10.6 Organizační bezpečnost

Tento dokument popisuje opatření, která MUSÍ, nebo BY MĚLA být implementována pro

- **Určení bezpečnostních rolí, jejich práv a povinností.**
- **Splnění požadavků na oddělení výkonu činností jednotlivých bezpečnostních rolí.**
- **Splnění požadavků na oddělení výkonu bezpečnostních a provozních rolí.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Systém řízení bezpečnosti informací (§ 6).

1 Určení bezpečnostních rolí a jejich práv a povinností

Cíl: Přiřadit, identifikovat a popisovat odpovědnosti jednotlivých bezpečnostních rolí Stanovení systematického přístupu vedoucího ke zvyšování kybernetické bezpečnosti, včetně požadavků na vrcholové vedení v oblasti organizační bezpečnosti a určení odpovědností v oblasti kybernetické bezpečnosti.

1.1 Bezpečnostní role

Organizace MUSÍ zavést řízení kybernetické a informační bezpečnosti (dále jen „organizační bezpečnost“), v rámci, kterého MUSÍ určit výbor pro řízení kybernetické bezpečnosti, bezpečnostní role, jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury.

Implementační pokyny:

1.1.1 **Výbor pro řízení kybernetické bezpečnosti** MUSÍ být tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností. Členem MUSÍ být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti.

1.1.2 Pro osoby, které zajišťují bezpečnostní role MUSÍ být zajištěny příslušné pravomoci a zdroje (včetně rozpočtu), aby mohly naplňovat své role a úkoly.

1.1.3 MUSÍ být zajištěno odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí viz směrnice SM-5 Bezpečnost lidských zdrojů.

1.1.4 MUSÍ být zajištěno zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.

1.1.5 MUSÍ být určeny osoby, které budou zastávat bezpečnostní role a zastupitelnost bezpečnostních rolí a) a b):

a) Manažer kybernetické bezpečnosti

- je bezpečnostní role odpovědná za systém řízení bezpečnosti informací, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti po dobu nejméně tří let, nebo po dobu jednoho roku, pokud absolvovala studium na vysoké škole
- odpovídá za pravidelné informování vrcholového vedení o činnostech vyplývajících z rozsahu jeho odpovědnosti a stavu kybernetické bezpečnosti.

b) Architekt kybernetické bezpečnosti

- je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti po dobu nejméně tří let, nebo po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

c) Garant aktiva

- je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.

d) Auditor kybernetické bezpečnosti

- je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací po dobu nejméně tří let, nebo po dobu jednoho roku, pokud absolvovala studium na vysoké škole,
- zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné.

Vedení společnosti při určování osob zastávajících bezpečnostní role přihlédne k doporučením uvedeným v následující RACI matici:

- **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 1: RACI matice základních procesů spojených s bezpečnostními rolemi (Zdroj: (1))

procesy	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

1.2 Zastupitelnost bezpečnostních rolí

1.2.1 MUSÍ být zajištěna zastupitelnost role manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti.

1.2.2 V případě zastupujících osob nejsou kladeny nároky na požadovanou praxi těchto osob.

2 Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí

2.1.1 Jedna osoba MŮŽE být zároveň manažerem a architektem kybernetické bezpečnosti a zároveň garantem aktiva. Žádná z těchto rolí však NESMÍ plnit i roli auditora

3 Požadavky na oddělení výkonu bezpečnostních a provozních rolí

3.1.1 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.

3.1.2 Auditor kybernetické bezpečnosti MUSÍ svoji roli vykonávat nestranně a výkon jeho role MUSÍ být oddělen od výkonu jiných bezpečnostních rolí. Role MŮŽE být předmětem outsourcingu.

Použité zdroje

(1) Bezpečnostní role a jejich začlenění v organizaci. In: *Podpůrné materiály* [online]. Verze 3.0. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2021-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

(2) ČESKÁ REPUBLIKA. Vyhláška 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. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)