Příloha RD03 - Práva a povinnosti manažera a architekta kybernetické bezpečnosti RÚIAN

č. sml. Objednatele: ČÚZK-16929/2019-24 č. sml. Zhotovitele: CZBAP-127

1. Úvod

Práva a povinnosti manažera a architekta kybernetické bezpečnosti uvedené v tomto dokumentu se týkají VIS ISÚI a KIS RÚIAN (v dokumentu jsou oba systémy dále označované souhrnně jako IS).

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:

- znalost ZoKB a jeho prováděcích vyhlášek,
- neprodleně hlásit manažerovi kybernetické bezpečnosti Objednatele kybernetické bezpečnostní incidenty IS a vede jejich evidenci,
- připravovat pro manažera kybernetické bezpečnosti Objednatele podklady pro NÚKIB,
- připravovat za IS pro manažera kybernetické bezpečnosti Objednatele podklady pro jednání Výboru pro řízení kybernetické bezpečnosti,
- zajišťovat poskytnutí podkladů a návrhů řešení pro zajištění odstranění nedostatků, zjištěných při kontrolách NÚKIB,
- zajišťovat podklady a návrhy řešení pro provedení reaktivních opatření,
- poskytovat součinnost auditorovi kybernetické bezpečnosti a auditorům Objednatele při provádění auditů a kontrol,
- vyhodnocovat a klasifikovat kybernetický bezpečnostní incident,
- klasifikovat, prošetřovat a určovat příčiny kybernetického bezpečnostního incidentu, vyhodnocuje účinnost preventivních a reaktivních opatření aplikovaných proti kybernetickému bezpečnostnímu incidentu,
- zajišťovat podklady k dokumentaci 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 IS,
- zajišťovat pravidelné provedení analýzy rizik a hodnocení aktiv,
- aktualizovat dokument *„Plán zvládání rizik“* na základě výstupů analýzy 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 IS a garantem aktiv IS aktualizaci dokumentu *„Prohlášení o aplikovatelnosti“*,
- připravovat podklady do dokumentu *„Zpráva z přezkoumání systému řízení bezpečnosti informací“* a předkládá je manažerovi kybernetické bezpečnosti Objednatele,
- zajišťovat ve spolupráci s garantem aktiv implementaci schválených bezpečnostních opatření a na vyžádání zajišťuje jejich audit,
- 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 aktualizovat o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro

přijatelnost rizik, doplnit dokument *„Plán zvládání rizik“*. Splnění oznamovat manažerovi kybernetické bezpečnosti Objednatele,

- stanovovat provozní pravidla a postupy k zajištění bezpečného provozu IS, v dokumentu *„Politika řízení provozu a komunikací“*,
- zajišťovat kontrolu přidělování jednoznačného identifikátoru uživatelům IS,
- stanovovat bezpečnostní požadavky na změny IS spojené s jeho akvizicí, vývojem a údržbou a uplatňovat jejich zahrnutí do projektu, jehož součástí je akvizice, vývoj a údržba daného IS,
- zajišťovat 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 IS za účelem zajištění kybernetické bezpečnosti.

2.2 Práva manažera kybernetické bezpečnosti:

- řídit a spolupracovat s architektem kybernetické bezpečnosti IS, 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.

2.3 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.

2.4 Povinnosti architekta kybernetické bezpečnosti:

- znalost ZoKB a jeho prováděcích vyhlášek,
- zajišťovat návrh opatření při 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 IS, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje IS,
- 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 IS v dokumentu *„Politika fyzické bezpečnosti“*,
- odpovídat za obsah a aktuálnost dokumentu *„Politika řízení provozu a komunikací“* IS,
- dohlížet na implementaci bezpečnostních opatření,

- navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- poskytovat součinnost dalším bezpečnostním rolím,
- na žádost garanta aktiv IS 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.),
- předkládat manažerovi kybernetické bezpečnosti IS návrhy změn bezpečnostních dokumentů,
- navrhovat změny architektury kybernetické bezpečnosti na Výbor pro řízení kybernetické bezpečnosti,
- aktualizovat pravidelně dokument *„Politika řízení kontinuity činností“* pro VIS,
- zajišťovat 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,
- 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 IS,
- zajišťovat aktuálnost dokumentu *„Politika bezpečnosti komunikační sítě“*, v kterém Zadavatel dokumentuje též užití nástroje zajišťujícího ochranu integrity vnitřní komunikační sítě,
- zajišťovat, že Dodavatel 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 bezpečnostní testů předává manažerovi kybernetické bezpečnosti IS *„Zprávu o výsledku provedení bezpečnostních testů“* s návrhy opatření,
- komunikovat s ostatními bezpečnostními rolemi IS pro zajištění kybernetické bezpečnosti.

2.5 Práva architekta kybernetické bezpečnosti:

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