DATA SYS

Služby externího konzultanta
Analýza stavu kybernetické bezpečnosti

NABÍDKA

ZADAVATEL
Město Sokolov

DATASYS s.r.o. Jeseniova 2829/20, 130 00 Praha 3, tel.: +420 225 308 111, fax: +420 225 308 110, e-mail: datasys@datasys.cz

Obsah

1. Zákon kybernetické bezpečnosti v kontextu NIS2

Hlavním cílem regulace kybernetické bezpečnosti je dosáhnout toho, aby důležité organizace zaváděly preventivní kroky k posílení své kybernetické bezpečnosti. Tento požadavek, reprezentovaný povinností zavádět tzv. bezpečnostní opatření, je ústředním smyslem existence zákona o kybernetické bezpečnosti, a ne jinak je tomu také v případě existence směrnice NIS2.
NIS2 představuje revidovanou verzi původní směrnice NIS (Network and Information Security) z roku 2016. Nová verze NIS2 výrazně rozšiřuje oblast působnosti platné legislativy a nabízí inovativní přístupy pro posílení a zabezpečení kyberprostoru v Evropě. Do našeho právního řádu se bude adaptovat prostřednictvím zcela nového Zákona o kybernetické bezpečnosti a návazných vyhlášek (předpoklad listopad 2025).
V současné době jsou povinné osoby zákonem o kybernetické bezpečnosti rozděleny do celé řady kategorií. Tyto kategorie mají svá specifika a rozdíly. Návrh zákona stanovuje dva režimy – režim vyšších povinností a režim nižších povinností. Tyto režimy jsou odrazem nového principu tzv. dvourychlostní kybernetické bezpečnosti.
Směrnice NIS2 zdůrazňuje odpovědnost vedení organizací za schválení a zavádění bezpečnostních opatření ke snížení rizik pro kybernetickou bezpečnost. Součástí těchto požadavků je také to, že vedení organizací má povinnost osobně absolvovat školení na téma kybernetické bezpečnosti a podporovat v těchto školeních také své zaměstnance.

2. Předmět nabídky

Tento dokument je nabídkou na provedení analýzy kybernetické bezpečnosti pro Město Sokolov (dále též Objednatel). Analýza bude vedena odborným konzultantem společnosti DATASYS s příslušnou profesní praxí a certifikací (např. CISA nebo Lead Auditor).
Objednateli budou v rámci plnění dle této nabídky poskytnuty služby, jejichž cílem je zjistit a posoudit aktuální stav kybernetické bezpečnosti informačních systémů a IT infrastruktury Objednatele, a to včetně procesů spojených s provozem těchto informačních systémů a infrastruktury. Tj. cílem je posoudit přiměřenost a stav technických i organizačních bezpečnostních kontrol, které jsou pro zajištění ochranu informací zavedeny, a cílem je též doporučit opatření vedoucí ke zlepšení stavu.

Hodnocení stavu kybernetické bezpečnosti bude provedeno ve struktuře dle relevantních požadavků nového zákona o kybernetické bezpečnosti v souladu s NIS2, a jeho doprovodné vyhlášky. Zohledněna bude též doporučení pro systém řízení bezpečnosti informací dle dlouhodobě uznávané normy ČSN ISO 27001 a na ní navazující normy ČSN ISO 27002, která je souborem doporučených opatření pro zajištění bezpečnosti informací.

Z pohledu kritérií pro identifikaci regulované služby, Město Sokolov spadá dle předpokladu pod regulovanou službu **Výkon svěřených pravomocí** v režimu **nižších povinností**.

Povinná osoba má povinnost zavést a provádět bezpečnostní opatření podle příslušné vyhlášky nového zákona o kybernetické bezpečnosti. Pro poskytovatele regulované služby v režimu nižších povinností jsou níže uvedená opatření. Povinná osoba v rámci zajišťování kybernetické bezpečnosti zavede a provádí přiměřená bezpečnostní opatření zohledňující bezpečnostní potřeby organizace.

Bezpečnostní opatření v režimu nižších povinností

1. *Zajišťování minimální úrovně kybernetické bezpečnosti*
2. *Povinnosti vrcholného vedení*
3. *Bezpečnost lidských zdrojů*
4. Řízení kontinuity činností
5. Řízení přístupu
6. Řízení identit a jejich oprávnění
7. *Detekce a zaznamenávání kybernetických bezpečnostních událostí*
8. *Řešení kybernetických bezpečnostních incidentů*
9. Bezpečnost komunikačních sítí
10. Aplikační bezpečnost
11. Kryptografické algoritmy

Analýza bude provedena v následujících krocích:

1. **Prostudování dokumentace**
   Veškerá dostupná dokumentace týkající se kybernetické bezpečnosti v organizaci bude analyzována s cílem získat přehled o současném stavu a identifikovat potenciální oblasti ke zlepšení.
2. **Posouzení stavu, vč. katalogu aktiv**
   Tato fáze zahrnuje rozhovory s odpovědnými osobami (vedoucí IT, administrátoři a další dle vzájemné dohody) s cílem získat relevantní informace o aktuálně zavedených bezpečnostních opatřeních a procesech.
   Součástí je spolupráce na sestavení katalogu aktiv a jejich ohodnocení, včetně posouzení dopadu. V rámci této činnosti proběhne také určení primárních aktiv a jejich garantů, stejně jako určení aktiv podpůrných. Primární aktiva budou popsána formou karet a provázána na příslušná podpůrná aktiva. V první fázi dojde k identifikaci aktiv ve spolupráci se zástupci IT a dle organizačního řádu, následně bude vytvořený koncept aktiv projednán a dopracován společně s garanty aktiv. Identifikace primárních aktiv bude provedena tak, aby bylo možné jednoznačně určit, zda tato aktiva souvisejí s regulovanou službou či nikoliv.
3. **Vypracování závěrečné zprávy**
   Na základě zjištěných informací bude vypracována závěrečná zpráva, která shrne popis aktuálního stavu, identifikované nedostatky z pohledu NIS2/nZKB a zároveň poskytne konkrétní doporučení ke zlepšení kybernetické bezpečnosti v organizaci. Součástí zprávy bude rovněž přehled bezpečnostních opatření zpracovaný ve formě tabulky, v níž budou jednotlivá opatření rozčleněna na zavedená, v procesu a nezavedená.
   Každé opatření bude uvedeno v samostatném řádku tabulky s přiřazeným číslem, popisem, prioritou, aktuálním stavem, plánovaným termínem zavedení a odpovědnou osobou. Tato struktura umožní vedení organizace jasně identifikovat klíčové oblasti pro okamžitou nápravu, efektivně plánovat další kroky a průběžně sledovat plnění povinností vyplývajících z příslušné legislativy a norem kybernetické bezpečnosti.
4. **Revize a úprava bezpečnostní dokumentace**
   Na základě výstupů z analýzy aktuálního stavu a identifikovaných nedostatků bude provedena revize stávající řídicí dokumentace, která zahrne zejména posouzení a aktualizaci bezpečnostní politiky tak, aby v ní byla jasně definována organizační a technická

bezpečnostní opatření v rozsahu odpovídajícím požadavkům kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti.

5. **Závěrečný workshop**
   Prezentace výsledků analýzy a opatření, která bude nutné zavést. Cílem tohoto workshopu bude seznámit vedoucí pracovníky s doporučeními a zajistit pochopení nezbytných kroků pro implementaci opatření vyplývajících z požadavků NIS2/nZKB.

Cílem analýzy je:

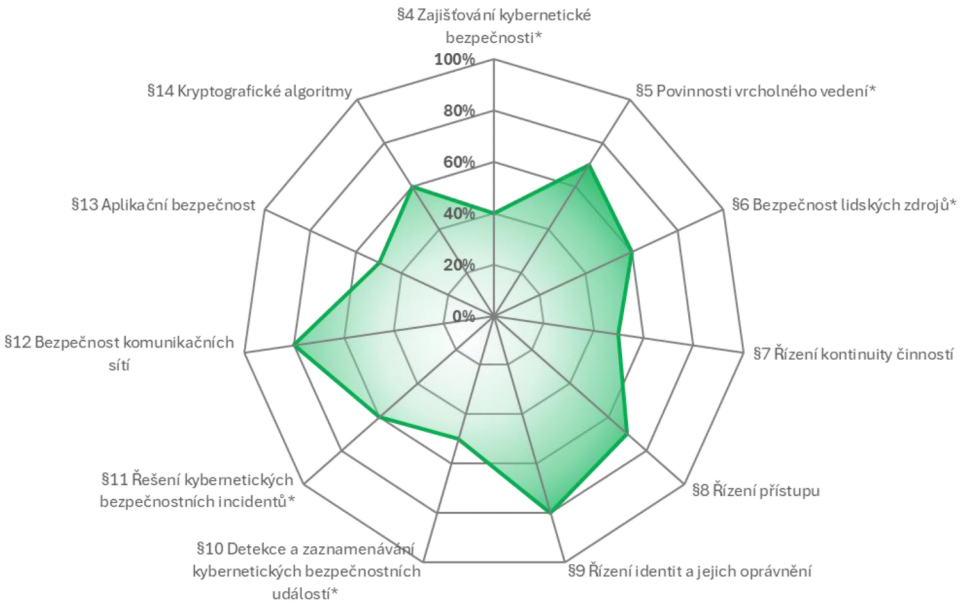
- Zjistit a posoudit aktuální stav a přiměřenost technických/organizačních opatření
- Zhodnotit kvalitu implementace těchto opatření
- Doporučit opatření vedoucí ke zlepšení stavu, vč. odhadu finančních/nefinančních zdrojů
- Poskytnout doporučená opatření pro naplnění souladu s požadavky zákona o kybernetické bezpečnosti v ČR v kontextu NIS2

Analýza bude poskytovat komplexní přehled o stavu kybernetické bezpečnosti Objednatele a bude sloužit jako základ pro další zlepšení a rozvoj bezpečnostních opatření, v souladu s legislativou a dalšími souvisejícími normami.

