

Jak se připravit na NIS2?

Praktický návod pro sociální služby

kyberpéče.cz



Proč se to týká právě vás?

Kybernetická bezpečnost se nově vztahuje i na poskytovatele sociálních služeb, kteří poskytují zdravotní péči.

Směrnice NIS2 bude v ČR platit od listopadu 2025

V této brožuře vás provedeme krok za krokem tím, co nová pravidla znamenají, koho se týkají a co konkrétně je potřeba udělat.

Najdete zde srozumitelně, jak se **připravit bez zbytečného stresu nebo složité právníčiny**.

Naším cílem je pomoci vám ochránit vaši organizaci, zaměstnance i klienty a zároveň splnit zákonné požadavky, které se na vás začnou vztahovat.

Na tvorbě řešení se podíleli **odborníci ze společností IRESOFT a Lexnova s.r.o.** pod vedením **Miroslava Kvapila**, který se dlouhodobě specializuje na bezpečnost v sociálních a zdravotních službách.

Výsledná koncepce vznikla v úzké spolupráci s **Asociací poskytovatelů sociálních služeb ČR**, aby **byla praktická, srozumitelná a šitá na míru reálným potřebám poskytovatelů**.

Samourčující test: Týká se NIS2 i vás?

Zkuste si odpovědět na následující otázky:



Využíváte při své práci IT systémy?

např. počítače, internet, elektronickou dokumentaci



Máte více než 50 zaměstnanců?



Poskytujete zdravotní péči, včetně odbornosti 913?

ANO

Pokud jste odpověděli všechny otázky **ANO**,
vztahují se na vás nově povinnosti podle směrnice NIS2.

Co je to NIS2 a proč se týká i vás?

Směrnice NIS2 je nový evropský předpis, který zpřísňuje pravidla kybernetické bezpečnosti pro organizace, které zajišťují důležité nebo citlivé služby.

Nově mezi ně patří i **poskytovatelé zdravotní péče**.

V České republice se pravidla NIS2 promítají do zákona č. 264/2025 Sb., o kybernetické bezpečnosti, která výrazně rozšiřuje okruh subjektů, na které se tato povinnost vztahuje.

Už to není jen o nemocnicích nebo velkých IT firmách, nově se jedná i o organizace, které **zaměstnávají 50 a více zaměstnanců a zároveň poskytují zdravotní služby**. V případě poskytovatelů sociálních služeb se bude nejčastěji jednat o služby pod odborností 913 - všeobecná sestra v sociálních službách.



Pokud vaše zařízení poskytuje některou zdravotní službu podle registrace s kódem 911, 913, 916, 917 nebo 925 spadáte pod povinnosti vyplývající z NIS2.

Monitoring systémů

Jedním z požadavků NIS2 je schopnost včas odhalit a reagovat na kybernetické bezpečnostní události. To vyžaduje mít přehled o dění napříč IT prostředím organizace, na počítačích a serverech.

Naše monitorovací aplikace vám tento přehled zajistí:



Přehled o aktuálnosti všech počítačů

Systém hlídá, zda jsou na počítačích a serverech nainstalovány aktuální verze operačního systému a důležitých programů – pomáhá tak předejít zranitelnostem.



Upozornění na podezřelé chování

Systém dokáže rozpoznat, pokud někdo opakovaně zadává špatné heslo, snaží se neoprávněně přihlásit nebo zasahuje do citlivých částí systému.



Kontrola nastavení hesel dle zákonných požadavků

Ověřuje, zda jsou v organizaci nastavena dostatečně silná a dlouhá hesla tak, jak to vyžadují bezpečnostní standardy.



Tvorba přehledných výstupů pro případ incidentu

V případě kybernetického bezpečnostního incidentu systém zaznamená, co se přesně stalo, kdy a kde – což výrazně usnadní jeho nahlášení i řešení.

Požadavek dle vyhlášky (NIS2)

Antivirus
+ Firewall

Naše aplikace
kyberpéče.cz

Ochrana před známým malwarem



Blokování podezřelého síťového provozu



Detekce opakovaných pokusů o přihlášení do OS



Kontrola aktualizací OS a programů



Evidence instalovaného softwaru a zařízení



Logování přístupů a aktivit na koncových zařízeních



Výstrahy při podezřelém chování uživatelů



Upozornění na podezřelé síťové aktivity



Kontrola nastavení složitosti hesel dle doporučení



Přehled o celkovém stavu zabezpečení v organizaci



Vytváření výstupů pro audit a hlášení incidentů



Praktický návod: Co udělat jako první

Nemusíte vědět vše hned. Začněte prvními pěti kroky, které zvládnete i bez složité techniky:

- 1. Udělejte si přehled o svém IT**
Seznamte se s tím, jaké systémy používáte, kdo je spravuje, kde jsou vaše data.
- 2. Stanovte odpovědnou osobu**
Jmenujte někoho, kdo se kybernetickou bezpečností bude zabývat. Může to být i externí specialista.
- 3. Zhodnoťte rizika**
Podívejte se, kde by mohlo dojít k útoku např. slabá hesla, nezabezpečená zařízení, staré systémy.
- 4. Zaveďte základní technická opatření**
Dvoufaktorové přihlašování, pravidelná aktualizace, zálohování – jednoduché věci, které výrazně zvýší bezpečnost.
- 5. Začněte školit zaměstnance**
Nejčastější hrozby přichází e-mailem – proto je zásadní, aby vaši lidé věděli, jak se chovat bezpečně.

Co vám hrozí, pokud nesplníte požadavky NIS2?

Zavedení NIS2 není dobrovolné. Pokud novým povinností nevyhovíte, hrozí vám:



Kolaps provozu

v případě kybernetického útoku může dojít k výpadku systémů, zastavení poskytování péče nebo výrazným provozním ztrátám



Ztráta důvěry kontrolních a financujících institucí

nedodržení povinností může ohrozit získávání dotací, financování či spolupráci s partnery.



Osobní odpovědnost vedení

statutární zástupci ručí za splnění povinností, a to i s možným trestněprávním dopadem.



Vysoké pokuty

až 10 milionů Kč nebo 2 % z ročního obrátu, podle toho, co je vyšší.

Jak vám s tím můžeme pomoci?

Ve spolupráci Lexnova s.r.o. a IRESOFT vám nabízíme praktickou pomoc vytvořenou na míru pro poskytovatele sociálních služeb:



Monitoring systémů

aplikace zajistí přehled o aktuálnosti systémů, sílu hesel, upozornění i reporty.



Školení zaměstnanců i vedení

formou online, prezenčně nebo jako e-learning.



Audit připravenosti

zhodnotíme, co už máte, a co ještě potřebujete udělat.



Podpora při implementaci

poradíme při zavádění opatření i při incidentu.



Vytvoření potřebné dokumentace

směrnice, postupy, určení odpovědností.



Zajištění kontaktní osoby

pomůžeme určit tzv. příslušnou osobu podle zákona.

Reference a spolupráce

Spolupracujeme s Asociací poskytovatelů sociálních služeb ČR (APSS)

připravili jsme pro členy APSS komplexní nabídku služeb na klíč, včetně školení, vzorové dokumentace a přímé podpory pro členské organizace.



Domov pro seniory
Vychodilova

Domov
U Bíříčky

Ceník pro členy APSS

Vyberte si formu spolupráce podle vašich potřeb:

Phishing kampaň 4 990 Kč

Vzdělávání zaměstnanců 4 990 Kč

Audit KB 39 990 Kč

Vypracování dokumentace 29 990 Kč

NEBO 4v1

Komplexní NIS2 balíček
za zvýhodněnou cenou

74 990 Kč

Manažer KB 3 990 Kč / měsíc

Balíček „Kyberpéče“ 9 990 Kč / měsíc

- ✓ Manažer KB
- ✓ Bezpečnostní monitoring
- ✓ Service Desk

% Akce pro členy APSS při
objednání do konce roku 2025

6 990 Kč / měsíc

Ceny jsou platné pro organizace spadající do nižšího režimu povinností.

* V tuto chvíli naše společnost není plátcem DPH, uvedené ceny jsou konečné.

Kontakty

Prvním krokem k NIS2 je audit připravenosti.

Ten vám ukáže, kde máte největší slabiny,
a zároveň nastaví konkrétní opatření v členění podle priorit.
Součástí je i seznam kroků, kterými povinnosti splníte.

*Zájem o audity je vysoký – kontaktujte nás co nejdříve
a získejte nabídku na míru pro vaši organizaci*

pomoc@kyberpece.cz

+420 737 328 987

kyber[~]peče.cz