Příloha SML03 - Práva a povinnosti manažera a architekta kybernetické bezpečnosti IS DMVS

č. sml. Objednatele: ČÚZK-20194/2021

1. Úvod

Práva a povinnosti manažera a architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají VIS IS DMVS.

2. Práva a povinnosti manažera kybernetické bezpečnosti

Manažer kybernetické bezpečnosti IS zajišťuje systém řízení bezpečnosti informací pro daný IS a odpovídá se manažeru kybernetické bezpečnosti Objednatele.

2.1 Povinnosti manažera kybernetické bezpečnosti:

- musí mít znalost ZoKB a jeho prováděcích vyhlášek,
- hlásí neprodleně manažerovi kybernetické bezpečnosti Objednatele kybernetické bezpečnostní incidenty IS a vede jejich evidenci,
- připravuje pro manažera kybernetické bezpečnosti Objednatele podklady pro NÚKIB,
- připravuje za IS pro manažera kybernetické bezpečnosti Objednatele podklady pro jednání Výboru pro řízení kybernetické bezpečnosti,
- zajišťuje poskytnutí podkladů a návrhů řešení pro zajištění odstranění nedostatků, zjištěných při kontrolách NÚKIB,
- zajišťuje podklady a návrhy řešení pro provedení reaktivních opatření,
- poskytuje součinnost auditorovi kybernetické bezpečnosti a auditorům Objednatele při provádění auditů a kontrol,
- vyhodnocuje a klasifikuje kybernetický bezpečnostní incident,
- klasifikuje, prošetřuje a určuje příčiny kybernetického bezpečnostního incidentu, vyhodnocuje účinnost preventivních a reaktivních opatření aplikovaných proti kybernetickému bezpečnostnímu incidentu,
- zajišťuje podklady k dokumentaci zvládání kybernetických bezpečnostních incidentů,
- navrhuje úpravy bezpečnostní dokumentace na základě zjištění z auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami v IS,
- zajišťuje pravidelné provedení analýzy rizik a hodnocení aktiv,
- aktualizuje dokument *„Plán zvládání rizik“* na základě výstupů analýzy rizik,
- provádí aktualizaci dokumentu *„Zpráva o hodnocení aktiv a rizik“*, *„Plán zvládání rizik“*, a to nejméně jednou za 3 roky, nebo v souvislosti s prováděnými nebo plánovanými změnami významně ovlivňujícími bezpečnost informací,
- zpracovává ve spolupráci s architektem kybernetické bezpečnosti IS a garantem aktiv IS aktualizaci dokumentu *„Prohlášení o aplikovatelnosti“*,
- připravuje podklady do dokumentu *„Zpráva z přezkoumání systému řízení bezpečnosti informací“* a předkládá je manažerovi kybernetické bezpečnosti Objednatele,
- zajišťuje ve spolupráci s garantem aktiv implementaci schválených bezpečnostních opatření a na vyžádání zajišťuje jejich audit,
- zohledňuje, do měsíce od informování manažerem kybernetické bezpečnosti Objednatele, reaktivní a ochranná opatření vydaná NBÚ (nyní NÚKIB) v dokumentu *„Zpráva o hodnocení aktiv a rizik“* a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplní dokument *„Plán zvládání rizik“*. Splnění oznámí manažerovi kybernetické bezpečnosti Objednatele,

- stanovuje provozní pravidla a postupy k zajištění bezpečného provozu IS, v dokumentu *„Politika řízení provozu a komunikací“*,
- zajišťuje kontrolu přidělování jednoznačného identifikátoru uživatelům IS,
- stanovuje bezpečnostní požadavky na změny IS spojené s jeho akvizicí, vývojem a údržbou a uplatňuje jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného IS,
- zajišťuje vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů detekovaných technickými nástroji, provádí jejich vyhodnocení a přijímá opatření k minimalizaci dopadů v důsledku jejich působení,
- komunikuje s ostatními bezpečnostními rolemi daného IS za účelem zajištění kybernetické bezpečnosti.

