# specifikace – Část 8 – Analytické práce v oblasti kyberbezpečnosti

Obsah

[Popis požadavků na činnost auditora a konkrétní zohledněné aspekty auditu 3](#_Toc197348836)

[rozsah auditu kybernetické bezpečnosti 3](#_Toc197348837)

# Popis požadavků na činnost auditora a konkrétní zohledněné aspekty auditu

Audit připravenosti společnosti pro plnění požadavků zákona o kybernetické bezpečnosti 181/2014 Sb., a na něj navazující vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti bude provedena v souladu s dokumentem „Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.“, vydaným Národním úřadem pro kybernetickou a informační bezpečnost (NUKIB).

Tento dokument bude využit jen jako pomocný, vlastní audit bude porovnávat stav Nemocnice vůči vyhlášce č. 82/2018 Sb., popřípadě norem řady ISO 27000, kde existuje převodní tabulka mezi jednotlivými bezpečnostními opatřeními z přílohy A, normy ISO 27001 a jednotlivými paragrafy vyhlášky.

Vlastní provedení bude sestávat z několika na sebe navazujících kroků:

* Prvním krokem bude studium dostupné dokumentace se vztahem k IT a IT bezpečnosti.
* Dalším krokem bude zjišťování nedokumentovaných bezpečnostních opatření. Tyto budou upřesněny formou řízených rozhovorů s odpovědnými zaměstnanci společnosti. Při tomto zjišťování stavu budeme předpokládat, že získané informace jsou pravdivé a nebudeme kontrolovat tyto informace v nastavení na technologických prvcích.

## rozsah auditu kybernetické bezpečnosti

1. **Posouzení stavu organizačních opatření**
2. Systém řízení bezpečnosti informací
3. Povinnosti vrcholového vedení
4. Bezpečnostní role
5. Řízení bezpečnostní politiky a dokumentace
6. Řízení aktiv
7. Řízení rizik
8. Řízení dodavatelů
9. Bezpečnost lidských zdrojů
10. Řízení změn
11. Akvizice, vývoj a údržba
12. Řízeni přístupu
13. Zvládání kybernetických bezpečnostních událostí a incidentů
14. Řízení kontinuity činností
15. Audit kybernetické bezpečnosti
16. **Posouzení stavu technických opatření**
17. Fyzická bezpečnost
18. Bezpečnost komunikačních sítí
19. Správa a ověřování identit
20. Řízení přístupových oprávnění
21. Detekce kybernetických bezpečnostních událostí
22. Zaznamenávání událostí
23. Vyhodnocování kybernetických bezpečnostních událostí
24. Aplikační bezpečnost
25. Kryptografické algoritmy
26. Zajištěni dostupnosti regulované služby
27. Zabezpečení průmyslových, řídících a obdobných specifických technických aktiv
28. **Návrh opatření pro zabezpečení shody s požadavky NIS2/ZoKB Nápravná opatření**
29. Návrh řešení nápravného opatření
30. Odhad finančních nákladů/pracnosti
31. Odhad nároků na interní lidské zdroje
32. Odhad doby implementace NO nebo harmonogram pravidelných činností v rámci NO
33. **zpracování zprávy auditu** – touto zprávou budou popsána bezpečnostní opatření, která jsou ve společnosti již implementována, opatření, která budou vyžadovat jen drobné úpravy a opatření, která ve společnosti implementovány nejsou a jsou vyžadována zákonem č. 181/2014 Sb., a vyhláškou 82/2018 Sb. Zpráva bude obsahovat jak manažerský přehled, tak i detailní zprávu určenou pro manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti.