oddělení OT sítí od ICT prostředí a způsoby zabezpečení jejich přístupu.
3. **Cloudové služby**:
   - Zabezpečení přístupu, šifrování dat, zálohování a smluvní ujednání s poskytovateli služeb. Posoudit aktuální stav zabezpečení cloudových služeb využívaných organizací. Zajistit, že přístup k těmto službám je bezpečný, data jsou šifrována a zálohována v souladu s požadavky kybernetické bezpečnosti, a smlouvy s poskytovateli služeb obsahují klíčová ustanovení zajišťující ochranu dat a dodržení legislativy. Navrhnout opatření v případě rozšiřování služeb.

Správa identit a přístupů (IAM):

- Posouzení, zda organizace používá centralizované řízení přístupů k cloudovým službám (např. Azure AD, Okta, AWS IAM).
- Kontrola, zda jsou přístupy řízeny podle zásady **„nejnižšího oprávnění“** (least privilege).
- Analýza pravidel pro odnímání přístupů (např. po ukončení pracovního poměru).

Autentizace:

- Zavedení vícefaktorové autentizace (MFA) pro všechny účty s přístupem do cloudu.
- Ověření, zda je implementována ochrana proti brute force útokům (např. omezení počtu pokusů o přihlášení, detekce podezřelých přístupů).

Monitorování přístupů:

- Logování a analýza všech přístupů do cloudových systémů.
- Použití nástrojů pro detekci anomálií a podezřelých aktivit (např. UEBA – User and Entity Behavior Analytics).

Šifrování dat

Šifrování dat v klidu (data at rest):

- Ověření, zda jsou všechna data uložená v cloudu šifrována pomocí moderních algoritmů (např. AES-256).
- Posouzení správy šifrovacích klíčů:
  - Použití dedikovaných HSM (Hardware Security Modules).

- Zavedení Key Management Systems (např. AWS KMS, Azure Key Vault).

Šifrování dat při přenosu (data in transit):

- Zajištění, že veškerá komunikace s cloudem probíhá přes šifrované protokoly (např. TLS 1.3).
- Ověření, zda aplikace a API používají zabezpečené kanály pro přenos dat.

Šifrování záloh:

- Posouzení, zda jsou zálohy v cloudu šifrovány, a zajištění, že k nim mají přístup pouze oprávněné osoby.

Zálohování dat

Strategie zálohování:

- Analýza nastavení zálohování v cloudu:
  - Frekvence záloh (např. denní, hodinové).
  - Možnost okamžité obnovy dat.
- Zajištění geografické redundance záloh.

Testování obnovy dat:

- Kontrola, zda jsou pravidelně prováděny testy obnovitelnosti dat.
- Zajištění, že testy obnovy neohrozí provozní systémy.

Automatizace zálohování:

- Zavedení nástrojů pro automatizované zálohování s notifikacemi o úspěšnosti.

Smluvní ujednání s poskytovateli služeb

Legislativní požadavky:

- Posouzení, zda smlouvy s poskytovateli služeb obsahují ustanovení o dodržování legislativy (např. GDPR, ZKB).
- Zajištění, že poskytovatelé mají odpovídající certifikace (např. ISO 27001, SOC 2).

Podmínky ochrany dat:

- Kontrola, zda smlouvy obsahují:
  - Závazek šifrování dat zákazníka.
  - Odpovědnost za bezpečnost dat uložených v cloudu.
  - Zásady přístupu poskytovatele k datům.

Podmínky provozu a dostupnosti:

- Analýza SLA (Service Level Agreements) pro zajištění dostupnosti služeb (např. 99,9 % uptime).

Postup při ukončení spolupráce:

- Ustanovení o bezpečném odstranění dat po ukončení smlouvy.
- Zajištění možnosti migrace dat k jinému poskytovateli.

4. **Fyzické zabezpečení**:
    - Posouzení přístupových systémů, kamerového dohledového systému a fyzického oddělení kritických zařízení.
5. **Aplikace**:
    - Bezpečnostní audit aplikací, správa přístupů a oprávnění, aktualizace a monitorování aktivit. Provést detailní analýzu bezpečnosti aplikací používaných v organizaci, zhodnotit jejich aktuální stav z pohledu kybernetické bezpečnosti, správy přístupů a oprávnění, a poskytnout doporučení pro zlepšení. Zajistit, že aplikace jsou aktualizovány, monitorovány a spravovány tak, aby nedocházelo k bezpečnostním incidentům či únikům dat. Tato část analýzy zajistí, že aplikace budou zabezpečeny proti hrozbám, jejich přístupy efektivně spravovány a aktualizace i monitorování prováděny v souladu s osvědčenými postupy.

Bezpečnostní audit aplikací

Identifikace používaných aplikací:

- Sestavení seznamu všech aplikací v organizaci:
    1. Kritické aplikace (např. ekonomické systémy, systémy pro správu dat).
    2. Aplikace využívané pro komunikaci a spolupráci (např. e-mailové systémy, MS Teams).
    3. Interní a externí aplikace (cloudové služby, SaaS platformy).
- Zohlednění aplikací provozovaných na různých platformách (on-premises, cloud, mobilní zařízení).

Zhodnocení zabezpečení aplikací:

- Analýza aplikací z hlediska:
    1. Autentizace a autorizace uživatelů.
    2. Použití šifrování dat (např. šifrování uložených dat i dat v přenosu).
    3. Odolnosti vůči zranitelnostem (např. SQL injection, XSS, CSRF).
- Provádění bezpečnostního testování:
    1. Penetrační testy pro simulaci možných útoků.
    2. Kontroly zranitelností pomocí nástrojů (např. Nessus, OpenVAS).

Posouzení souladu s legislativou a normami:

- Ověření, zda aplikace splňují požadavky legislativy (např. GDPR, ZKB) a standardů (např. ISO 27001).

Správa přístupů a oprávnění

Audit uživatelských oprávnění:

- Analýza, kdo má přístup k aplikacím a jaká oprávnění jsou přiřazena.
- Zjištění, zda je uplatňován princip **„nejnižšího oprávnění“** (least privilege).
- Identifikace neaktivních účtů a zajištění jejich deaktivace.

Autentizace a autorizace:

- Zhodnocení používaných metod autentizace:
    1. Podpora vícefaktorové autentizace (MFA).
    2. Bezpečnostní standardy hesel (délka, komplexita, expirace).
- Posouzení řízení přístupů podle rolí (RBAC – Role-Based Access Control) nebo atributů (ABAC – Attribute-Based Access Control).

Správa přístupů externistů a dočasných účtů:

- Zajištění, že přístupy externích dodavatelů nebo projektových týmů jsou časově omezené a kontrolované.

Aktualizace aplikací

Zhodnocení procesu aktualizací:

- Analýza, zda jsou aplikace pravidelně aktualizovány a záplatovány.
- Zjištění, zda jsou aplikace monitorovány na známé zranitelnosti (např. pomocí databází CVE).

Automatizace záplatování:

- Posouzení, zda organizace využívá nástroje pro automatizaci záplat (např. WSUS, SCCM, cloudové platformy).
- Identifikace aplikací s omezenou podporou aktualizací nebo zastaralými verzemi.

Plánování a testování aktualizací:

- Zajištění, že záplaty jsou testovány před nasazením do produkčního prostředí.
- Plánování aktualizací tak, aby minimalizovaly dopad na provoz organizace.

Monitorování aktivit

Logování a sledování uživatelských aktivit:

- Kontrola, zda aplikace logují klíčové aktivity:
    1. Přístupy uživatelů (kdo, kdy, odkud).

2. Změny konfigurace a oprávnění.
3. Neúspěšné pokusy o přístup nebo útoky.

- Zavedení standardizovaného formátu logů a jejich integrace do SIEM systémů.

Detekce a analýza anomálií:

- Implementace nástrojů pro detekci neobvyklých aktivit (např. přístupy mimo pracovní dobu, přístupy z neznámých IP adres).
- Analýza chování uživatelů pomocí UEBA (User and Entity Behavior Analytics).

Reakce na incidenty:

- Provázání monitorovacích nástrojů s procesy řízení incidentů (např. SOAR systémy).
- Zajištění okamžitého upozornění na kritické události.

6. **Šifrovací technologie**:
   - Zhodnocení použitých šifrovacích mechanismů pro data na koncových zařízeních a pro přenosové trasy. Posoudit stávající šifrovací technologie používané v organizaci pro ochranu dat na koncových zařízeních a při jejich přenosu. Identifikovat slabiny, posoudit, zda šifrování odpovídá aktuálním standardům, navrhnout konkrétní opatření pro zajištění bezpečnosti citlivých informací (správa klíčů, identifikace nešifrované komunikace a uložených dat, použití zastaralých šifrovacích mechanismů, šifrování e-mailové komunikace, interní síťové komunikace, webové služby, VPN připojení apod.)
7. **Logování a monitorování**:
   - Nastavení SIEM systémů, pokrytí monitoringu událostí a detekce bezpečnostních událostí a incidentů. Zajistit efektivní logování a monitorování veškeré IT infrastruktury a procesů, které jsou klíčové pro detekci, analýzu a prevenci kybernetických hrozeb. Tato část se zaměřuje na zhodnocení aktuálního stavu logování a monitorování, identifikaci slabin a návrh zlepšení, včetně integrace do systémů řízení bezpečnostních událostí (SIEM). Organizace získá komplexní přehled a návrhy efektivního systému logování a monitorování, který podpoří detekci a prevenci bezpečnostních incidentů, zvýší transparentnost a splní legislativní požadavky. Analýza by měla zahrnovat:

<u>Analýzu stávajícího logování</u>

Identifikaci logovaných systémů a událostí:

- Přehled systémů, které generují logy:
  1. Servery, síťová zařízení (firewally, přepínače, směrovače), koncová zařízení.
  2. Aplikace, databáze, cloudové služby apod.
- Typy logovaných událostí:
  1. Přihlašování a odhlašování uživatelů.
  2. Změny oprávnění a konfigurací.
  3. Neúspěšné pokusy o přístup (např. brute force útoky).