Výstupem plnění dle této nabídky budou:

- **Úvodní workshop.**
- Dokument **Studie stavu kybernetické bezpečnosti** v kontextu NIS2/nZKB, vč. návrhu doporučených opatření.
- Dokument **Katalog primárních aktiv,** který představuje souhrn veškerých relevantních IT služeb a jejich požadovaných parametrů.
- **Revize/doplnění bezpečnostní dokumentace**.
- **Závěrečný workshop.**

Ukázka zpracování: Přehled úrovně bezpečnostních opatření před zavedením bezpečnostních opatření dle NIS2/nZKB



3. Nabídková cena v Kč bez DPH

Položka	Cena bez DPH
Analýza stavu kybernetické bezpečnosti	150 000 Kč

4. Platnost nabídky, platební podmínky a harmonogram realizace

Platnost nabídky jsou 3 měsíce. DPH činí 21 %. Splatnost faktury vystavené na základě této nabídky je 30 dnů od protokolárního převzetí. Harmonogram realizace bude stanoven po dohodě se Zadavatelem. DATASYS je připraven práce zahájit do 2 týdnů od objednávky.

5. Kvalifikace firmy Datasys

Společnost Datasys svým zákazníkům poskytuje služby v oblasti kybernetické bezpečnosti dlouhodobě. Jedná se zejména o zpracování bezpečnostních studií a rizikových analýz, penetrační testy a technické prověrky.

Rozsahem podobné bezpečnostní studie (výběr):

1. **GAP analýza v rámci projektu kybernetická bezpečnost ICT Městského úřadu Lanškroun**
   Provedení GAP analýzy zahrnující hodnocení procesů, politik a konfigurace informačních systémů, doplněné o návrhy procesních i technických opatření. Posouzení stavu a doporučení vycházely z nového zákona o kybernetické bezpečnosti, který implementuje požadavky směrnice NIS2, a zároveň byly výsledky porovnávány s platnou legislativou v oblasti kybernetické bezpečnosti.

2. **Analýza stavu kybernetické bezpečnosti města Rýmařov, vč. skenu zranitelností, dokumentace a školení**
   Komplexní analýza kybernetické bezpečnosti včetně skenu zranitelností, vypracování potřebné dokumentace, realizace školení uživatelů a zpracování katalogu aktiv. Projekt byl zpracován v souladu s požadavky nového zákona o kybernetické bezpečnosti a zaměřil se na přípravu města k plnění jeho povinností.

3. **Analýza stavu kybernetické bezpečnosti města Orlová, vč. skenu zranitelností a školení**
   Analýza kybernetické bezpečnosti včetně skenu zranitelností a školení garantů aktiv v rámci zpracování katalogu aktiv. Projekt byl proveden s ohledem na požadavky nového zákona o kybernetické bezpečnosti a připravil město na splnění jeho legislativních povinností.

4. **Studie stavu kybernetické bezpečnosti ve společnosti Ostravské komunikace, a.s.**
   Provedení GAP analýzy kybernetické bezpečnosti s cílem identifikovat nedostatky a navrhnout cílový stav v souladu s legislativou a směrnicí NIS2. Součástí bylo testování odolnosti vůči ransomwaru a pokročilým hrozbám, sken zranitelností IT infrastruktury a návrh opatření k jejich odstranění. Výstupem bylo komplexní vyhodnocení bezpečnostní úrovně organizace a doporučení ke zvýšení její odolnosti vůči kybernetickým rizikům.

5. **GAP analýza kybernetické bezpečnosti Zdravotního ústavu se sídlem v Ostravě**
   GAP analýza zahrnující hodnocení procesů, politik a konfigurace informačních systémů, doplněná o návrhy procesních i technických opatření. Posouzení stavu a doporučení vycházely z nového zákona o kybernetické bezpečnosti, který implementuje požadavky směrnice NIS2, a byly zaměřeny na vyšší povinnosti organizace vyplývající z této legislativy.

6. Realizační tým

7. Závěr

Jménem společnosti DATASYS si dovolujeme vyjádřit přesvědčení, že výše uvedená nabídka bude po technické i ekonomické stránce vyhovovat potřebám Vaší organizace a její realizace přispěje ke zkvalitnění prostředí a služeb provozovaných informačních technologií a systémů.
Věříme současně, že náš výklad zadání, navržené postupy, stejně tak jako know-how, technické i lidské zdroje, kterými společnost DATASYS disponuje, skýtají záruky realizace předmětného projektu v nejvyšší kvalitě a k plné spokojenosti Vaší společnosti.

Reference

Hledáte spolehlivého partnera pro své IT?

DATA
SYS