10.13 Systém řízení informační bezpečnosti

Tento dokument popisuje opatření, která MUSÍ, nebo BY MĚLA být implementována pro

- **Cíle, principy a potřeby řízení informační bezpečnosti.**
- **Rozsah a hranice systému řízení bezpečnosti informací.**
- **Pravidla a postupy pro řízení dokumentace**
- **Pravidla a postupy pro řízení zdrojů a provozu systému řízení informační bezpečnosti.**
- **Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.**
- **Pravidla a postupy pro přezkoumání systému řízení informační bezpečnosti.**
- **Pravidla a postupy pro nápravná opatření a zlepšování systému řízení informační bezpečnosti.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Systém řízení bezpečnosti informací (§ 3).

1 Cíle, principy a potřeby řízení informační bezpečnosti

Cíl: Cílem je efektivní a účinné řízení informační a kybernetické bezpečnosti (KB).

1.1 Cíle

Společnost MUSÍ stanovit cíle systému řízení informační bezpečnosti (IB).

1.2 Principy

Společnost MUSÍ stanovit principy systému řízení informací postavené na modelu PDCA (průběžného a neustálého zlepšování).

1.3 Potřeby

Společnost MUSÍ systémem řízení IB chránit vlastní aktiva.

2 Rozsah a hranice

Cíl: Stanovení rozsahu a hranic systému řízení informační a kybernetické bezpečnosti a dle cílů zavést adekvátní bezpečnostní opatření.

2.1 Rozsah

Společnost MUSÍ stanovit rozsah s ohledem na požadavky dotčených stran a aktiv.

2.2 Hranice

Společnost MUSÍ definovat hranice dotčených organizačních a technických aktiv.

2.3 Návaznosti

Společnost MUSÍ řídit rizika dle stanovené metodiky a kritérií pro akceptovatelnost rizik. Společnost MUSÍ identifikovat a následně řídit významné změny. Společnost MUSÍ zajistit pravidelné vyhodnocování účinnosti systému řízení IB a KB.

3 Řízení bezpečnostní dokumentace

Cíl: Zajistit pravidla a postupy spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

Implementační pokyny:

3.1.1 Společnost MUSÍ stanovit, přezkoumat a schválit bezpečnostní politiku dle vyhlášky o kybernetické bezpečnosti (VKB).

3.1.2 Společnost MUSÍ definovat dílčí politiky jako bezpečnostní zásady dle struktury VKB.

3.2 Bezpečnostní směrnice

Společnost MUSÍ zajistit bezpečnostní úroveň směrnic pro realizaci bezpečnostních politik včetně schválení Výborem pro kybernetickou bezpečnost.

Implementační pokyny:

3.2.1 Vypracování souboru bezpečnostních směrnic na základě, kterých budou vypracovány/doplněny provozní manuály pro jednotlivá aktiva.

3.2.2 Seznam bezpečnostních směrnic MUSÍ korespondovat minimálně s bezpečnostními politikami dle VKB.

3.3 Bezpečnostní dokumentace

Společnost MUSÍ dodržet strukturu bezpečnostní dokumentace dle VKB.

Implementační pokyny:

3.3.1 Obsah bezpečnostní dokumentace:

- Zpráva z auditu KB
- Zpráva z přezkoumání systému řízení IB a KB
- Metodika pro identifikaci a hodnocení aktiv a rizik
- Zpráva o hodnocení aktiv a rizik
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik
- Plán rozvoje bezpečnostního povědomí

- Evidence změn
- Hlášené kontaktní údaje
- Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

3.3.2 Doporučená dokumentace:

- Topologie infrastruktury
- Přehled síťových zařízení

4 Řízení zdrojů a provozu systému řízení informační bezpečnosti

Cíl: Závazek vedení společnosti na zajištění nezbytných zdrojů pro řízení bezpečnosti informací.

4.1 Personální zabezpečení

Společnost MUSÍ určit povinné osoby dle VKB.

Implementační pokyny:

4.1.1 Společnost MUSÍ určit:

- Manažera kybernetické bezpečnosti
- Architekta kybernetické bezpečnosti
- Garanty aktiv
- Auditora kybernetické bezpečnosti
- Vytvořit výbor pro řízení kybernetické bezpečnosti, jehož členem je alespoň jeden zástupce vrcholového vedení a Manažer kybernetické bezpečnosti

4.2 Technické zabezpečení

Společnost MUSÍ zajistit zdroje a podporu pro naplnění cílů řízení informační a kybernetické bezpečnosti.

