kyberpéče.cz

LEXNOVA

Nabídka od společnosti Lexnova Technology s.r.o.

PROJEKT

Komplexní zhodnocení organizace z pohledu kybernetického zákona a NIS 2 a další navazující služby

KLIENT

Centrum sociálních služeb Děčín, p.o.

DATUM ZPRACOVÁNÍ

5. 11. 2025

1. Obsah

2. Úvod

Společnost **Lexnova Technology s.r.o.** si dovoluje předložit Vám nabídku týkající se rozdílové **analýzy, zhodnocení a návrhu dalšího postupu v oblastech specifikovaných směrnicí NIS 2 a zákonem č. 264/2025 Sb., zákon o kybernetické bezpečnosti (**dále také „kybernetický zákon“**).**

Po seznámení s prostředím klienta obvykle přicházíme s návrhy na optimalizaci IT prostředí a návrhy k jeho rozvoji, aby bylo funkční, uživatelsky přívětivé, bezpečné a nákladově optimální.

Děkujeme Vám za možnost předložit tuto nabídku. Jsme přesvědčeni, že navrhované řešení naplní vaše očekávání.

Název společnosti předkládající nabídku	Lexnova Technology s.r.o.
Sídlo	Na rovnosti 2274/12, Žižkov, 130 00 Praha 3
IČO	22340564
Vypracoval:	Adam Zahradník, MA.
Telefon	+420 604 256 016
E-mail	zahradnik@lexnova.cz
Nabídka vytvořena	5.11.2025
Nabídka platná do	5.12.2025

3. Kdo jsme a co děláme

Ve spolupráci s **Asociací poskytovatelů sociálních služeb České republiky** a společností **IRESOFT s.r.o.** jsme vyvinuli **komplexní, oborově specializované řešení, které je určeno výhradně pro poskytovatele sociálních služeb.**

Informace, metodiku a zkušenosti z realizovaných auditů a implementací budeme systematicky přenášet na další poskytovatele, tak aby bylo možné **zajistit jednotný, efektivní a praktický postup napříč celým sektorem poskytovatelů sociálních služeb**.

Digitalizace a zefektivnění IT sociálních služeb

- Poskytujeme manažerské poradenství zaměřené na zvyšování efektivity a digitalizaci procesů ve vaší organizaci.
- Provádíme detailní analýzy využívaného HW, SW a licenčních podmínek, včetně hodnocení smluv a nákladů.
- Vyhodnocujeme aktuální stav vašeho IT z pohledu poměru **ceny vs. výkonu vs. potřeb organizace** a navrhujeme cílový stav s konkrétním harmonogramem a vyčíslením úspor.
- Připravujeme IT strategie přizpůsobené vašemu zaměření, která minimalizuje plýtvání zdroji a dává vašim technologiím jasný směr i rozpočet.

Outsourcing IT

- Zajistíme pro vaši organizaci manažera kybernetické bezpečnosti, který doplní Váš stávající tým.
- Kompletně se postaráme o fungování vašeho IT – od správy systémů po podporu koncových uživatelů, a to buď přímo na místě, nebo vzdáleně.
- Navrhujeme způsoby, jak zlepšit efektivitu, zabezpečení a rozvoj technologických služeb, abyste měli jistotu stabilního provozu.
- Zajišťujeme správu a monitoring IT infrastruktury včetně zálohování, řešení incidentů a pravidelné údržby systémů.
- Nabízíme End User Support a Service Desk s jasně definovanými standardy služeb (SLA).

Kybernetická bezpečnost

- Chráníme vaši organizaci před kybernetickými hrozbami a sledujeme nejnovější trendy v oblasti bezpečnosti.
- Identifikujeme a odstraňujeme zranitelnosti včetně testování odolnosti vůči útokům, jako je phishing nebo sociální inženýrství.
- Zajišťujeme průběžný monitoring vaší IT infrastruktury a klíčových prvků, od sítě až po aplikace.
- Jsme **vendor agnostic** – navrhujeme řešení, která odpovídají vašim potřebám, nikoli zájmům dodavatelů.

Školení, vzdělávání a workshopy

- Nabízíme školení zaměřená na **IT bezpečnost a gramotnost**, aby vaši zaměstnanci dokázali efektivně a bezpečně pracovat s technologiemi.
- Realizujeme workshopy pro správné využití implementovaných systémů a zlepšení každodenních procesů.
- Poskytujeme specializovaný vzdělávací program zaměřený výhradně na **digitalizaci práce v sociálních službách**. Vzdělávací program probíhá kombinací online workshopů a osobních schůzek a je v rámci České republiky zcela unikátní.
- Pomáháme zajistit financování vzdělávacích aktivit prostřednictvím dotačních programů.

GPDR a ochrana oznamovatelů

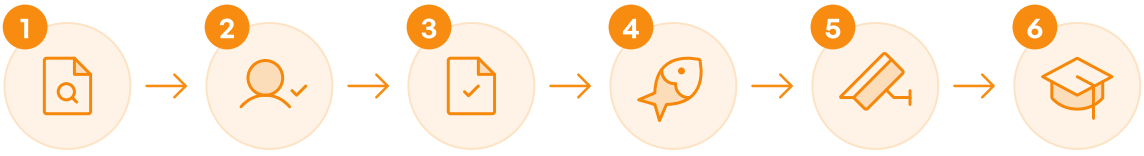
- Nabízíme komplexní řešení v oblasti ochrany osobních údajů (GDPR) a ochrany oznamovatelů. Připravíme pro vás potřebnou dokumentaci, včetně vnitřních předpisů, směrnic a praktických postupů, které zajistí soulad s legislativními požadavky.
- Součástí naší nabídky služeb je také provoz interního oznamovacího systému Oznam.to, který splňuje všechny zákonné náležitosti, je uživatelsky přívětivý a umožňuje bezpečné a anonymní podávání oznámení.

4. Předmět nabídky

Naše nabídka je navržena tak, aby pomohla vaší organizaci posílit kybernetickou bezpečnost, připravit se na legislativní požadavky nového kybernetického zákona a minimalizovat rizika spojená s kybernetickými hrozbami. Nabízíme ucelené řešení obsahující:

- **Phishingovou kampaň**, která odhalí slabiny v povědomí zaměstnanců o kybernetických hrozbách a pomůže zvýšit jejich odolnost vůči podvodným útokům.
- **Audit kybernetické bezpečnosti (Rozdílovou analýzu)**, která vyhodnotí aktuální stav vaší organizace ve vztahu k požadavkům NIS2 a poskytne doporučení pro dosažení souladu.
- **Vypracování chybějící dokumentace**, jež zajistí splnění klíčových legislativních a bezpečnostních požadavků.

Níže naleznete detailní popis jednotlivých služeb, jejich průběh a přínosy pro vaši organizaci. Phishingovou kampaň doporučujeme udělat jako první krok, ještě před auditem kybernetické bezpečnosti. Vaše organizace tak zjistí výchozí pozici, kterou může průběžnými kampaněmi dále sledovat a výsledkům přizpůsobovat vzdělávání zaměstnanců.



Audit kybernetické bezpečnosti → **Manažer KB** → **Vypracování dokumentace** → **Phishingová kampaň** → **Monitoring** → **Školení**

4.1 Phishingová kampaň

Co je phishing a proč vás ohrožuje?
Phishing je druh kybernetického útoku, kdy útočníci posílají podvodné e-maily nebo zprávy, které se tváří jako legitimní. Tyto zprávy často obsahují škodlivé odkazy nebo přílohy a jejich cílem je:

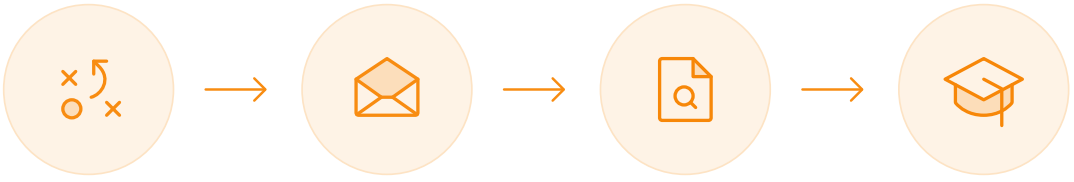
- **Získat přístup k citlivým údajům** – osobní údaje klientů, zdravotní záznamy, finanční informace.
- **Infikovat systémy malwarem** – například ransomwarem, který může ochromit váš provoz.
- **Získat přístup do vašich systémů** – zneužitím přihlašovacích údajů vašich zaměstnanců.

Proč pořádat phishingové kampaně?
Phishingové kampaně, simulované v bezpečném prostředí, vám umožní:

- **Identifikovat slabiny** v povědomí zaměstnanců o kybernetických rizicích.
- **Ověřit reakci vašich zaměstnanců** na podezřelé e-maily a zprávy.
- **Zlepšit celkovou odolnost organizace** vůči reálným útokům.
- **Posílit povědomí a znalosti zaměstnanců** prostřednictvím cíleného školení po skončení simulace.

Takové kampaně jsou klíčovou součástí prevence a pomáhají minimalizovat riziko lidské chyby – jednoho z nejčastějších důvodů úspěchu phishingových útoků.

Průběh phishingové kampaně



Příprava kampaně na míru	Rozeslání simulovaných phishingových e-mailů	Analýza výsledků	Návrh školení a edukace
3 dny	*2 týdny*	*2 dny*	

4.2 Audit kybernetické bezpečnosti (GAP analýza)

Cílem projektu/auditu **je zhodnotit stávající stav v oblasti IT a kybernetické bezpečnosti z pohledu požadavků zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti**.

Výstupem auditu je nejen **jasné pojmenování oblastí, které nejsou v souladu s kybernetickým zákonem**, ale také **pojmenování kroků, opatření a povinností vedoucích ke splnění požadavků na IT infrastrukturu a kybernetické zabezpečení organizace**.

Opatření, která jsou kybernetickým zákonem vyžadována, jsou níže shrnuta do základních oblastí. Těmto oblastem se bude audit věnovat.

Oblast	Cíl
Identifikace dat	Organizace ví, s jakými daty pracuje, jsou identifikovaná a popsaná informační aktiva (data a jejich závislost na software, hardware a službách).
Řízení rizik	Organizace má implementované hodnocení a řízení rizik. Organizace má plán opatření ke snížení rizik a zvýšení kybernetické odolnosti.
Řízená ochrana informací a dat	Organizace má pod kontrolou informace a data, má zajištěnou jejich bezpečnost a ochranu.
Řízení IT a IT bezpečnost	Organizace má zajištěnou bezpečnost software, hardware a IT vybavení. Organizace řídí údržbu, ochranu a monitoring IT infrastruktury.
Řízení dodavatele	Organizace má pod kontrolou nakupované služby a jejich dodavatele a smlouvy s nimi.
Řízení zaměstnanců	Organizace vnímá kybernetickou bezpečnost jako součást HR procesů a vzdělává pracovníky v oblasti bezpečnosti informací.
Řízení incidentů	Organizace má implementovaný nástroj a procesy pro řízení incidentů, tedy hlášení incidentů, i jejich důsledků
Řízení kontinuity provozu	Organizace má implementované řešení pro obnovu provozu IT infrastruktury v případě útoku nebo jiné havárie.
Řízená dokumentace	Organizace má implementovanou směrnici informační bezpečnosti, dodavatelů, IT, a zaměstnanců.
Pravidelný monitoring a kontrola	Organizace má zajištěn systém pro pravidelný monitoring a vyhodnocování funkčnosti výše uvedeného.

Audit bude probíhat v následujících na sebe navazujících krocích:

Celý audit od kroku 1 až po krok 6 trvá v rozmezí 3 – 8 týdnů. V závislosti na velikosti organizace a míře/frekvenci poskytnuté součinnosti.

V rámci nabízené spolupráce navrhujeme postupovat v následujících krocích. Jednotlivé kroky jsou do většího detailu popsány v následujících kapitolách.

4.2.1 Vyžádání dokumentace a podkladů

Pokud nejsou některé z požadovaných vstupů k dispozici, není nutné tyto dokumenty tvořit. Potřebné informace budou získány v rámci workshopů.

a. Organizační / Funkční struktura firmy
b. Seznamu vnitřních řídících dokumentů
c. Seznam formalizovaných procesů ve společnosti a jejich popis, včetně IT procesů
d. Seznam smluvních dodavatelů
e. Seznam využívaných SW pro potřeby řízení firmy a vykonávání regulované služby
f. Architektura SW a HW prostředí v organizaci
g. Recovery plan / plán obnovy
h. Zálohovací postupy
i. Asset Management (správa aktiv)
j. Analýza rizik

4.2.2 Vyplnění elektronického dotazníku

V rámci této etapy klient obdrží **elektronický interaktivní dotazník**, který je rozdělen do dvou částí:

- **Organizační část** – zaměřená na identifikaci klíčových procesů, odpovědností, řízení a dokumentace v oblasti kybernetické bezpečnosti.
- **Technická část** – zaměřená na získání základních informací o používaných IT systémech, infrastruktuře, způsobu správy dat a bezpečnostních opatřeních.

Dotazník je navržen tak, aby efektivně shromáždil důležité vstupní informace o současném stavu kybernetické bezpečnosti organizace. Tyto informace budou následně využity jako podklad pro **online workshopy**, kde budou jednotlivé oblasti dále rozpracovány a doplněny o podrobnosti.

4.2.3 Online workshopy

Workshopy budou probíhat formou **online (případně on-site) strukturovaných rozhovorů** s vybranými vedoucími zaměstnanci a zástupci IT oddělení. Cílem této fáze je získat jasný přehled o aktuálním stavu IT procesů a způsobu, jakým organizace nakládá s daty, informacemi, datovými úložišti a dalšími prostředky manažerského řízení.

V rámci workshopů budou prováděny následující kroky:

a. **Identifikace stakeholderů na straně organizace**

   Určení klíčových osob zapojených do kybernetické bezpečnosti (zástupci IT, vedoucí jednotlivých organizačních útvarů, vrcholové vedení).

b. **Strukturované rozhovory dle klíčových oblastí**

   Rozhovory budou rozděleny podle oblastí definovaných kybernetickým zákonem a doporučeními Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

   Pro každou oblast je připraven **checklist / kontrolní seznam**, který zahrnuje témata vyžadovaná režimem vyšších povinností – např.:

   1. **Organizační opatření**

      a. § 3 Povinná osoba zavede a provádí bezpečnostní opatření

      b. § 4 Systém řízení bezpečnosti informací

      c. § 5 Povinnosti vrcholového vedení

      d. § 6 Bezpečnostní role

      e. § 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace

      f. § 8 Řízení aktiv

      g. § 9 Řízení rizik

h. § 10 Řízení dodavatelů

i. § 11 Bezpečnost lidských zdrojů

j. § 12 Řízení změn

k. § 13 Akvizice, vývoj a údržba

l. § 14 Řízení přístupu

m. § 15 Zvládání kybernetických bezpečnostních událostí a incidentů

n. § 16 Řízení kontinuity činností

o. § 17 Audit kybernetické bezpečnosti

2. Technická opatření

a. § 18 Fyzická bezpečnost

b. § 19 Bezpečnost komunikačních sítí

c. § 20 Správa a ověřování identit

d. § 21 Řízení přístupových oprávnění

e. § 22 Detekce kybernetických bezpečnostních událostí

f. § 23 Zaznamenávání bezpečnostních a relevantních provozních událostí

g. § 24 Vyhodnocování kybernetických bezpečnostních událostí

h. § 25 Aplikační bezpečnost

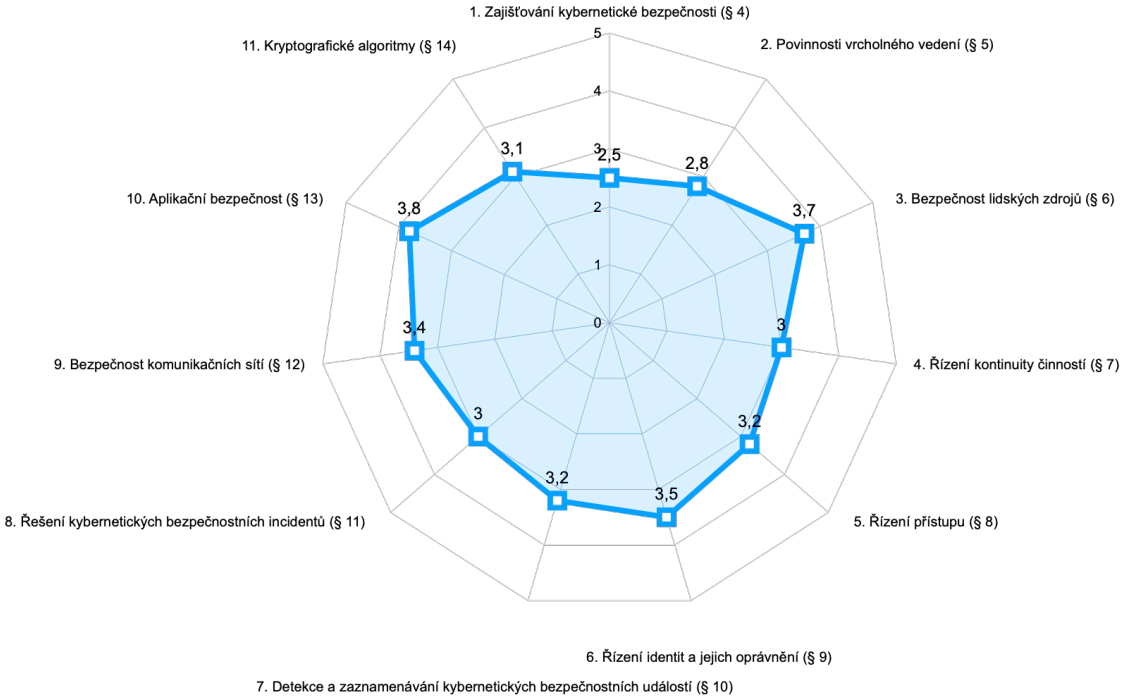
i. § 26 Kryptografické prostředky

j. § 27 Zajišťování dostupnosti regulované služby

k. § 28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

4.2.4 Analýza a zhodnocení stávajícího stavu

V rámci této etapy budou zohledněny získané informace z předchozích kroků. Každý z vyžadovaných paragrafů kybernetického zákona bude ohodnocen nejen slovně, ale také graficky (ilustrativní ukázka níže).



Níže jsou popsány činnosti, které budou realizovány a na jejichž základě budou následně navržena optimalizační opatření.

a. Analýza a popis stávajících procesů a postupů.
b. GAP analýza

   GAP analýza se skládá z následujících kroků

   i. popis stávajícího stavu
   ii. stanovení cílů (popis cílového stavu dle požadavků kybernetického zákona
   iii. určení rozdílu mezi stávajícím a cílovým stavem

GAP analýza se bude věnovat všem oblastem, které jsou vyžadovány kybernetickým zákonem.