4. Síťový provoz (např. blokované pokusy o přístup, DDoS útoky).

Pokrytí a granularita logování:

- Zjištění, zda jsou logovány všechny důležité události a s dostatečnou úrovní podrobnosti.
- Identifikace mezer v logování (např. chybějící logy pro určité aplikace nebo zařízení).

Ukládání a přístup k logům:

- Doba uchovávání logů (např. 6 měsíců, 1 rok) a splnění legislativních požadavků.
- Bezpečnost uložených logů (např. šifrování, přístupové kontroly).
- Posouzení, zda jsou logy centralizovány (např. v SIEM systému).

Analýza stávajícího monitorování

Sledované systémy:

- Přehled infrastruktury pokryté aktivním monitorováním:
- Klíčové systémy, jako jsou servery, firewally, VPN, koncová zařízení, aplikace.
- Externí služby a clustery (např. cloudové služby, SaaS).

Technologie monitorování:

- Zhodnocení používaných nástrojů (např. Zabbix, Nagios, Splunk, Microsoft Sentinel).
- Posouzení, zda jsou nástroje schopny detekovat anomálie a generovat alerty.

Reakce na incidenty:

- Zjištění, zda je zavedena automatizace při detekci problémů (např. automatické blokování IP při detekci neautorizovaného přístupu).
- Provázanost monitorovacích systémů s procesy řízení incidentů.

Návrh vylepšení logování

Rozšíření pokrytí logování:

- Zajištění, že všechny klíčové systémy a aplikace generují logy.
- Zavedení logování na úrovni aplikační vrstvy, operačních systémů a síťových zařízení.

Centralizace logů:

- Implementace SIEM systému (např. Splunk, IBM QRadar, Microsoft Sentinel) pro centralizované ukládání a analýzu logů.
- Vytvoření standardního formátu logů pro snadnější zpracování a analýzu.

Ochrana a archivace logů:

- Šifrování logů a zavedení přístupových kontrol pro zajištění integrity.
- Definice politik pro uchovávání logů v souladu s legislativními požadavky a potřebami organizace.

Návrh vylepšení monitorování

Zavedení pokročilých nástrojů:

- Implementace nástrojů pro detekci anomálií na základě strojového učení.
- Rozšíření pokrytí o monitorování chování uživatelů (UEBA – User and Entity Behavior Analytics).

Automatizace reakce:

- Zavedení SOAR (Security Orchestration, Automation, and Response) systémů pro automatizované řešení incidentů.
- Například automatické blokování podezřelých IP adres nebo izolace infikovaných zařízení.

Integrace monitorovacích systémů:

- Provázání monitorovacích nástrojů se SIEM pro jednotný pohled na bezpečnostní incidenty.
- Vytvoření přehledných dashboardů pro sledování aktuálního stavu a alertů.

Systémy pro hlášení a notifikace

- **Alertování a eskalace**:
- Definování pravidel pro generování alertů na základě předdefinovaných podmínek (např. podezřelá aktivita, dosažení prahových hodnot).
- Nastavení eskalace podle závažnosti incidentu.

Real-time notifikace:

- Implementace nástrojů pro okamžité notifikace (e-mail, SMS, push notifikace).
- Možnost sledování alertů v mobilních aplikacích

2. Analýza procesů a dokumentace

1. **Řízení přístupů**:
    - Politiky správy uživatelských oprávnění, autentizace a přidělování přístupů. Zajistit, že řízení přístupů v organizaci je efektivní, bezpečné a odpovídá nejlepším praxím a legislativním požadavkům (ZKB, směrnice NIS2). Analýza řízení přístupů zahrnuje posouzení stávajících politik, procesů a technologií pro správu uživatelských oprávnění, autentizaci a přidělování přístupů.

Zmapování stávajících pravidel a postupů:

- Přezkum existujících dokumentů a směrnic upravujících správu uživatelských oprávnění a přístupů.

- Zjištění, zda jsou jasně definovány následující aspekty:
- Kdo je oprávněn přidělovat přístupy.
- Jaké procesy musí být dodrženy při přidělování, změně nebo odebrání přístupů.
- Frekvence a metody kontroly oprávnění.

Existence formální politiky správy přístupů:

- Zhodnocení, zda je implementována a aplikována zásada **„nejnižšího oprávnění“** (princip least privilege).
- Posouzení, zda existují pravidla pro dočasné oprávnění (např. při specifických projektech nebo dočasném přístupu externistů).

Audit přístupů:

- Zjištění, zda organizace pravidelně kontroluje oprávnění a přístupové logy.
- Analýza, zda existuje mechanismus pro detekci neautorizovaných přístupů.

Analýza technických prostředků pro řízení přístupů

Mechanismy autentizace:

- Posouzení aktuálního stavu autentizačních metod:
- Silné heslové politiky (např. minimální délka, expirace hesel).
- Vícefaktorová autentizace (MFA) pro citlivé systémy a vzdálený přístup (např. VPN).
- Biometrické ověřování (pokud je implementováno).

Technologie správy identit (IAM):

- Zjištění, zda organizace využívá centrální nástroje pro správu identit (např. Active Directory, Azure AD, Okta).
- Posouzení schopností IAM systémů:
- Automatizace přidělování oprávnění.
- Integrace s dalšími aplikacemi a systémy.
- Sledování přístupů a generování auditních zpráv.

Logování přístupů:

- Zhodnocení, zda jsou všechny přístupy zaznamenávány a logy pravidelně kontrolovány.
- Posouzení, zda jsou logy integrovány do SIEM systému pro detekci neobvyklých aktivit.

Posouzení procesů přidělování, změny a odebrání přístupů

Přidělování oprávnění:

- Analýza procesů pro přidělování nových oprávnění:
- Existují definované pracovní role a jejich oprávnění?

- Je zajištěno, že přístupy jsou přiděleny na základě zásady „nejnižšího oprávnění“?

Změna oprávnění:

- Jakým způsobem se mění oprávnění při změně pracovní pozice, oddělení nebo zodpovědnosti.
- Zda existuje dokumentace a evidence změn oprávnění.

Odebrání přístupů:

- Postupy při ukončení pracovního poměru nebo při odchodu zaměstnance z organizace.
- Zajištění, že přístupy jsou okamžitě deaktivovány.
- Kontrola, zda byly deaktivovány i přístupy k externím systémům a aplikacím.

Detekce a prevence neautorizovaných přístupů

Monitorování a alerting:

- Zjištění, zda organizace používá nástroje pro detekci neautorizovaných přístupů (např. přístupy mimo pracovní dobu, přístupy z neznámých IP adres).

Reakce na incidenty:

- Existence procesů pro reakci na detekci neautorizovaného přístupu.
- Dokumentace a analýza bezpečnostních incidentů spojených s přístupem.

2. **Incident management**:
    - Doporučení postupů pro hlášení, řešení a dokumentaci kybernetických incidentů. Zajistit, aby organizace měla efektivní systém pro detekci, hlášení, řešení a dokumentaci kybernetických incidentů. Tato část analýzy má pomoci vytvořit strukturovaný a funkční proces řízení incidentů, který zajistí rychlou a efektivní reakci na hrozby, minimalizuje dopady incidentů a umožní jejich následnou analýzu pro prevenci podobných situací v budoucnu.
3. **Řízení rizik**:
    - Metodiky identifikace, hodnocení a mitigace rizik v oblasti kybernetické bezpečnosti.
    - Posoudit a zhodnotit stávající přístup organizace k řízení rizik v oblasti kybernetické bezpečnosti, identifikovat případné mezery a navrhnout implementaci efektivních metodik pro identifikaci, hodnocení a mitigaci rizik. Výsledkem této části GAP analýzy bude zvýšení schopnosti organizace předcházet bezpečnostním incidentům a efektivně reagovat na potenciální hrozby.
4. **Zálohování a obnova dat**:
    - Analýza plánů zálohování, zálohovací strategie a úložišť.

- Analýza retence zálohování a pravidelného reportování o stavu záloh
- Testování obnovy zálohování
- Konfigurace šifrování záloh, datových prostupů, zabezpečení

5. **Školení a povědomí**:
    - Hodnocení školení zaměstnanců o kybernetických hrozbách a postupech.
    - Posoudit stávající úroveň povědomí zaměstnanců o kybernetických hrozbách, jejich připravenost reagovat na bezpečnostní incidenty a aktuálnost a kvalitu školení zaměřených na kybernetickou bezpečnost. Výsledky pomohou identifikovat slabá místa v oblasti lidského faktoru, který bývá klíčovým rizikem při zabezpečení organizace.
6. **Soulad s legislativou**:
    - Porovnání procesů a dokumentace s požadavky ZKB a směrnice NIS2.

2. Rozhovory s vybranými respondenty zadavatele

Rozhovory s klíčovými respondenty zadavatele jsou zásadním krokem při zjišťování aktuálního stavu systému kybernetické bezpečnosti. Účelem je získat detailní informace o fungování technických a procesních opatření přímo od osob odpovědných za různé aspekty kybernetické bezpečnosti a jejich implementaci. Tato část GAP analýzy zajistí hlubší pochopení specifických potřeb organizace a umožní navrhnout opatření, která budou reflektovat skutečný stav a požadavky jednotlivých částí úřadu.

Specifikace činností:

1. Identifikace respondentů

Pro efektivní rozhovory je nezbytné zapojit tyto role a oblasti:

- **Vedení organizace** (manažeři, vedoucí odborů):
    - Informace o strategických prioritách organizace v oblasti kybernetické bezpečnosti.
    - Přístup k financování a rozhodování o implementaci bezpečnostních opatření.
- **IT oddělení a správci systémů**:
    - Detaily o technické infrastruktuře, včetně serverů, firewallů, VPN a síťových prvků.
    - Informace o správě uživatelských účtů, logování událostí a aktualizacích systémů.
- **Zodpovědné osoby za fyzické zabezpečení**:
    - Informace o přístupových systémech, monitorování prostor a bezpečnosti zařízení.
- **Zaměstnanci úřadu – běžní uživatelé**:
    - Zpětná vazba na používané aplikace, bezpečnostní povědomí a případné problémy při práci s technologií.