2.2 Práva manažera kybernetické bezpečnosti:

- spolupracovat s architektem kybernetické bezpečnosti IS a řídit jeho činnost, spolupracovat s garantem aktiv IS a administrátory technických aktiv pro zajištění splnění požadavků ZoKB a VoKB, k tomu vyžadovat součinnost a plnění úkolů,
- vyžadovat spolupráci a konzultaci s manažerem kybernetické bezpečnosti Objednatele,
- v případech, kdy nelze pravidla, postupy a opatření stanovená v bezpečnostních dokumentech nebo uvedená v ZoKB a VoKB naplnit nebo IS neumožňuje jejich aplikaci, předkládat opodstatněnou žádost o výjimku, prostřednictvím manažera kybernetické bezpečnosti Objednatele, ke schválení Výboru pro řízení kybernetické bezpečnosti.

3. Práva a povinnosti architekta kybernetické bezpečnosti IS

Architekt kybernetické bezpečnosti IS zajišťuje návrh bezpečnostních opatření. Odpovídá za návrh bezpečné architektury IS a dohlíží na jeho následnou implementaci.

3.1 Povinnosti architekta kybernetické bezpečnosti:

- musí mít znalost ZoKB a jeho prováděcích vyhlášek,
- zajišťuje návrh opatření při rozhodnutí NÚKIB o reaktivním opatření, ochranném opatření nebo varování,
- posuzuje zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva,
- určuje klíčové podmínky, principy a modely architektury IS, posuzuje a vybírá technologie a stanoví koncepci bezpečnostního rozvoje IS,
- připomínkuje bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv,
- definuje požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti,
- odpovídá za popis zajištění fyzické bezpečnosti IS v dokumentu *„Politika fyzické bezpečnosti“*,
- odpovídá za obsah a aktuálnost dokumentu *„Politika řízení provozu a komunikací“* IS,
- dohlíží na implementaci bezpečnostních opatření,
- navrhuje opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- poskytuje součinnost dalším bezpečnostním rolím,
- na žádost garanta aktiv IS analyzuje úrovně architektury kybernetické bezpečnosti, definuje pro ni metriky a identifikuje existující rizika a navrhuje strategii pro zmírnění rizik,
- vytváří a udržuje model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.),
- předkládá manažerovi kybernetické bezpečnosti IS návrhy změn bezpečnostních dokumentů,

- navrhuje změny architektury kybernetické bezpečnosti na Výbor pro řízení kybernetické bezpečnosti,
- aktualizuje pravidelně dokument *„Politika řízení kontinuity činností“* pro VIS,
- zajišťuje ve spolupráci s manažerem kybernetické bezpečnosti IS a garantem aktiv IS minimálně 1x ročně aktualizaci a otestování plánů obnovy IS,
- navrhuje opatření pro zvýšení odolnosti IS vůči kybernetickým incidentům s využitím technických nástrojů pro zajišťování stanovené úrovně dostupnosti,
- stanovuje a aktualizuje postupy pro provedení opatření vydaných NÚKIB, se zohledněním výsledků hodnocení rizik, provedených opatření, stavu dotčených bezpečnostních opatření a vyhodnocuje případné negativní dopady na provoz a bezpečnost IS,
- zajišťuje aktuálnost dokumentu *„Politika bezpečnosti komunikační sítě“*, ve kterém Objednatel dokumentuje též užití nástroje zajišťujícího ochranu integrity vnitřní komunikační sítě,
- zajišťuje, že Zhotovitel dle harmonogramu konkrétní dodávky nebo na žádost Objednatele provede bezpečnostní testy zranitelnosti aplikací, minimálně těch, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní konfigurační změně, změně topologie infrastruktury, použitého operačního systému nebo aplikačního softwaru anebo změně bezpečnostních mechanismů. O provedení bezpečnostních testů předává manažerovi kybernetické bezpečnosti IS *„Zprávu o výsledku provedení bezpečnostních testů“* s návrhy opatření,
- komunikuje s ostatními bezpečnostními rolemi IS pro zajištění kybernetické bezpečnosti.

3.2 Práva architekta kybernetické bezpečnosti:

- mít přístup k potřebné dokumentaci IS,
- vyžadovat součinnost garanta aktiv IS a manažera kybernetické bezpečnosti.