Vademecum ISMM aneb možný postup vytvoření příručky systému řízení bezpečnosti informací

1. Rozsah a odpovědnosti

- Jmenujte „odpovědného manažera“, tedy osobu odpovědnou za systém řízení informační bezpečnosti (ISMS). V malé společnosti to může být někdo ze stávajících jmenovaných manažerů za předpokladu, že má potřebné kompetence a zdroje.
- Definujte, které systémy a údaje ISMS zahrnuje; zaměřte se především na ty s dopadem na bezpečnost letectví. Není nutné zahrnout do systému každý kancelářský počítač na stejné úrovni zabezpečení – ale pouze ta zařízení, která by v případě ohrožení mohla ovlivnit bezpečnost letového provozu, údržby nebo navigace.
- Uveďte prohlášení o bezpečnosti, podepsané odpovědným vedoucím, které bude obsahovat závazek organizace zachovávat bezpečnost informací a dodržovat soulad s N 2023/203 a vlastním ISMM [detaily IS.I.OR.250 (a) (1)].
- Uveďte organizační schéma, zejména s ohledem na to kdo navrhuje architekturu kybernetické bezpečnosti, kdo navrhuje a zavádí pravidla používání IT systémů, kdo prosazuje a kontroluje dodržování těchto pravidel, a kdo vypracovává plány obnovy dat/systémů (případně kde a jak plány obnovy publikuje). Zohledněte velikost organizace a skutečný počet zařízení, která spadají do ISMS; a zohledněte také to, zda a jak vaše organizace IT služby outsourcuje.

2. Řízení rizik (jádro příručky)

V příručce popište postupy pro:

- Identifikaci aktiv (majetku): soupis kritických systémů informačních a komunikačních technologií (ICT), jako jsou např. software pro plánování letů, databáze údržby, EFB zařízení atp.
- Vyhodnocení rizik (IS.I.OR.205): popište metody identifikace hrozeb (např. phishing, malware) a zranitelnosti. K posouzení vlivu na bezpečnost letectví použijte jednoduchou matici 3x3 nebo 5x5 (příklad takové tabulky najdete v GM1 IS.I.OR.205(c) nebo v již zavedeném SMS).
- Řízení rizik (IS.I.OR.210): Dokumentujte řídící prvky, které máte k dispozici nebo je zavádíte (např. silná hesla, pravidelné zálohování, vícefaktorové ověřování [MFA], pravidelné aktualizace softwaru), abyste rizika snížili na přijatelnou úroveň.

3. Schémata hlášení událostí

Připravte jasné, jednoduché postupy pro:

- Interní hlášení (IS.I.OR.215): Jak zaměstnanci hlásí „bezpečnostní událost“ (např. „*Kliknul jsem na podezřelý odkaz*“ nebo „*Ztratil jsem firemní notebook/tablet*“). Ideálně vytvořte jednoduchý formulář nebo zadejte e-mailovou adresu; vyjděte z již zavedeného SMS.
- Externí hlášení (IS.I.OR.230): Použijte postupy pro hlášení událostí příslušnému národnímu úřadu, v tomto případě události v oblasti bezpečnosti informací, která ***může mít dopad na bezpečnost letectví*** (nezapomeňte na lhůtu 72 hodin pro podání hlášení).

4. Správa incidentů

Popište, jak budete reagovat, když se něco pokazí:

- Detekce: Jak například zjistíte, že vás někdo „hacknul“? (antivirové výstrahy, výpadky systému, nesoulad údajů atp.).
- Řešení & Obnova/zotavení (IS.I.OR.220), neboli plán obnovy: Kdo co dělá? Jak obnovujete systémy ze záloh? Jak zajistíte, že během obnovy dat nebude ohrožena bezpečnost? (Znovu s ohledem na velikost organizace a rozsah systému; malému týmu stačí jednoduchý scénář [tzv. „playbook“] či dokonce jen soubor checklistů s jasně stanoveným postupem).

5. Auditování, školení a neustálé zlepšování

- Popište, jak školíte personál; zohledněte přitom velikost organizace (pro malou firmu by mohly stačit pravidelné a krátké bezpečnostní briefingy nebo newslettery). Nezapomeňte popsat způsob, jak záznamy o školení dokladujete.
- Zahrňte ISMS do stávajícího plánu interních auditů organizace.
- Přezkum řízení: Odpovědný manažer by měl ISMS přezkoumat alespoň jednou ročně. V malé organizaci lze ideálně spojit s vyhodnocením SMS.

Doporučený obsah ISMM (zjednodušený, podrobně viz IS.I.OR.250)

1. Úvod a politika: Účel, rozsah a závazek odpovědného manažera.
2. Organizace a odpovědnost: Kdo je odpovědný za informační bezpečnost?
3. Systém řízení informační bezpečnosti: Seznam kritických systémů a externích rozhraní (dodavatelé/partneři).
4. Rámec pro řízení rizik: Jak hodnotíte rizika a zacházíte s nimi.
5. Provozní postupy:
    - Řízení přístupu (hesla/MFA);
    - Správa aktualizací softwaru/oprav;
    - Malware Protection;
    - Fyzická bezpečnost serverů/zařízení.
6. Hlášení a reakce na incidenty: Vnitřní a vnější toky hlášení o událostech.
7. Školení a povědomí: Záznamy o školení zaměstnanců.
8. Sledování shody s předpisy: Jak zkontrolujete, zda systém funguje.

Pro-tipy pro malé firmy:

• Nezačínejte od nuly: Pokud již máte příručku pro řízení bezpečnosti (SMM) nebo příručku organizace údržby (MOE), můžete ISMS přidat jako vyhrazenou kapitolu nebo samostatný dodatek, který odkazuje na již zavedené postupy auditů a hlášení.

Obecně doporučujeme – alespoň v úvodní fázi – zpracovat ISMM jako samostatný dokument, na který uvedete odkaz v MOE, kapitola 3.23

• Zachovejte zásadu proporcionality: vytvořte a udržte systém „úměrný velikosti a složitosti“ organizace. Pokud máte jen pět zaměstnanců, měl by být váš manuál výstižným pracovním nástrojem, nikoli 200stránkovým akademickým textem.

• Lhůta: Nezapomeňte, že pro většinu organizací je nejzazší termín pro plný soulad s nařízením č. 2023/203 22. únor 2026.