2. Příprava rozhovorů

- **Strukturované otázky**:

- Pro každou skupinu respondentů budou připraveny otázky zaměřené na konkrétní oblasti, jako jsou technické postupy, organizace procesů, povědomí o kybernetické bezpečnosti a spolupráce s dodavateli.
- Příklad otázek pro IT oddělení:
  - Jaké technologie a nástroje jsou aktuálně používány pro detekci a prevenci kybernetických hrozeb?
  - Jak často dochází k aktualizaci systémů, včetně aplikací a operačních systémů?
  - Jaké jsou postupy při řešení kybernetických incidentů?
- Příklad otázek pro vedení organizace:
  - Jaká je strategie organizace pro zlepšení kybernetické bezpečnosti?
  - Jaké jsou klíčové překážky při implementaci bezpečnostních opatření?

- **Záznam rozhovorů**:
  - Všechny rozhovory budou zaznamenány (se souhlasem respondentů) pro účely následné analýzy.

3. Oblasti hodnocení

- **Technické zabezpečení**:
  - Informace o aktuální konfiguraci zařízení (firewally, VPN, servery).
  - Problémy a překážky při implementaci technických opatření.
- **Procesní nastavení**:
  - Zhodnocení existence postupů pro řízení incidentů, správu přístupů a zálohování.
  - Identifikace mezer v procesní dokumentaci.
- **Lidský faktor**:
  - Povědomí o kybernetických rizicích a úroveň školení zaměstnanců.
  - Chování uživatelů v rámci pracovních postupů (např. správa hesel, používání neautorizovaných aplikací).

4. Zpracování výsledků rozhovorů

- **Analýza získaných dat**:
  - Konsolidace odpovědí od respondentů do přehledné struktury (např. silné stránky, nedostatky, návrhy zlepšení).
- **Identifikace rizik a nedostatků**:
  - Nedostatečná školení zaměstnanců, absence klíčových dokumentů, zastaralé technologie nebo nejednotné postupy.
- **Návrhy opatření**:
  - Na základě rozhovorů budou formulovány doporučení pro zlepšení v oblastech technické i procesní bezpečnosti.

3. Ostatní požadavky

- Posouzení, podle návrhu Vyhlášky o regulovaných službách*, zda zadavatel je poskytovatelem regulované služby v režimu vyšších povinností nebo nižších povinností. Posouzení, zda zadavatel spadá pod režim **vyšších** nebo **nižších povinností** dle návrhu Vyhlášky o regulovaných službách, je zásadní pro určení rozsahu a povahy bezpečnostních opatření, která organizace musí zavést. Tento krok zajistí, že doporučení z GAP analýzy odpovídají přesně legislativním požadavkům na poskytovatele regulovaných služeb.
- Posouzení, podle návrhu Vyhlášky o regulovaných službách*, zda zadavatel je poskytovatelem regulované služby v režimu vyšších povinností nebo nižších povinností.
- Provedení rozdílové analýzy bude provedeno vůči návrhu Zákona o kybernetické bezpečnosti a vůči návrhu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*, v případě, že zadavatel bude poskytovatelem regulované služby v režimu vyšších povinností.
- Provedení rozdílové analýzy bude provedeno vůči návrhu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinnost*, v případě, že zadavatel bude poskytovatelem regulované služby v režimu nižších povinností

VÝSTUPY GAP ANALÝZY

1. **Zpráva z GAP analýzy**:
    - **Manažerské shrnutí**:
        - Stručné zhodnocení aktuálního stavu kybernetické bezpečnosti organizace.
        - Klíčová rizika a doporučené priority pro vedení.
    - **Detailní technické hodnocení, stav bezpečnostních opatření**:
        - Popis stávajícího stavu ICT a OT infrastruktury, včetně zranitelností.
        - Návrhy konkrétních technických opatření (např. konfigurace firewallů, segmentace sítě, šifrování pro všechny výše uvedené systémy).
        - Popis aktuálních procesů a postupů v organizaci v oblasti kybernetické bezpečnosti
        - Vyhodnocení procesních požadavků ZKB vůči stávajícímu stavu (např. dokumentace, monitorování, incident management apod.)
        - Specifikace problémů na infrastruktuře z hlediska konfigurací, verzí, zranitelností šifrování
        - Podrobné porovnání současného a požadovaného technického nastavení.
        - Identifikace kritických závislostí (např. potřebná aktualizace systému před implementací dalšího opatření).
        - Přehled logovaných událostí a monitorovaných systémů, zhodnocení stavu.

- Přehled používaných aplikací, jejich zabezpečení, oprávnění a stavu aktualizací, Identifikace zranitelností a neaktuálních aplikací.
- Zpráva o stávajícím stavu zabezpečení cloudových služeb. Přehled bezpečnostních opatření, jako je šifrování dat, správa přístupů a zálohování. Identifikace slabin v zabezpečení cloudových služeb.

- **Procesní hodnocení**:
  - Analýza souladu současných procesů s legislativou.
  - Chybějící procesy a návrhy na tvorbu konkrétních nových procesů včetně návrhu jejich obsahu a aktualizaci dokumentace.

- **Návrh nápravných opatření**
  - Návrhy organizačních a technických opatření v souladu s novým ZKB.
  - Detailní popis implementace:
    1. Organizační opatření: školení zaměstnanců, revize dokumentace.
    2. Technická opatření: specifikace konkrétních konfiguračních kroky, aktualizace softwaru.
  - Podrobné porovnání současného a požadovaného technického nastavení.
  - Identifikace kritických závislostí (např. potřebná aktualizace systému před implementací dalšího opatření).
  - Doporučení na pravidelné provádění auditů a testování bezpečnosti.
  - Konkrétní návrhy na rozšíření pokrytí logování, zavedení standardů a ochranu logů, na základě identifikace slabin, konkrétní opatření na zavedení standardů a vhodných opatření na ochranu logů apod.
  - Doporučení pro správu uživatelských přístupů, návrh postupů pro pravidelné audity uživatelských oprávnění, aktualizaci aplikací, bezpečného přístupu apod.
  - Všechna opatření budou řešena z pohledu procesního i technického a zaměřena na zvýšení kybernetické bezpečnosti organizace.
  - Návrhy opaření pro zabezpečení cloudových služeb.

- **Zhodnocení aktuálního stavu řízení rizik:**
  - Přehled používaných metodik, nástrojů a postupů.
  - Identifikace nedostatků v současném přístupu k řízení rizik.
  - Mapa rizik organizace:
  - Seznam klíčových aktiv a jejich hrozeb.
  - Kategorizace rizik podle závažnosti.

- Doporučení na mitigaci rizik
- Konkrétní technická a organizační opatření pro snížení identifikovaných rizik apod.
- Návrh procesu pro průběžné řízení rizik (identifikace, hodnocení, mitigace).
- Doporučení na pravidelnou aktualizaci mapy rizik.

- **Podrobná rozdílová analýza všech výše uvedených bodů**:

  Porovnání současného stavu s požadavky ZKB a NIS2, zejména s ohledem

  na body uvedené v kapitole SPECIFIKACE PŘEDMĚTU PLNĚNÍ. Zhodnocení bude provedeno z pohledu procesního i z pohledu technické realizace.

- **Harmonogram implementace**:
  - Prioritizace kroků na krátkodobé, střednědobé a dlouhodobé opatření.

2. **Podklady pro výběrové řízení**:
   - **Obecné technické požadavky a funkcionality**:
     - Požadavky na HW, SW – funkcionality, implementační práce, včetně technických návrhů pro realizaci opatření jako možný podklad pro výběrového řízení na dodávku technologií s cílem zajistit soulad organizace se zákonem o kybernetické bezpečnosti (ZKB) a směrnicí NIS2. Technické požadavky zohlední potřeby organizace, identifikované v GAP analýze, a budou navrženy tak, aby zlepšily úroveň kybernetické bezpečnosti.
   - **Doporučení pro smluvní podmínky**:
     - Zahrnutí klíčových aspektů kybernetické bezpečnosti do smluv s dodavateli.
3. **Vyhodnocení rozhovorů s respondenty**
   - Zhodnocení povědomí o kybernetických rizicích, identifikace chybějících témat apod.

2. Termíny plnění zakázky
Zakázku bude možné realizovat v období od podpisu smlouvy o dílo s ukončením a předáním předmětu veřejné zakázky dle čl. 1. Termín celkového ukončení díla je nejpozději do 28.02.2025.

3. Místo plnění veřejné zakázky: Lanškroun, Městský úřad Lanškroun

4. Podmínky kvalifikace dle § 73 – 88 ZZVZ

4.1 Základní způsobilost dle § 74 ZZVZ
1) Způsobilým není dodavatel, který:

a) byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 k tomuto zákonu nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,
b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
e) je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

2) Je-li dodavatelem právnická osoba, musí podmínku podle odstavce 1 písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku podle odstavce 1 písm. a) splňovat
a) tato právnická osoba,
b) každý člen statutárního orgánu této právnické osoby a
c) osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

3) Účastní-li se zadávacího řízení pobočka závodu
a) zahraniční právnické osoby, musí podmínku podle odstavce 1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu,
b) české právnické osoby, musí podmínku podle odstavce 1 písm. a) splňovat osoby uvedené v odstavci 2 a vedoucí pobočky závodu.

Dodavatel prokazuje základní způsobilost způsobem dle § 53 odst. 4 ZVZZ. Vzor čestného prohlášení je v příloze č. 3 této ZD.

4.2 Profesní způsobilost dle § 77 ZZVZ

Dodavatel prokáže, že splňuje profesní způsobilosti ve vztahu k České republice doložením alespoň jedné z certifikací z oblasti kontroly a řízení bezpečnosti informačních technologií.

