Příloha RD03 - Práva a povinnosti manažera a architekta kybernetické bezpečnosti VIS ISKN

č. sml. Objednatele: ČÚZK-12466/2018 -24 č. sml. Zhotovitele: B181228

1. Úvod

Práva a povinnosti manažera i architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají VIS ISKN.

2. Práva a povinnosti manažera kybernetické bezpečnosti VIS

Manažer kybernetické bezpečnosti VIS odpovídá za systém řízení bezpečnosti informací pro daný VIS a odpovídá se manažeru kybernetické bezpečnosti Objednatele.

2.1 Povinnosti manažera kybernetické bezpečnosti VIS:

- znalost ZoKB a jeho prováděcích vyhlášek,
- neprodleně hlásit manažerovi kybernetické bezpečnosti Objednatele kybernetické bezpečnostní incidenty VIS a vést jejich evidenci,
- připravovat pro manažera kybernetické bezpečnosti Objednatele podklady pro NÚKIB,
- za VIS připravovat pro manažera kybernetické bezpečnosti Objednatele podklady pro jednání Výboru pro řízení kybernetické bezpečnosti,
- odpovídat za zajištění odstranění nedostatků zjištěných při kontrolách NÚKIB,
- zajišťovat provedení reaktivních opatření,
- poskytovat součinnost auditorovi kybernetické bezpečnosti a auditorům KÚ/ZÚ/ČÚZK při provádění auditů a kontrol,
- vyhodnocovat a klasifikovat kybernetický bezpečnostní incident,
- klasifikovat, prošetřovat a určovat příčiny kybernetického bezpečnostního incidentu, vyhodnocovat účinnost preventivních a reaktivních opatření aplikovaných proti kybernetickému bezpečnostnímu incidentu,
- dokumentovat zvládání kybernetických bezpečnostních incidentů,
- navrhovat 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 ve VIS,
- zajišťovat provedení analýzy rizik a hodnocení aktiv,
- na základě výstupů analýzy rizik zpracovávat a vytvořit dokument *„Plán zvládání rizik“*,
- provádět 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,
- zpracovávat ve spolupráci s architektem kybernetické bezpečnosti VIS a garantem aktiv VIS dokument *„Prohlášení o aplikovatelnosti“*,
- připravovat podklady do dokumentu *„Zpráva z přezkoumání systému řízení bezpečnosti informací“* a předkládat je manažerovi kybernetické bezpečnosti Objednatele,
- garantovat implementaci schválených bezpečnostních opatření,
- zohledňovat, 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,

- stanovovat provozní pravidla a postupy, k zajištění bezpečného provozu VIS, v dokumentu *„Politika řízení provozu a komunikací“*,
- odpovídat za kontrolu přidělování jednoznačného identifikátoru uživatelům VIS,
- stanovovat bezpečnostní požadavky na změny VIS spojené s jeho akvizicí, vývojem a údržbou a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného VIS,
- zpracovávat na základě bezpečnostních potřeb a výsledků hodnocení rizik dokument *„Prohlášení o aplikovatelnosti“*,
- zajistit vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů detekovaných technickými nástroji, provádět jejich vyhodnocení a přijímat opatření k minimalizaci dopadů v důsledku jejich působení,
- komunikovat s ostatními bezpečnostními rolemi daného VIS za účelem zajištění kybernetické bezpečnosti,

2.2 Práva manažera kybernetické bezpečnosti VIS:

- řídit a spolupracovat s architektem kybernetické bezpečnosti VIS, garantem aktiv VIS 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 VIS 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 VIS

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

3.1 Povinnosti architekta kybernetické bezpečnosti VIS:

- znalost ZoKB a jeho prováděcích vyhlášek,
- implementovat rozhodnutí NÚKIB o reaktivním opatření, ochranném opatření nebo varování,
- posuzovat zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva,
- určovat klíčové podmínky, principy a modely architektury VIS, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje VIS,
- připomínkovat bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv,
- definovat požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti,
- odpovídat za popis zajištění fyzické bezpečnosti VIS v dokumentu *„Politika fyzické bezpečnosti“*,
- odpovídat za obsah a aktuálnost dokumentu *„Politika řízení provozu a komunikací“* VIS,
- dohlížet na implementaci bezpečnostních opatření,
- navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- poskytovat součinnost dalším bezpečnostním rolím,

- na žádost garanta aktiv VIS analyzovat úrovně architektury kybernetické bezpečnosti, definovat pro ni metriky a identifikovat existující rizika a navrhovat strategii pro zmírnění rizik,
- vytvářet a udržovat model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.),
- manažerovi kybernetické bezpečnosti VIS předkládat návrhy změn bezpečnostních dokumentů,
- na Výbor pro řízení kybernetické bezpečnosti navrhovat změny architektury kybernetické bezpečnosti,
- vytvářet a pravidelně aktualizovat dokument *„Strategie řízení kontinuity činností"* pro VIS,
- ve spolupráci s manažerem kybernetické bezpečnosti VIS a garantem aktiv VIS zajistit minimálně 1x ročně aktualizaci a otestování plánů obnovy VIS,
- navrhovat opatření pro zvýšení odolnosti VIS vůči kybernetickým incidentům s využitím technických nástrojů pro zajišťování stanovené úrovně dostupnosti,
- stanovovat a aktualizovat postupy pro provedení opatření vydaných NÚKIB, se zohledněním výsledků hodnocení rizik, provedených opatření, stavu dotčených bezpečnostních opatření a vyhodnocovat případné negativní dopady na provoz a bezpečnost VIS,
- odpovídat za aktuálnost dokumentu *„Politika bezpečnosti komunikační sítě"*, v kterém dokumentuje též užití nástroje zajišťujícího ochranu integrity vnitřní komunikační sítě,
- odpovídat za to, že Zhotovitel 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 bezpečnostní testů předává manažerovi kybernetické bezpečnosti VIS *„Zprávu o výsledku provedení bezpečnostních testů"* s návrhy opatření,
- komunikovat s ostatními bezpečnostními rolemi VIS pro zajištění kybernetické bezpečnosti.

3.2 Práva architekta kybernetické bezpečnosti VIS:

- vyžadovat součinnost garanta aktiv VIS a manažera kybernetické bezpečnosti VIS.