NÚKIB

BEZPEČNOSTNÍ ROLE

a jejich začlenění v organizaci

Verze 3.0, platná ke dni 6. 4. 2020

Obsah

Úvod

Tento podpůrný materiál vznikl jako vodítko pro správné začlenění výboru pro kybernetickou bezpečnost a bezpečnostních rolí v organizaci vyžadovaných vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „vyhláška o kybernetické bezpečnosti“), které povinné osoby podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“) musí v rámci systému řízení bezpečnosti informací (dále také „ISMS“) zavést a řídit. Zároveň, v rámci bezpečnosti lidských zdrojů, musí být zajištěno odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí (vstupní a pravidelná školení).

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

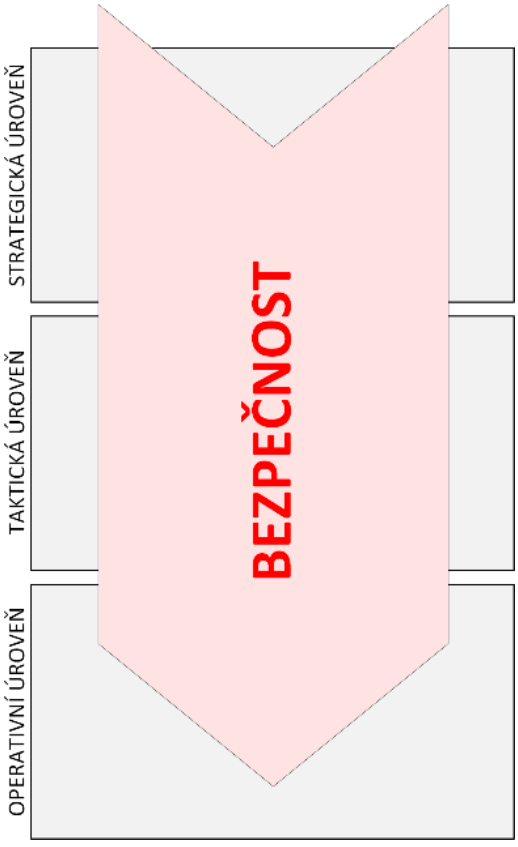
Tento materiál popisuje jednu z možných variant, jak bezpečnostní role, definované vyhláškou o kybernetické bezpečnosti, implementovat do organizační struktury organizace. Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Bezpečnost a úrovně managementu organizace

V ideálním případě je vhodné útvar kybernetické/ICT bezpečnosti zařadit pod tzv. ICT Governance, který je přímo řízený vrcholovým vedením organizace. Jeho cílem je, zjednodušeně řečeno, maximalizovat efektivitu organizace za použití ICT prostředků. Obecně existuje celá řada nejrůznějších metodik a principů, jak sestavit podnikovou architekturu (známou taktéž pod anglickým názvem Entreprise Architecture). Zákon o kybernetické bezpečnosti ani související právní předpisy toto nijak neupravují.

Především je nutné mít na paměti, že kybernetická/ICT bezpečnost prochází napříč všemi úrovněmi managementu. Z toho důvodu by měly být stanoveny role, které budou bezpečnost na jednotlivých úrovních managementu zajišťovat.

Žádoucí je, aby byl útvar kybernetické/ICT bezpečnosti oddělen od útvaru, který zajišťuje provoz ICT.



Obrázek č. 1: Bezpečnost a úrovně managementu organizace

2 Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role

2.1 Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti je organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury (dále jen „KII"), významného informačního systému (dále jen „VIS") nebo informačního systému základní služby (dále jen „ISZS"), anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.

Vyhláška o kybernetické bezpečnosti stanovuje, že mezi členy výboru pro řízení kybernetické bezpečnosti musí být zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti.

V praxi může být výbor tvořen lidmi z vrcholového i středního managementu, zároveň by měl mít většinu zástupců z oblasti ICT a bezpečnosti (může se lišit podle způsobu řízení jednotlivých organizací). Konkrétní způsob sestavení výboru pro řízení kybernetické bezpečnosti je plně v rukou vedení organizace, zákon o kybernetické bezpečnosti ani jeho prováděcí právní předpisy jej nad rámec výše uvedeného neregulují.