4.2.5 Návrh optimalizačních opatření

V rámci této etapy budou identifikována a pojmenována optimalizační opatření, která povedou ke splnění požadavků kybernetického zákona. Opatření budou specifikována pro každou řešenou oblast zvlášť. Níže je popsán postup a obsah návrhové části auditu.

a. Návrh optimálního řešení pro implementaci

   Návrh bude koncipován modulárně – tj. dle jednotlivých auditovaných oblastí.

b. **Identifikace priority či důležitosti dle semaforového principu (zelená, oranžová, červená).**

   Vizuální reprezentace závažnosti / důležitosti / priority zjištění:

Semafor	Barva	Vysvětlení
	**Červená**	Vyžaduje okamžitou pozornost a zásadní zlepšení.
	**Oranžová**	Vyžaduje další zlepšení a rozvoj.
	**Zelená**	Splňuje nebo překračuje požadavky, žádná další akce není nutná.

Pro ilustraci níže uvádíme ukázku zpracování rozdílové analýzy jednoho z požadavků kybernetického zákona (dle § 4 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností).

Nejprve je slovně popsána problematika řešená daným paragrafem, následně je uveden popis stávajícího stavu dané oblasti, které obsahuje jak pozitivní zjištění, tak oblasti, na kterých je potřeba zapracovat.

Následuje popis klíčových zjištění a konkrétní kroky návrhu dalšího postupu.

Tento přístup umožňuje okamžitou orientaci v dané problematice.

Systém zajišťování minimální kybernetické bezpečnosti (§ 4)

Oblast se soustředí na celkový rámec a systematické řízení kybernetické bezpečnosti v organizaci. Hodnotí se, zda jsou nastavena a průběžně prováděna přiměřená opatření, která odpovídají velikosti, povaze a rizikovému profilu organizace. Součástí je existence a aktualizace dokumentace, zavedení procesů pro hodnocení rizik a opatření k jejich minimalizaci. Posuzuje se, zda jsou zavedené politiky a směrnice nejen formálně vydány, ale také prakticky uplatňovány a zda existuje přehled povinných opatření dle vyhlášky.

Popis stávajícího stavu

Organizace zatím neurčila osobu odpovědnou za oblast kybernetické bezpečnosti, a tudíž neexistuje formální řízení této oblasti. Chybí organizační ukotvení a odborná způsobilost této funkce.

Řízení kybernetické bezpečnosti není začleněno do vnitřních struktur a vedení organizace není pravidelně informováno o stavu zabezpečení IT prostředí.

Vedení sice formálně schvaluje interní dokumenty, avšak samostatná bezpečnostní politika či přehled bezpečnostních opatření zpracovány nejsou. Role a odpovědnosti nejsou popsány, evidence aktiv (technických i aplikačních) chybí a smlouvy s IT dodavateli neobsahují bezpečnostní ustanovení.

Celkově organizace zatím přistupuje ke kybernetické bezpečnosti spíše ad-hoc, bez systémového rámce nebo dlouhodobého plánu.

Pozitivní zjištění

- Vedení organizace aktivně schvaluje dostupné dokumenty a projevuje zájem o zavedení systematičtějšího přístupu ke kybernetické bezpečnosti.
- Z provedeného rozhovoru vyplývá, že organizace si uvědomuje potřebu zlepšit tuto oblast a audit iniciovala dobrovolně. To dokládá proaktivní přístup vedení.

Oblasti ke zlepšení

- Neexistuje osoba odpovědná za řízení kybernetické bezpečnosti.
- Chybí organizační ukotvení a odborné zajištění této role.
- Vedení není pravidelně informováno o stavu zabezpečení IT prostředí.
- Není zpracována bezpečnostní politika ani přehled bezpečnostních opatření.
- Role a odpovědnosti nejsou popsány.
- Chybí evidence technických a aplikačních aktiv.
- Smlouvy s IT dodavateli neřeší odpovědnost a povinnosti v oblasti zabezpečení.