Dodavatel prokazuje profesní způsobilost způsobem dle § 53 odst. 4 ZVZZ. Vzor čestného prohlášení je v příloze č. 3 této ZD.

4.3 Technická kvalifikace dle § 79 ZZVZ

K prokázání kritérií technické kvalifikace dle §79 odst. 2 písm. b), c), d), a e) zákona o zadávání veřejných zakázek zadavatel požaduje:

- Předložení minimálně 2 referenčních zakázek, jejichž předmětem byla GAP analýza, která zahrnovala zhodnocení procesů, politik, nastavení informačních systémů včetně návrhů opatření procesních i technických. Minimální objem jedné zakázky činí 300 000 Kč bez DPH.
- předložení seznamu techniků nebo technických útvarů, které se budou podílet na plnění veřejné zakázky, bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli. **Požadovaná minimální úroveň:**

1. **Specialista na kybernetickou bezpečnost:**
   - Certifikovaný odborník s hlubokou znalostí ICT a OT prostředí, bezpečnostních technologií a legislativy (ZKB , znalost NIS2).
   - Certifikace v oblasti kontroly a řízení bezpečnosti informačních technologií – certifikace CISA (http://www.isaca.cz/cs/certifikace-cisa) nebo Lead Auditor Information Security Management System (Lead Auditor ISMS)
   - Zkušenost na uvedené nebo jiné obdobné pozici u minimálně 3 projektů v posledních 3 letech v oblasti informačních technologií, na pozici specialista kybernetické bezpečnosti nebo obdobné pozici související s návrhem nebo implementací opatření v oblasti kybernetické bezpečnosti, zahrnující analýzu rizik a návrhy opatření. Minimální rozsah projektů ve výši 300 000 Kč bez DPH;
2. **Technický specialista – architekt ICT infrastruktury:**
   - Zkušenosti s implementací technických opatření dle ZKB znalost NIS2.
   - Certifikace pro návrh a implementaci informačních systémů dle jedné z následujících certifikací: TOGAF, Archimate, BPMN nebo podle jiné rovnocenné certifikace metodiky pro návrh architektury informačních systémů rovnocenné uvedeným certifikacím; minimálně na úrovni „Certified“ či obdobné úrovně.
   - Zkušenost na uvedené nebo jiné obdobné pozici v posledních 3 letech u minimálně 3 projektů v oblasti informačních technologií, na pozici architekt řešení nebo obdobné pozici související s návrhem enterprise nebo solution architektury informačních systémů, zahrnující analýzu prostředí a návrh technických opatření kybernetické bezpečnosti. Minimální rozsah projektů ve výši 300 000 Kč bez DPH;
3. **Procesní analytik:**
   - Schopnost mapovat procesy, analyzovat rizika a navrhovat procesní opatření.
   - Pro roli procesního analytika zabývajícího se kybernetickou bezpečností je ideální kombinace certifikací zaměřených na kybernetickou bezpečnost (např. CISM, CISSP), procesní řízení (např. CBPP, ITIL) a řízení rizik (např. CRISC). Tato kombinace zajišťuje, že analytik má nejen technické znalosti, ale i schopnosti mapovat, optimalizovat a řídit procesy v kontextu bezpečnostních požadavků.
   - Zkušenost na uvedené nebo jiné obdobné pozici v posledních 3 letech u minimálně 3 projektů v oblasti informačních technologií, na pozici architekt řešení nebo obdobné pozici související s návrhem enterprise nebo solution architektury informačních systémů, zahrnující analýzu
   - doložení zkušenosti na uvedené nebo jiné obdobné pozici u minimálně 3 projektů v oblasti informačních technologií, na pozici specialista kybernetické bezpečnosti nebo obdobné pozici

související s návrhem nebo implementací opatření v oblasti kybernetické bezpečnosti, zahrnující analýzu rizik a návrhy opatření. Minimální rozsah jednoho projektu ve výši 300 000 Kč bez DPH.

4.4 Doklady o způsobilosti a kvalifikaci

Dodavatel prokáže kvalifikaci dle § 53 odst. 4 ZVZZ. Doklady o kvalifikaci předkládají dodavatelé v nabídkách v kopiích a mohou je nahradit čestným prohlášením (příloha 3 této ZD) nebo jednotným evropským osvědčením pro veřejné zakázky podle § 87 ZZVZ.
Zadavatel si může v průběhu zadávacího řízení dle § 53 odst. 4 ZVZZ vyžádat předložení originálů nebo úředně ověřených kopií dokladů o kvalifikaci. Doklady prokazující základní způsobilost podle §74 ZVZZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem podání nabídky.

4.5 Jiné podmínky účasti

Dodavatel prokáže splnění ustanovení §4b zákona o střetu zájmu čestným prohlášením – viz příloha č.3 ZD.

5. Obchodní nebo jiné smluvní podmínky

Obchodní podmínky jsou staveny v příloze č. 2 této ZD – návrh smlouvy o dílo.