Doporučení pro Výbor pro řízení kybernetické bezpečnosti jsou uvedena v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

2.2 Bezpečnostní role

Manažer kybernetické bezpečnosti je osoba, odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let nebo jednoho roku, pokud absolvovala studium na vysoké škole. Manažer kybernetické bezpečnosti je zodpovědný za pravidelné informování vrcholového vedení o činnostech, které vyplývají z rozsahu jeho odpovědnosti a stavu systému řízení informační bezpečnosti.

V praxi je manažer kybernetické bezpečnosti jakýmsi mezistupněm mezi vrcholovým vedením (strategickou úrovní managementu) a operativní úrovní. Výkon role manažera kybernetické bezpečnosti musí být oddělen od rolí, které jsou odpovědné za provoz informačního a komunikačního systému a s dalšími provozními nebo řídicími rolemi.

Doporučení pro manažera kybernetické bezpečnosti naleznete v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

Architekt kybernetické bezpečnosti je osoba zajišťující návrh implementace bezpečnostních opatření (pro zajištění bezpečné architektury informačního a komunikačního systému), která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let nebo jednoho roku, pokud absolvovala studium na vysoké škole.

V praxi je architekt odpovědný za návrh implementace bezpečné architektury (např. od infrastruktury až po bezpečnost na aplikační úrovni).

Doporučení pro architekta kybernetické bezpečnosti naleznete v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti je osoba, provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let nebo jednoho roku, pokud absolvovala studium na vysoké škole. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu jiných bezpečnostních rolí.

Doporučení pro auditora kybernetické bezpečnosti naleznete v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

Garantem aktiva je fyzická osoba pověřená organizací k zajištění rozvoje, použití a bezpečnosti aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva)[1].

Doporučení pro garanta aktiva naleznete v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

2.3 Zastupitelnost bezpečnostních rolí

Správci a provozovatelé KII a ISZS zajistí zastupitelnost role manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti.

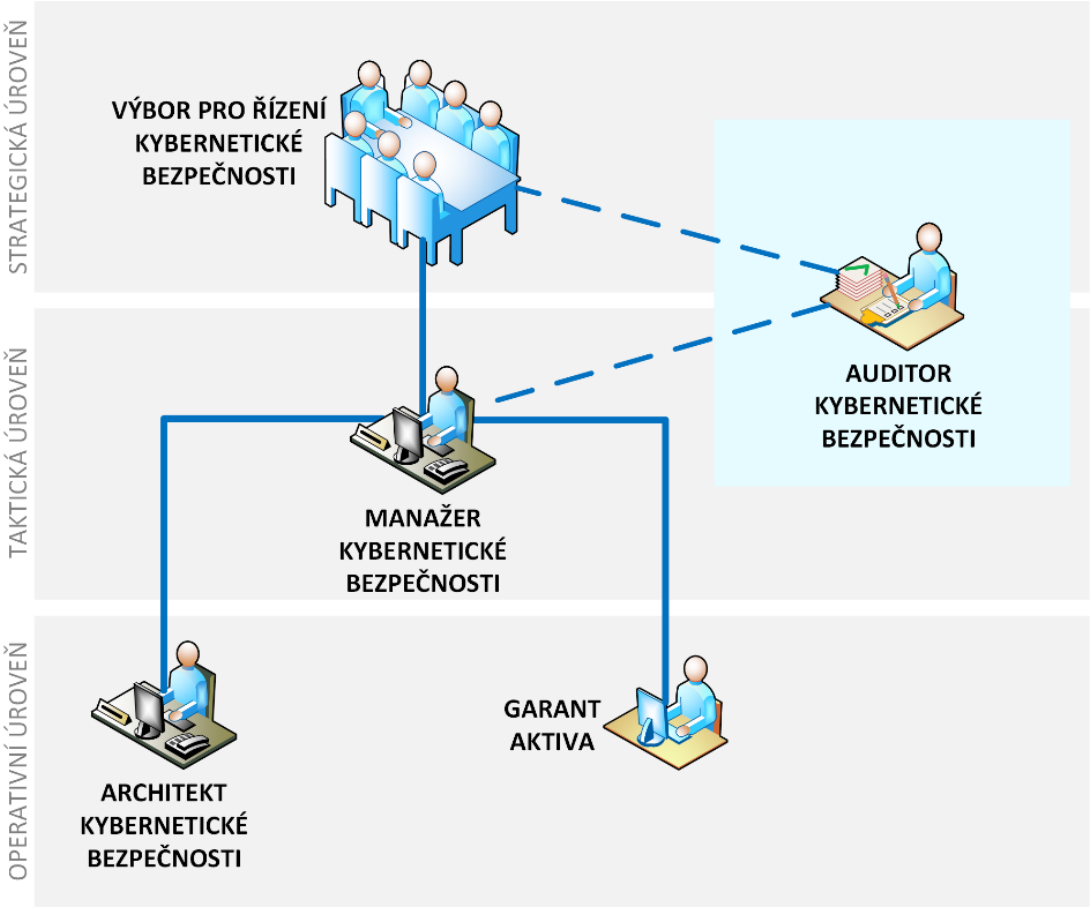
Správci a provozovatelé VIS zajistí zastupitelnost manažera kybernetické bezpečnosti.

