Řízení informační bezpečnosti v organizaci

Dodatek

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

Dodatek přednášky

Oblasti řízení ovlivněné prosazováním informační bezpečnosti a přehled odpovědností a činností managementu organizace:

- Dosažení souladu všech strategií činností organizace
- Řízení rizik
- Dodávání (navyšování) hodnoty činností organizace
- Řízení zdrojů
- Měření výkonu
- Zajišťování integrace procesů

Dosažení souladu všech strategií činností organizace

Dosažení souladu strategií organizace – koncept

- ✓ Musí se dosáhnout sladění strategie informační bezpečnosti s celkovou strategií činností organizace tak, aby informační bezpečnost podporovala dosahování cílů organizace, ne více, ne méně
- ✓ přijatá bezpečnostní opatření musí pokrývat bezpečnostní potřeby organizace v oblasti informační bezpečnosti
- ✓ musí být určeny role a stanoveny jejich povinnosti a pravomoci pro navrhování, schvalování, prosazování a kontrolu informační bezpečnosti
- ✓ bezpečnostní řešení musí být vybíraná a implementovaná s respektem ke stávajícím procesům a používaným technologiím, firemní kultuře a organizační struktuře
- ✓ investice do informační bezpečnosti musí být prováděné v souladu se strategií činností organizace tak, aby řešily adekvátní pokrytí identifikovaných rizik

Dosažení souladu všech strategií činností organizace

- Dosažení souladu strategií – povinnosti na úrovních řízení
- Správní rada
  - ✓ Vyžaduje prokazatelnost dosažení souladu všech strategií organizace (prokazování typicky důkazy dodanými auditní zprávou)
- Výkonný management
  - ✓ Ustanovuje procesy nutné k propojení informační bezpečnosti a cílů organizace
- Řídicí výbor (informační bezpečnosti)
  - ✓ Přezkoumává a podporuje strategie informační bezpečnosti a usiluje o jejich integraci
  - ✓ Zajišťuje, aby management podporoval integraci informační bezpečnosti do strategií organizace
- ↓

Dosažení souladu všech strategií činností organizace

- Dosažení souladu strategií – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Vytváří strategii dosahování informační bezpečnosti (→ politiku informační bezpečnosti)
  - ✓ Dohlíží na plnění bezpečnostního programu (→ na prosazování politiky informační bezpečnosti)
  - ✓ Komunikuje s manažery a vlastníky organizace pro zajištění trvalého souladu strategií
- Audit
  - ✓ Vyhodnocuje dosažený soulad strategií a o výsledku podává auditní zprávu

Řízení rizik

Řízení rizik – koncept

- ✓ Řízení a realizace opatření pro zmírnění rizik resp. snížení potenciálních dopadů na aktiva organizace na akceptovatelnou úroveň
- ✓ Vedení organizace musí vyjádřit zájem o řešení rizik a určit v souladu s cíli organizace úroveň tolerance rizik
- ✓ V organizaci musí být známé zranitelnosti, hrozby a rizika ohrožující aktiva a dosažení cílů
- ✓ Management musí porozumět rizikům, kterým je organizace vystavena, a dopadům, které mohou nastat
- ✓ Management musí stanovit způsoby řízení rizik vč. priorit, s jakými budou rizika zvládaná nebo akceptovaná
- ✓ Musí být zavedený proces řízení rizik pokrývající zejména analýzu rizik, vyhodnocování rizik, analýzy trendů a zvládání rizik navrhováním opatření pro zmírnění rizik

Řízení rizik

- Řízení rizik – povinnosti na úrovních řízení
- Správní rada
  - ✓ Určuje politiku řízení rizik, úroveň tolerance rizik a garantuje regulatorní soulad (soulad s legislativou, smlouvami, . . .)
- Výkonný management
  - ✓ Zajišťuje role a odpovědnosti vč. řízení rizik všech činností
  - ✓ Monitoruje dodržování regulatorního souladu
- Řídicí výbor (bezpečnosti)
  - ✓ Identifikuje nová rizika
  - ✓ Podporuje bezpečnostní praktiky organizačních jednotek a identifikuje otázky/problémy v dodržování jejich souladu
- ↓

Řízení rizik

- Řízení rizik – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Zajišťuje, že se provádí hodnocení rizik a dopadů informačních aktiv
  - ✓ Vytváří strategii pro zmírnění rizik (→ politiku informační bezpečnosti)
  - ✓ Prosazuje tuto politiku a regulatorní soulad
- Audit
  - ✓ Vyhodnocuje řízení rizik a podává o výsledku zprávy

Dodávání (navyšování) hodnoty činností organizace

Dodávání (navyšování) hodnoty činností organizace – koncept

- ✓ Optimalizace investic do informační bezpečnosti potřebné pro podporu dosahování cílů organizace
- ✓ Musí být vytvořena standardní sada bezpečnostních praktik tvořící základní úroveň bezpečnosti a přiměřeně pokrývající rizika
- ✓ Úsilí musí být vhodně rozdělované tak, aby primárně byla zvládaná nejvyšší rizika
- ✓ Bezpečnostní opatření musí být vhodně standardizovaná s ohledem na efektivní spotřebu zdrojů dostupných pro zajišťování bezpečnosti
- ✓ Všichni v organizaci musí chápat informační bezpečnost jako trvalý proces, nikoli jako jednorázovou akci
- ✓ Bezpečnostní řešení musí být zaváděna tak, aby i při spotřebě zdrojů přinášela přidanou hodnotu a příspívala k plnění cílů organizace