6. Zadávací podklady

Podkladem pro vypracování cenové nabídky je tato ZD a její přílohy. Kompletní ZD je uveřejněna na profilu zadavatele. Žádosti o vysvětlení zadávací dokumentace ze strany dodavatele musí být doručeny přes elektronický nástroj zadavatele. Zadavatel bude postupovat dle ustanovení § 98 ZZVZ. Při změně nebo doplnění zadávací dokumentace bude zadavatel postupovat dle § 99 ZZVZ.

7. Požadavky na jednotný způsob zpracování nabídky

- Nabídka bude zpracována v českém jazyce.
- Nabídka nebude obsahovat přepisy a opravy, které by mohly zadavatele uvést v omyl.
- Zadavatel nepřipouští variantní nabídky.
- Nabídka dodavatele se podávají pouze v elektronické podobě přes https://zakazky.lanskroun.eu/
- Zadavatel přijímá nabídky pouze v elektronické podobě, přes svůj profil zadavatele. Dodavatelé jsou povinni se registrovat na tomto profilu zadavatele: https://zakazky.lanskroun.eu/

8. Struktura podané nabídky

Zadavatel pro přehlednost doporučuje zpracování nabídky v následující struktuře:

Krycí list nabídky

Pro zpracování Krycího listu nabídky dodavatel závazně použije vzor Krycího listu nabídky (tvoří Přílohu č. 1 této ZD) a chybějící požadované údaje do něj doplní. Takto vyplněný Krycí list nabídky podepíše a vloží jako první list do nabídky.
Celková nabídková cena uvedená v Krycím listu bude obsahovat veškeré náklady na splnění zakázky za celou dobu plnění veřejné zakázky. Celková nabídková cena bude stanovena jako cena „**nejvýše přípustná“**,

konečná, a musí obsahovat veškeré náklady na vyhotovení předmětu veřejné zakázky, včetně cestovních výdajů a dalších vedlejších nákladů v celkovém členění bez DPH a s DPH.
Účastník odpovídá za kompletnost poskytovaných činností a je povinen provést i veškeré činnosti, které nejsou výslovně uvedeny a souvisí s předmětem plnění, zahrnout do ceny (zejména nezbytné průzkumy, zaměření apod.). Nabídková cena musí být platná až do celkového dokončení díla.

Doklady prokazující způsobilost a kvalifikaci
Požadavky na prokázání kvalifikace jsou uvedeny v článku 4 ZD.

Návrh Smlouvy
Obchodní podmínky jsou upraveny návrhem smlouvy (příloha č. 2 ZD.) Dodavatel není oprávněn tento návrhy upravovat nad rámec částí označených k doplnění dodavatelem. Dodavatel do nabídky vloží podepsaný návrh smlouvy. Dodavatel doplní ve smlouvě své identifikační údaje v záhlaví smlouvy a dále označená místa. Tento návrh smlouvy podepíše osoba oprávněná jednat jménem či za dodavatele.

9. Místo a doba pro podání nabídek
Lhůta pro podání nabídek končí dnem **16. 12. 2024 v 9.00** hod. Všechny nabídky musí být doručeny zadavateli před skončením lhůty pro podání nabídek. Nabídky se podávají do elektronického nástroje zadavatele (tedy do profilu zadavatele).

10. Otevírání nabídek
Otevírání nabídek není veřejné, protože se nabídky podávají pouze elektronicky.

11. Zrušení zadávacího řízení
Zadavatel je oprávněn zrušit zadávací řízení dle § 127 ZZVZ. Pokud zadavatel toto právo uplatní, může tak učinit i bez uvedení důvodu. Vyzvaným dodavatelům nevzniká vůči zadavateli jakýkoliv nárok.

12. Ekonomická výhodnost nabídky
Zadavatel stanovil, že nabídky budou hodnoceny, dle § 114 odst. 2 ZZVZ, dle nejnižší celkové ceny v Kč bez DPH. Ekonomicky nejvýhodnější bude vybrána nabídka s nejnižší cenou v Kč bez DPH.

13. Rozhodnutí o vyloučení a oznámení o výběru
Zadavatel dle § 53 odst. 5 ZZVZ určuje, že rozhodnutí o vyloučení a oznámení o výběru nejvhodnější nabídky uveřejní na profilu zadavatele. V tomto případě se rozhodnutí o vyloučení a oznámení o výběru bere jako doručené okamžikem uveřejnění na profilu zadavatele.

14. Závěrečná ustanovení
Zadavatel si vyhrazuje právo ověřit informace o dodavateli z veřejně dostupných zdrojů.
Zadavatel nepřiznává dodavateli právo na náhradu nákladů spojených s účastí v zadávacím řízení. Rovněž zadavatel nepožaduje poplatky za to, že se dodavatel může o veřejnou zakázku ucházet.
Dodavatel je v rámci plnění „osobou povinnou spolupůsobit při výkonu finanční kontroly“ ve smyslu §2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů.

Mgr. Radim Vetchý, starosta města

Přílohy:
Příloha č. 1.: Krycí list nabídky
Příloha č. 2.: Návrh smlouvy o dílo
Příloha č. 3.: Čestné prohlášení

Financováno Evropskou unií

NextGenerationEU