V případě zastupujících osob nejsou vyhláškou o kybernetické bezpečnosti kladeny nároky na požadovanou praxi těchto osob. Pro osoby, které zajišťují bezpečnostní role, je potřeba zajistit příslušné pravomoci a zdroje (včetně rozpočtu), aby mohly naplňovat své role a úkoly.

Povinná osoba, která určuje osoby zastávající bezpečnostní role, přihlédne k doporučením uvedeným v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

[1] V normách řady ISO/IEC 27000 se setkáme s pojmem **vlastník aktiva**, v praxi se jedná o tutéž roli. Avšak pozor, v tomto případě pojem vlastník neznamená, že by měla role k aktivu vlastnická práva.

Hierarchii výboru kybernetické bezpečnosti a bezpečnostních rolí je možno v rámci úrovní managementu organizace znázornit následovně



Obrázek č. 2: Hierarchie výboru kybernetické bezpečnosti a bezpečnostních rolí

3 RACI matice

Tzv. RACI matice se používá pro popis procesů ve formě tabulky. Tabulka představuje matici aktivit (procesů) a rolí, které mají k dané aktivitě předem definovaný vztah. Tento vztah je tvořen z písmen R, A, C, I, která znamenají:

- R (Responsible) – procesní role má fyzickou odpovědnost za vykonání dané aktivity.
- A (Accountable) – procesní role má odpovědnost za fakt, že daný proces je vykonáván tak, jak bylo předdefinováno. U každého procesu může být jen jedna tato role (většinou se jedná o vedoucího pracovníka, který je odpovědný za práci svého týmu).
- C (Consulted) – procesní role podílející se na výkonu procesu, avšak nepřebírá za výkon procesu odpovědnost (jde o konzultační či spolupracující roli).
- I (Informed) – procesní role, která musí být o výstupech procesu informována.

Tabulka č. 1: RACI matice – příklad popisu základních procesů spojených s bezpečnostními rolemi

Příklady procesů týkajících se kybernetické bezpečnosti	Výbor KB	Bezpečnostní role			
		Manažer KB	Architekt KB	Auditor KB	Garant aktiva
Celkové řízení a rozvoj KB	R, A	C, I	C, I	C, I	C, I
Audit KB	A, C, I	C, I	C, I	R	C, I
Systém řízení bezpečnosti informací	A, C, I	R	C, I	C	C, I
Návrh bezpečnostních opatření	C, I	A, C, I	R	C	C, I
Implementace bezpečnostních opatření	C, I	A, C, I	R	C	C, I
Zajištění rozvoje, použití a bezpečnosti aktiva	C, I	A, C, I	C, I	C	R

Pozn.: Vztahy výboru kybernetické bezpečnosti, stejně tak jako jednotlivých rolí a procesů se mohou u organizací mírně lišit

4 Časté dotazy ohledně výboru kybernetické bezpečnosti a bezpečnostních rolí

Je možné pro zajištění jednotlivých bezpečnostních rolí najmout externího odborníka?

Ano, možné to je. V takovém případě by organizace nad externími odborníky měla řídit rizika. Takový externí odborník bude také obvykle v pozici významného dodavatele.

Jaké by měly mít jednotlivé role certifikace a jak a kým by měli být pracovníci zastávající tyto role vyškoleni?

Účinnost zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů doslova otevřela trh s nabídkou nejrůznějších školení těchto bezpečnostních rolí, důležité je však mít na paměti, že klíčová není forma školení, ale obsah. Jestliže organizace nedisponuje odborníkem, který by pracovníka pro potřebnou roli vyškolil, pak pravděpodobně bude nutné zvolit některé ze školení na trhu, volba je však na organizaci samotné.

Vyhláška o kybernetické bezpečnosti v příloze č. 6 uvádí doporučené certifikace pro jednotlivé bezpečnostní role:

Manažer kybernetické bezpečnosti

- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Security Professional (CISSP)
- Manažer BI (akreditační schéma ČIA)

Architekt kybernetické bezpečnosti

- Certified Ethical Hacker (CEH)
- CompTIA Security +
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Security Professional (CISSP)
- Manažer BI (akreditační schéma ČIA)

Auditor kybernetické bezpečnosti

- Certified Information Systems Auditor (CISA)
- Certified Internal Auditor (CIA)
- Certified in Risk and Information Systems Control (CRISC)

- Lead Auditor Information Security Management Systém (Lead Auditor ISMS)
- Auditor BI (akreditační schéma ČIA)

Certifikace může být i jiná, než jsou výše uvedené, avšak jen jestliže certifikace dokládající odbornou způsobilost bezpečnostních rolí splňuje požadavky ISO 17024.

Jak prokazovat požadovanou praxi u manažera, architekta a auditora?

Zákon o kybernetické bezpečnosti, ani jeho prováděcí předpisy toto blíže nespecifikují. Cílem však je, aby stanovené role vykonávaly osoby způsobilé. Např. roli manažera kybernetické bezpečnosti můžeme přiřadit projektovému manažerovi v oblasti ICT bezpečnosti, který má v této oblasti více než 3 letou praxi nebo alespoň roční praxi a absolvované studium na vysoké škole s tím, že mu organizace zajistí školení ISMS a projektový manažer výkon této role zvládne. Obdobně je možné postupovat i u ostatních rolí.

Může jedna osoba zajišťovat více rolí současně?

Ano, je možné, aby jedna osoba byla zároveň manažerem a architektem kybernetické bezpečnosti a zároveň garantem aktiva. Žádná z těchto rolí však nemůže zastávat i roli auditora.

Musí správci a provozovatelé VIS určovat bezpečnostní role?

Vyhláška o kybernetické bezpečnosti říká, že správci a provozovatelé VIS určí role manažera kybernetické bezpečnosti a garantů aktiv. Ostatní bezpečnostní role určí přiměřeně vzhledem k rozsahu a potřebám ISMS. Na správce a provozovatele VIS jsou kladeny obecně nižší požadavky po stránce bezpečnostních opatření, než na správce a provozovatele KII a ISZS. Ve skutečnosti však vždy někdo v organizaci nese odpovědnost např. za zajištění bezpečnosti informací či odpovědnost za implementaci nové bezpečnostní technologie.

5 Použité zdroje

Česká republika. Zákon č. 181 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014.

Česká republika. Vyhláška č. 82 ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2018.

ČSN ISO/IEC 27 000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 31 s.

ČSN ISO/IEC 27 001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 25 s.

ČSN ISO/IEC 27 002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 74 s.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
13. 9. 2018	1.0	Odb. RAP	Vytvoření dokumentu
28. 1. 2019	1.1	Odb. regulace	Změna kontaktních údajů
18. 2. 2020	2.0	Odb. kontroly	Úpravy v souvislosti s novou legislativou
6. 4. 2020	3.0	Odb. kontroly	Oprava