Název předmětu: Kybernetická bezpečnost

Téma: 4. Management kybernetické bezpečnosti a bezpečnostní role

Cíl: Cílem je seznámit studenty s cíli a posláním managementu kybernetické bezpečnosti. Objasnit studentům obsah a cíle jednotlivých bezpečnostních rolí.

Úkoly pro samostatnou práci: naučit se a zopakovat si základní pojmy z oblasti kybernetické bezpečnosti, zopakovat si obsah a cíle jednotlivých bezpečnostních rolí.

Studijní literatura:

1. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
2. HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav; PTÁČEK, Bohumil; SKORUŠA, Leopold; SLOŽIL, Richard. *Kybernetická bezpečnost: teorie a praxe.* Praha: Powerprint s.r.o., 2015, 250 s. ISBN 978-80-87994-72-6.
3. HRŮZA, Petr; PITAŠ, Jaromír; ŠANDA, Jaroslav; BRECHTA, Bohumil. *Kybernetická bezpečnost II.* Brno: Univerzita obrany, Brno, 2013, 100 s. ISBN 978-80-7231-931-2.
4. HRŮZA, Petr. *Kybernetická bezpečnost.* Brno: Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5.
5. Vydané normy ISO/ČSN řady 27000, platné zákony a vyhlášky z oblasti kybernetické bezpečnosti

Obsah:

Vymezení pojmů

a) administrátorem osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva,

b) akceptovatelným rizikem riziko, které je přijatelné pro orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona, (dále jen „povinná osoba“) a není nutné jej zvládat pomocí dalších bezpečnostních opatření,

c) bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv,

d) hodnocením rizik celkový proces identifikace, analýzy a vyhodnocení rizik,

e) hrozbou potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu,

f) podpůrným aktivem technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému,

g) primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém,

h) rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu,

i) řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,

j) systémem řízení bezpečnosti informací část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat,

k) technickým aktivem takové technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém,

l) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, které využívají aktiva,

m) vrcholovým vedením osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby,

n) významným dodavatelem provozovatel informačního nebo komunikačního systému (dále jen „provozovatel“) a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému,

o) významnou změnou změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko,

p) zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Pro důsledné zajišťování informační strategie je potřebné určit jejího zodpovědného reprezentanta ve firmě. Roli reprezentanta zodpovědného za informační strategii firmy zastává obvykle **informační manažer**.

Monitoruje situaci uvnitř i vně firmy a na základě důkladné analýzy svých poznatků dokáže posoudit riziko jednotlivých akcí celé informační strategie firmy.

Informační manažer nebo jiný subjekt, odpovědný za **informační strategii** (například externí firma) pak odpovídá za kvalitu specifikace klíčových informací pro podporu rozhodování

řídících pracovníků firmy a výběr standardů, které chce firma uplatňovat při budování informačního systému.

Povinná osoba v rámci systému řízení bezpečnosti informací

a) stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká,

b) stanoví cíle systému řízení bezpečnosti informací,

c) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření,

d) řídí rizika podle § 5,

e) vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 30 a zavede přiměřená bezpečnostní opatření,

f) zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“) podle § 16,

g) zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací,

h) průběžně identifikuje a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací,

i) aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými významnými změnami a

j) řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

Organizační bezpečnost

(1) Povinná osoba s ohledem na systém řízení bezpečnosti informací

a) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 3 slučitelných se strategickým směřováním povinné osoby,

b) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,

c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,

d) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,

e) zajistí podporu k dosažení zamýšlených výstupů systému řízení bezpečnosti informací,

f) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,

g) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,

h) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,

i) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,

j) zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,

k) pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a

l) zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

(2) Povinná osoba v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona určí osobu, která bude zastávat bezpečnostní roli

a) manažera kybernetické bezpečnosti,

b) architekta kybernetické bezpečnosti,

c) garanta aktiva a

d) auditora kybernetické bezpečnosti.

(4) Povinná osoba uvedená v § 3 písm. e) zákona určí role manažera kybernetické bezpečnosti a garanta aktiva. Ostatní bezpečnostní role podle odstavce 3 určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací.

(5) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 3 písm. a) a b).

(6) Povinná osoba uvedená v § 3 písm. e) zákona zajistí zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti.

(7) Výbor pro řízení kybernetické bezpečnosti je 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, jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.

Bezpečnostní role

Povinná osoba uvedená v § 3 písm. c), d) a f) zákona určí osobu, která bude zastávat bezpečnostní roli

1. **manažera kybernetické bezpečnosti,**
2. **architekta kybernetické bezpečnosti,**
3. **garanta aktiva a**
4. **auditora kybernetické bezpečnosti.**

(1) Manažer kybernetické bezpečnosti

a) 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 nebo s řízením bezpečnosti informací

   1. po dobu nejméně tří let, nebo

   2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) odpovídá za pravidelné informování vrcholového vedení o

1. činnostech vyplývajících z rozsahu jeho odpovědnosti a

2. stavu systému řízení bezpečnosti informací a

c) nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.

(2) 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

a) po dobu nejméně tří let, nebo

b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

(3) Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.

(4) Auditor kybernetické bezpečnosti

a) 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

1. po dobu nejméně tří let, nebo

2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné, a

c) nesmí být pověřen výkonem jiných bezpečnostních rolí.

(5) Povinná osoba při určování osob zastávajících bezpečnostní role přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.