Implementační pokyny:

4.2.1 Společnost MUSÍ realizovat:

- Zajištění integrace systému řízení bezpečnosti informací do procesů společnosti
- Zajištění dostupnosti zdrojů potřebných pro řízení IB a KB
- Zajištění podpory k dosažení zamýšlených výstupů systému řízení IB a KB
- Podpora osob zastávajících bezpečnostní role v oblastech jejich odpovědnosti
- Zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů
- Informuje zaměstnance o významu systému řízení BI a významu dosažení shody s jeho požadavky a všemi dotčenými stranami
- Zajištění mlčenlivosti administrátorů a osob zastávajících bezpečnostní role
- Zajištění příslušných pravomocí a zdrojů pro naplnění bezpečnostních rolí a plnění souvisejících úkolů
- Zajištění školení a vzdělávání zaměstnanců v dosažení zamýšlených výstupů systému řízení IB a KB

5 Audit kybernetické bezpečnosti

Cíl: Zabezpečit nezávislý interní audit plně v souladu s VKB.

5.1 Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

Společnost MUSÍ zajistit pravidelné interní audity (vnitřně nebo dodavatelský).

Implementační pokyny:

5.1.1 Společnost MUSÍ určit Auditora kybernetické bezpečnosti, který vyhovuje podmínkám VKB.

5.1.2 Společnost MUSÍ posoudit zjištěné rozdíly a nedostatky včetně potenciálních oblastí ke zlepšení.

5.1.3 Posoudit MUSÍ zejména:

- soulad s právními předpisy,
- soulad s jinými předpisy a smluvními závazky, které se vztahují k informačnímu a komunikačnímu systému,
- soulad s bezpečnostní dokumentací a bezpečnostními politikami společnosti,
- účinnost systému řízení bezpečnosti informací podle vyhlášky o kybernetické bezpečnosti.

5.1.4 Plánování auditu – pravidelný audit MUSÍ být proveden minimálně 1x za 2 roky a v případě významné změny či incidentu, které mohou mít negativní dopad na KB.

5.1.5 Zpráva z interního auditu MUSÍ vycházet z auditních zjištění podložených důkazy.

5.1.6 Klasifikace auditních zjištění:

- shoda (bez zjištění), lze uvést doporučení, upozornit na potenciál pro zlepšení
- neshoda (čí více neshod) - nesplnění požadavku dle stanovených kritérií (nejsou naplněny zákonné požadavky, ustanovení vnitřních předpisů nejsou plněna,…),
- potenciální riziko (pozorování) - typ zjištění, kdy auditor upozorňuje na možné riziko.

5.1.7 V případě zjištění typu neshoda jsou součástí zprávy **návrhy nápravných opatření**.

6 Přezkoumání systému řízení informační bezpečnosti

Cíl: Zabezpečit přezkoumání systému řízení IB a KB plně v souladu s VKB a s dodržením principů auditu.

6.1 Pravidla a postupy při přezkoumání systému řízení IB

Společnost MUSÍ stanovit potřebná pravidla pro přezkoumání systému řízení IB. Implementační pokyny:

6.1.1 MUSÍ být vyhodnoceny informace z předchozího přezkoumání.

6.1.2 MUSÍ být identifikovány změny a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.

- Zpětná vazba o výkonnosti řízení bezpečnosti informací
  1. neshody a nápravná opatření,
  2. výsledky monitorování a měření,
  3. výsledky auditu,
  4. naplnění cílů bezpečnosti,

6.1.3 MUSÍ být hodnoceny rizika a stav plánu zvládání rizik.

6.1.4 MUSÍ být identifikovány možnosti pro neustálé zlepšování.

6.1.5 MUSÍ být doporučena potřebná rozhodnutí, stanovena opatření a odpovědné osoby.

7 Nápravná opatření

Cíl: V případě zjištění neshody MUSÍ být po schválení Zprávy z interního auditu navržen a schválen auditovanou osobou harmonogram nápravných opatření.

Použité zdroje

(1) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(2) *MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD* [online]. Verze 1.0. NÚKIB, 2020 [cit. 2022-04-20]. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)