Unikátní benchmark kyberbezpečnosti 100 zařízení sociálních služeb

XVII. Výroční kongres poskytovatelů sociálních služeb

kyberpéče.cz



Kde se dnes nacházíte?

1. Legislativu už známe

- Mnozí poskytovatelé sociálních služeb nově spadají pod regulovanou službu 18.1. – Poskytování zdravotní péče
- Zákon č. 264/2025 Sb. a vyhláška č. 410/2025 Sb. stanoví režim nižších povinností.

2. Audit máte na stole

- Mnoho organizací v tomto sále již s námi prošla rozdílovou GAP analýzou.
- Máte v rukou své individuální výstupy a konkrétní zjištění.
- Studie vznikla agregací právě těchto vašich reálných dat z praxe.

3. Od diagnózy k řešení

- Audit nebyl cílem, ale rentgenem stavu vaší IT infrastruktury a procesů.
- Dnes se podíváme na to, co výsledky znamenají pro strategické řízení ředitele.
- Cílem je přejít od obav ze sankcí k věcnému, klidnému a postupnému plánu.

HLAVNÍ POSELSTVÍ DNEŠNÍ PREZENTACE:

Výsledky, které vám v auditu svítily oranžově, nejsou vaše osobní selhání. Je to přirozený stav celého odvětví v ČR.

Unikátní vzorek: 100 organizací

Poskytovatelé sociálních služeb v režimu nižších povinností

100

Auditovaných organizací sociálních služeb v ČR

11

Hodnocených oblastí vyhlášky č. 410/2025 Sb.

Rozděleno do 2 pilířů: Organizační opatření a Technická opatření

Metodika hodnocení (Semafor)

Hodnocení od 0 do 5 bodů, kde známka 5,0 představuje plný soulad s požadavky vyhlášky.

Červené pásmo (< 2,0 bodu):
Kritický nesoulad s požadavky vyhlášky.

Oranžové pásmo (2,0 – 3,9 bodu):
Stav vyžadující zlepšení, opatření jsou zavedena jen částečně.

Zelené pásmo (≥ 4,0 bodu):
Vyhovující stav v souladu se standardem vyhlášky.

kyberpéče.cz

Výsledky benchmarku 100 zařízení

Průměrná známka sektoru: 3,0 z 5

(Oranžové pásmo)

2 %

Červené pásmo (Kritický nesoulad)

2 organizace ze 100

97 %

Oranžové pásmo (Částečný soulad)

97 organizací ze 100

1 %

Zelené pásmo (Soulad)

Pouze 1 organizace ze 100

Technický pilíř: 3,1 z 5

Počítače fungují, antiviry běží, 89 % zařízení používá cloudový software (např. Cygnus).

Technika je hodnocena lépe u 81 % organizací.

Organizační pilíř: 2,8 z 5

Kámen úrazu: chybí určené role (OZKB), směrnice, plány obnovy, postupy pro incidenty a smluvní garance dodavatelů IT.

ZÁSADNÍ ZJIŠTĚNÍ:

Známku 5,0 (plné splnění standardu vyhlášky) nedosáhla ani jedna organizace v žádné z 11 oblastí.

kyberpece.cz

Tři systémové bolesti, které jste našli ve svých zprávách

1. Hesla a přístupy

- **49 % organizací má sdílené účty** na sesternách (účet sestra1@...)
- **Jen 3 % zařízení má zavedené dvoufázové ověření** (MFA) v mobilu
- **0 % organizací splňuje minimální délku hesel** dle vyhlášky

Právní důsledek: Při úniku dat či přepsání medikace nelze prokázat, kdo záznam změnil. Nulová auditní stopa.

2. Zálohy a Plán B

- **62 % organizací nemá** žádný plán kontinuity a obnovy péče
- **57 % organizací** nikdy nezkusilo obnovit data ze zálohy
- **Zálohy na síti:** často na stejném disku jako provozní data (snadný cíl pro ransomware)

Zlaté pravidlo: Neotestovaná záloha v kyberbezpečnosti neexistuje.

3. Externí IT správci

- **89 % zařízení** spoléhá na externího správce IT či firmu
- **51 %** organizací nemá žádné bezpečnostní ujednání ve smlouvě
- **Nulové SLA:** ředitel neví, do kolika hodin IT garantuje zásah a obnovu

Osobní riziko: Statutár nese plnou odpovědnost, pokud dodavatel selže a nemá smlouvu.

Dobrá zpráva ze studie:
Řešení není v nákupu drahého IT

Co vám nabízejí IT vendoři

- Nová serverovna a hardware za 800 000+ Kč
- Bezpečnostní dohledové centrum (SOC) za 40 000 Kč měsíčně
- Manažer kybernetické bezpečnosti (CISO) na plný úvazek
- Složitý korporátní/enterprise software s drahými licencemi

Co skutečně žádá vyhláška č. 410/2025 Sb.

- **Zapnout dvoufázové ověření (MFA) v cloudu, který už platíte**
- **Zrušit sdílené účty – alespoň každá sestra vlastní účet (ideálně všichni zaměstnanci)**
- **Vyzkoušet obnovu z provedených záloh**
- **Papírový scénář nouzového provozu (desky na oddělení)**
- **Školit zaměstnance na základy KB**
- **Pověřit odpovědnou osobu (OZKB) interně či externě**

80 % nápravných kroků tvoří organizační opatření s nulovými nebo minimálními náklady.

kyberpéče.cz

Role statutára: Co se od vás jako ředitele čeká (a co není vaše práce)

Co není vaší rolí?

- Rozumět technickým kódům a síťovým portům
- Konfigurovat firewall, switche nebo servery
- Dělat IT mikromanagement sester a pečovatelek
- Osobně vyšetřovat technické příčiny incidentů
- Trávit hodiny čtením technických manuálů

Co je vaší rolí? (Péče hospodáře)

1. **Určit odpovědnost:** Jmenovat Osobu pověřenou KB (OZKB).
2. **Stanovit priority obnovy:** Rozhodnout, co musí běžet první (léky a záznamy do 4 h, účetnictví počká).
3. **Schválit "Přehled opatření":** Podepsat seznam zavedených a plánovaných kroků – tím kryjete sebe i organizaci.
4. **Smluvně zavázat IT:** Chtít do smluv se správci garanci reakční doby a obnovy dat (SLA).
5. **Absolvovat školení:** Prokazatelně projít školením pro vedoucí pracovníky.

ZLATÉ PRAVIDLO: Ředitel neřídí techniku. Ředitel řídí lidi, pravidla, smlouvy a priority.

Shrnutí na závěr

1. To nejtěžší máte za sebou

Audit máte hotový a znáte svou diagnózu. Většina ostatních subjektů v ČR ani netuší, kde jim do lodi teče – vy máte přesnou mapu.

2. Vyhláška dává časový prostor

Zákonná lhůta je 1 rok od registrace. NÚKIB neposílá přepadová komanda ani nerozdává pokuty za to, že nejste stoprocentní hned.

3. Přehled opatření je váš štít

Pokud máte podepsaný plán postupné nápravy, prokazujete aktivní péči řádného hospodáře. Před kontrolou jste plně obhajitelní.

4. Základy řádné digitální hygieny

Studie ukázala, že naprostá většina bezpečnostních opatření nejsou žádné drahé technologie, ale praktické nastavení základních postupů. Jedná se vlastně o nastavení základů řádné digitální hygieny.

Děkuji za pozornost!

pomoc@kyberpece.cz

+420 721 200 445

Adam Zahradník, MA.

zahradnik@lexnova.cz

kyberpéče.cz