Příloha č. 2

Práva a povinnosti Manažera KB

(1) Manažer KB odpovídá za plánování a řízení realizace kybernetických bezpečnostních projektů schválené Komisí KB tak, aby informační a komunikační infrastruktura VŠTE poskytovala služby v této oblasti v souladu s právní úpravou v oblasti kybernetické bezpečnosti.

(1) Manažer KB odpovídá za vytvoření systému řízení bezpečnosti informací od průzkumu a analýz, přes průběžné testování prevence až po eliminaci následků a vyhodnocení „úspěšných“ kybernetických incidentů na VŠTE.

(2) Manažer KB odpovídá za zajištění schopnosti VŠTE implementovat opatření ukládaná kybernetickým zákonem a za včasnou a hospodárnou implementaci těchto opatření.

(3) Průběžně analyzuje vývoj SŘBI a vyhodnocuje identifikovaná kybernetická rizika, detekované kybernetické bezpečnostní události a odhalené kybernetické incidenty a předkládá o tom zprávu Komisi KB. Periodicita předložení zprávy je roční. Obsahem zprávy jsou i návrhy na zmírnění nepřijatelných rizik a návrhy na změnu priorit bezpečnostních projektů.

(4) Je oprávněn stanovit:

a) rozsah a hranice SŘBI (s ohledem na aktiva a organizační bezpečnost), ve kterých určí, kterých organizačních částí a technických prvků se SŘBI týká;

b) jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik;

c) cíle kontinuity činností a strategii (plán) řízení kontinuity další činnosti pro oblast kybernetické bezpečnosti;

d) provozní pravidla a postupy SŘBI;

e) plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, včetně určení osoby zajišťující prosazování bezpečnostních opatření.

(5) Podílí se na schvalování závazných norem pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií VŠTE.

(6) V případě projektů týkajících se informačních systémů:

a) konzultuje organizaci kontrol etap dílčího plnění;

b) rozhoduje se systémovým integrátorem o přípravě testovacích dat a organizaci bezpečnostního testování;

c) je informován o zkušebním a ověřovacím provozu a zátěžových testech;

d) podílí se na přípravě a organizaci akceptačního řízení.

(7) Po věcné stránce kontroluje formulaci zadávacích požadavků veřejných zakázek (včetně veřejných zakázek malého rozsahu) na výstavbu a modernizaci informačních a komunikačních systémů VŠTE, či na pořízení dodávek či služeb, jejichž komponenty

mohou mít vliv na kybernetickou bezpečnost VŠTE, z hlediska standardů kybernetické bezpečnosti a poskytuje součinnost zadavateli v zadávacích řízeních týkající se vyřešení otázek souvisejících s kybernetickou bezpečností. Podrobnější úprava je případně stanovena ve zvláštních interních předpisech a normách VŠTE.

(8) Řídí proces řešení kybernetické bezpečnostní události, nebo kybernetického incidentu a rozhoduje o způsobu řešení.

(9) Rozhoduje o realizaci bezpečnostního opatření na základě informací z monitorovacích a dohledových systémů, rozhodnutí Komise KB, nebo Národního úřadu pro kybernetickou a informační bezpečnost.

(10) Zajišťuje:

a) detekci kybernetických bezpečnostních událostí;

b) zpracovávání zpráv o hodnocení aktiv a rizik a prohlášení o aplikovatelnosti, které obsahuje přehled zavedených bezpečnostních opatření;

c) u dodavatelů pravidelné hodnocení rizik, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků;

d) aktualizaci SŘBI a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení účinnosti bezpečnostních opatření;

e) aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky; plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí;

f) realizaci reaktivních opatření vydaných Národním úřadem pro kybernetickou a informační bezpečnost;

g) součinnost při provádění kontrolních auditů prováděných Národním úřadem pro kybernetickou a informační bezpečnost.

(11) Navrhuje změny strategie kybernetické bezpečnosti VŠTE a bezpečnostní politiky SŘBI.

(12) Vypracovává plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje Komisi KB.

(13) Koordinuje opatření ke zvýšení bezpečnostního povědomí v organizaci včetně školení a cvičení kybernetické bezpečnosti.

(14) Odpovídá za stanovení pravidel pro dodavatele, která zohledňují potřeby SŘBI.

(15) Manažer KB je oprávněn vyžadovat:

a) od Komise KB rozhodnutí o přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik, včetně stanovení ještě přijatelné míry rizika a stanovení limitu finančních prostředků na eliminaci nepřijatelných rizik, a o prioritách realizace bezpečnostních opatření a navržených bezpečnostních projektů, a určení osob pro výkon rolí garantů aktiv a provedení základní identifikace aktiv;

b) od garantů primárních aktiv zpracování a předložení:

1. účelu systému a podmínek jeho provozování;

1. identifikovaných primárních aktiv a jejich rizik;

2. ohodnocení přijatelnosti těchto rizik;
3. stanovení bezpečnostních parametrů (úrovní) systémem poskytovaných služeb SLA (Service Level Agreement).

c) od garantů podpůrných aktiv a administrátorů (tzv. power users)

1. identifikování podpůrných aktiv a jejich rizik;
2. ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik;
3. vyhodnocení účinnosti kybernetických bezpečnostních opatření.