Klíčová zjištění

- Organizace nemá formálně nastavený systém řízení kybernetické bezpečnosti ani jmenovanou odpovědnou osobu.
- Základní prvky, jako bezpečnostní politika, přehled opatření či reporting vedení, nejsou zavedeny.
- Vedení přistupuje ke schvalování dokumentů formálně, ale bez obsahu pokrývajícího oblast kybernetické bezpečnosti.
- Současný stav lze považovat za výchozí úroveň, vhodnou k postupnému doplnění o klíčové prvky systému řízení bezpečnosti.

Systém zajišťování minimální kybernetické bezpečnosti (§ 4)

Návrh dalšího postupu	- Určit osobu odpovědnou za koordinaci kybernetické bezpečnosti (interní nebo externí). - Vytvořit jednoduchý dokument „Bezpečnostní politika organizace“, který stanoví cíle, odpovědnosti a základní zásady. - Zpracovat základní přehled aktiv (počítače, cloudové služby, účty, aplikace) a určit, kdo za ně odpovídá. - Zavést pravidelné (např. pololetní) informování vedení o stavu kybernetické bezpečnosti. - Prověřovat smlouvy s dodavateli IT služeb a doplnit ustanovení o povinnostech v oblasti ochrany dat a dostupnosti služeb. - Postupně doplňovat další dokumenty dle potřeb (např. plán řešení incidentů, řízení rizik).
Priorita	STŘEDNÍ
Hodnocení	**2,5**

V závěrečné části auditu je pro manažery organizace připraven harmonogram postupu implementace opatření dle priorit. V harmonogramu jsou pojmenovány všechny implementační kroky.

4.2.6 Seznámení managementu s výsledky auditu

Tento krok slouží k formálnímu odprezentování analytických zjištění, návrhu dalšího postupu a k formálnímu **ukončení** auditu kybernetické bezpečnosti. Součástí auditní zprávy je manažerský souhrn, který pro ředitelku nebo ředitele organizace popisuje klíčové závěry auditu kybernetické bezpečnosti organizace.

5. Návazné služby pro zajištění kybernetické bezpečnosti

Pro další posílení kybernetické bezpečnosti vaší organizace nabízíme doplňkové služby, které rozšiřují hodnotu základní nabídky a umožní vám lépe reagovat na aktuální i budoucí výzvy. Tyto služby jsou navrženy s ohledem na specifické potřeby vaší organizace a přispívají k zajištění komplexní ochrany dat a IT systémů.

Níže naleznete podrobný popis jednotlivých návazných služeb, které si můžete objednat v rámci rozšíření spolupráce. Obrátit se na nás můžete prostřednictvím kontaktních údajů uvedených v sekci 2 - Úvod.

5.1 Vypracování chybějící dokumentace dle kybernetického zákona

Pokud vaše organizace nemá vypracovanou nebo aktualizovanou dokumentaci vyžadovanou kybernetickým zákonem, jsme připraveni vám s jejím zpracováním pomoci. Níže uvádíme seznam klíčových dokumentů, které jsou nezbytné pro prokázání souladu a zajištění kybernetické bezpečnosti v režimu vyšších povinností.

5.2 Manažer kybernetické bezpečnosti

Tato role je vyžadována kybernetickým zákonem. Manažera kybernetické bezpečnosti (dále také „Manažer KB “) vám poskytneme formou služby, která vám umožňuje mít **odborníka na kybernetickou bezpečnost** na dosah ruky, aniž byste museli investovat do plného úvazku. S Manažerem KB budete mít jistotu, že splňujete požadavky kybernetického zákona a zároveň chráníte svou organizaci i klienty.

- **Poradenství v oblasti kybernetické bezpečnosti**
  Pravidelné konzultace a odborná pomoc při řešení konkrétních bezpečnostních otázek, přizpůsobená potřebám vaší organizace. Manažer KB bude na vaše vyžádání spolupracovat s vaším manažerským nebo IT týmem.

- **Podpora při řízení bezpečnostních incidentů**
  Manažer KB je k dispozici pro asistenci při vyhodnocování a řešení bezpečnostních incidentů, včetně návrhu opatření na zmírnění dopadů.

- **Zajištění souladu s požadavky kybernetického zákona**
  Pomoc s dokumentací, implementací a udržováním procesů potřebných pro splnění legislativních požadavků.

- **Hodnocení a řízení rizik**
  Průběžné posuzování rizik v oblasti IT a doporučení kroků ke zlepšení bezpečnostního stavu.

- **Vedení záznamů o kybernetické bezpečnosti**
  Manažer KB zajišťuje správné vedení požadovaných evidencí, jako jsou bezpečnostní incidenty, logy nebo zprávy o shodě.
- **Školení a osvěta zaměstnanců**
  Návrh a koordinace školení zaměstnanců v oblasti kybernetické bezpečnosti pro zvýšení povědomí o hrozbách a prevenci rizik.
- **Pravidelné reporty**
  Poskytování přehledů o bezpečnostním stavu organizace, včetně doporučení pro další kroky.

5.3 Bezpečnostní monitoring

- **Monitorování klíčových systémů a aplikací**
  Průběžný dohled nad chodem vašich IT systémů a aplikací, s cílem odhalit anomálie a potenciální hrozby včas.

- **Detekce a hlášení bezpečnostních incidentů**
  Automatická identifikace podezřelých aktivit, jako jsou pokusy o neoprávněný přístup nebo zneužití zranitelností, a jejich hlášení pro okamžitou reakci.

- **Logování a analýza událostí**
  Centralizované shromažďování a analýza logů z vašich zařízení a systémů pro splnění požadavků na evidenci bezpečnostních událostí dle kybernetického zákona.

- **Průběžné sledování integrity dat**
  Kontrola změn v důležitých souborech a konfiguracích, aby bylo možné rychle identifikovat případné neoprávněné zásahy.

- **Podpora ochrany před malwarem a útoky**
  Detekce a blokování škodlivého softwaru nebo pokusů o útok díky pravidelné aktualizaci databází hrozeb.

- **Zabezpečení přístupů a uživatelských aktivit**
  Sledování, kdo přistupuje k vašim systémům, kdy a s jakými právy, což zajišťuje lepší řízení přístupů.

- **Přehledné reporty a doporučení**

Pravidelné přehledy o bezpečnostním stavu vašich systémů, včetně doporučení na základě identifikovaných hrozeb a zranitelností.

- **Připravenost na audity a plnění legislativních požadavků**
  Nástroj a procesy nastavené tak, aby splňovaly požadavky kybernetického zákona v režimu vyšších povinností

5.4 Vzdělávání zaměstnanců

Nabízíme individuálně sestavené vzdělávací programy zaměřené na témata kybernetické bezpečnosti, počítačové gramotnosti a další oblasti podle potřeb vaší organizace. Obsah školení je přizpůsoben specifikům vašeho provozu a úrovni znalostí zaměstnanců, aby bylo dosaženo maximální efektivity.

- **Možnost výuky přímo ve vaší organizaci** – Lektor přijede na místo a zajistí školení na míru vašemu týmu.
- **Využití aktuálně dostupných dotačních titulů** – Pomůžeme vám zajistit financování vzdělávacích aktivit prostřednictvím vhodných dotačních programů.

Tato služba je klíčová pro zvýšení povědomí zaměstnanců o kybernetických rizicích, zlepšení jejich IT dovedností a celkového zabezpečení vaší organizace.

6. Cenová nabídka

Položka	Cena
Audit kybernetické bezpečnosti (GAP analýza) Režim vyšších povinností dle NIS2	74 990 Kč
Manažer kybernetické bezpečnosti	Dle rozsahu – dle výsledku Auditu Kybernetické bezpečnosti

Další služby popsané v této nabídce budou naceněny až po výsledku Auditu kybernetické bezpečnosti (GAP analýze).

Lexnova Technology s.r.o. ***není plátcem DPH.***