Dodávání (navyšování) hodnoty činností organizace

- Dodávání (navyšování) hodnoty činností organizace – povinnosti na úrovních řízení
- Správní rada
  - ✓ Vyžaduje zprávy o nákladech a přínosech bezpečnostních aktivit a ochrany aktiv
- Výkonný management
  - ✓ Analyzuje konkrétní případové studie bezpečnostních řešení
- Řídicí výbor (bezpečnosti)
  - ✓ Přezkoumává a doporučuje adekvátní bezpečnostní kroky podporující ostatní činnosti organizace
- ↓

Dodávání (navyšování) hodnoty činností organizace

- Dodávání (navyšování) hodnoty činností organizace – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Monitoruje využívání a efektivitu zdrojů na informační bezpečnost
- Audit
  - ✓ Vyhodnocuje efektivitu a výkonnost bezpečnostních opatření a podává o výsledku zprávy

Řízení zdrojů

- Řízení zdrojů – koncept
  - ✓ Cílem je účinné a účelné využívání bezpečnostních znalostí, infrastruktury a zdrojů organizace
  - ✓ Nabyté a osvojené bezpečnostní znalosti musí být dostupné a chráněné
  - ✓ Bezpečnostní procesy a aktivity musí být vhodně standardizované
  - ✓ Zavedené procesy a praktiky musí být dokumentované
  - ✓ Bezpečnostní architektura musí být vytvořena tak, aby určovala a efektivně využívala zdroje na bezpečnost
  - ✓ Všechna aktiva musí být využívána a spotřebovávána v souladu s cíli organizace

Řízení zdrojů

- Řízení zdrojů – povinnosti na úrovních řízení
- Správní rada
  - ✓ Dohlíží na politiku řízení znalostí a využití zdrojů
- Výkonný management
  - ✓ Zajišťuje procesy pro nabývání znalostí a měření účinnosti a účelnosti využívání zdrojů
- Řídicí výbor (bezpečnosti)
  - ✓ Přezkoumává procesy pro nabývání a šíření znalostí
- ↓

Řízení zdrojů

- Řízení zdrojů – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Vytváří metody pro nabývání a šíření znalostí
  - ✓ Vytváří metriky pro měření účinnosti a účelnosti využívání zdrojů
- Audit
  - ✓ Vyhodnocuje řízení zdrojů a podává o výsledku zprávy

Měření výkonu

Měření výkonu – koncept

- ✓ Nepřetržité sledování naplňování cílů organizace požaduje měření, monitorování a reportování procesů řízení bezpečnosti
- ✓ Bezpečnostní metriky musí být definovány v souladu se strategickými cíli organizace a musí být odsouhlaseny
- ✓ Procesy řízení bezpečnosti musí být měřeny tak,
  aby byly identifikovány nedostatky a
  aby byla zajištěna zpětná vazba do implementovaných nápravných opatření
- ✓ Musí být prováděny nezávislé analýzy a audity bezpečnosti

Měření výkonu

- Měření výkonu – povinnosti na úrovních řízení
- Správní rada
  - ✓ Vyžaduje zprávy o efektivitě bezpečnosti
- Výkonný management
  - ✓ Požaduje provádět monitorování a metriky pro bezpečnostní činnosti
- Řídicí výbor (bezpečnosti)
  - ✓ Přezkoumává a doporučuje zda a jak bezpečnostní aktivity naplňují cíle organizace
- ↓

Měření výkonu

- Měření výkonu – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Vytváří a zavádí přístupy k monitorování a měření
  - ✓ Řídí a monitoruje bezpečnostní aktivity
- Audit
  - ✓ Vyhodnocuje úroveň účinnosti a účelnosti měření a metrik a podává o výsledku zprávy

Zajišťování integrace procesů

Zajišťování integrace procesů – koncept

- ✓ Činnosti zajišťování bezpečnosti musí musí být prováděné v souladu se strategií činností organizace a tak, aby byla minimalizovaná možnost výskytu skrytých rizik
- ✓ Nesmí existovat nedostatky v ochraně aktiv organizace
- ✓ Bezpečnostní opatření se nesmí zbytečně překrývat, nesmí být neúčelně redundantní
- ✓ Činnosti pro zajištění bezpečnosti musí být implementovány v souladu se strategií organizace a musí být vzájemně provázány
- ✓ Musí být správně určeny role a odpovědnosti za bezpečnostní procesy
- ✓ Pracovníci zajišťujícíc bezpečnost musí vzájemně komunikovat a rozumět svým potřebám

Zajišťování integrace procesů

- Zajišťování integrace procesů – povinnosti na úrovních řízení
- Správní rada
  - ✓ Dohlíží na politiku zajišťující integraci procesů
- Výkonný management
  - ✓ Dohlíží nad činnostmi zajišťujícími bezpečnost a nad plány pro integraci
- Řídicí výbor (bezpečnosti)
  - ✓ Indikuje kritické procesy a odpovědnosti
  - ✓ Řídí aktivity vedoucí k provázání procesů bezpečnosti
- ↓

Zajišťování integrace procesů

- Zajišťování integrace procesů – povinnosti na úrovních řízení
- ↓
- CISO, Chief of Information Security Officer
  - ✓ Udržuje kontakt s ostatními odpovědnými pracovníky
  - ✓ Zajišťuje, aby byly identifikovány a řešeny nedostatky v informační bezpečnosti
- Audit
  - ✓ Vyhodnocuje efektivitu procesů pro zajištění bezpečnosti prováděných v rámci různých oblastí a podává o výsledku zprávy