Řízení informační bezpečnosti

PV017

Kamil Malinka
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

Osnova

- Stručně o řízení rizik
- Politika informační bezpečnosti
- Legislativa informační bezpečnosti

Stručně o řízení rizik

Řízení informační bezpečnosti PV017

Kamil Malinka

(využity materiály Doc. Staudka a konzultace Prof. Matyáše)

Verze: podzim 2024

Základní pojmy informační bezpečnosti

- **Aktivum** (Assets) - cokoli hodnotného, užitečného, věc, výhoda, zdroj
- **Zranitelnost** (Vulnerability) - slabina využitelná ke způsobení škod/ztrát organizaci útokem
- **Hrozba** (Threat) – potenciální příčina nechtěného incidentu
- **Útok** (Attack) – pokus o způsobení škody na aktivech
- **Bezpečnostní incident** (Security incident) – událost, která může ohrozit bezpečnost informací
- **Riziko** (Risk) - pravděpodobnost, že se v daném zranitelném místě uplatní hrozba
- **Opatření** (Control) – prostředek, který modifikuje riziko

Rizika

- Reprezentace negativního dopadu využití zranitelnosti, tj. útoku, přičemž zohledňuje jak pravděpodobnost tak i škodní dopad útoku
- Rizika mohou plynout
  - Z cílů a řešení podnikatelských procesů
  - Nedokonalého vyhovění zákonným/smluvním závazkům
  - Úrovně kvality návrhových, implementačních a provozních procedur aplikačních systémů
- Rizika mohou existovat nezávisle na naší vůli -
  - Výpadek energie, záplava, zemětřesení, požár, …
- Standard ISO/IEC 27001:2013, odst. 6.1.2 požaduje:
  - Organizace musí přistupovat k výběru a k provozování bezpečnostních opatření na základě znalosti rizik
  - K rizikům se přistupuje na bázi scénářů, nikoli pouze na bázi aktiv
  - Rizika se je nutné zvažovat napříč celé chráněné oblasti, nikoli jednotlivě vůči hrozbám jednotlivým aktivům

Riziko se vyjadřuje

- V pravděpodobnostních pojmech (s jakou pravděpodobností se hrozba uplatní)
- V pojmech charakterizujících dopad hrozby (velikost škody způsobené útokem)
- Generické kombinované vyjádření úrovně rizika:

  úroveň rizika = F(pravděpodobnost útoku) × F´(dopad útoku)

- Do úvahy se bere jak dopad relevantního útoku, tak i pravděpodobnost realizace/uplatnění hrozby (útoku)
- Velmi významné riziko se staví na roveň velkému dopadu a velké pravděpodobnosti výskytu relevantního útoku
- Nevýznamné riziko se staví na roveň malému dopadu a malé pravděpodobnosti výskytu relevantního útoku

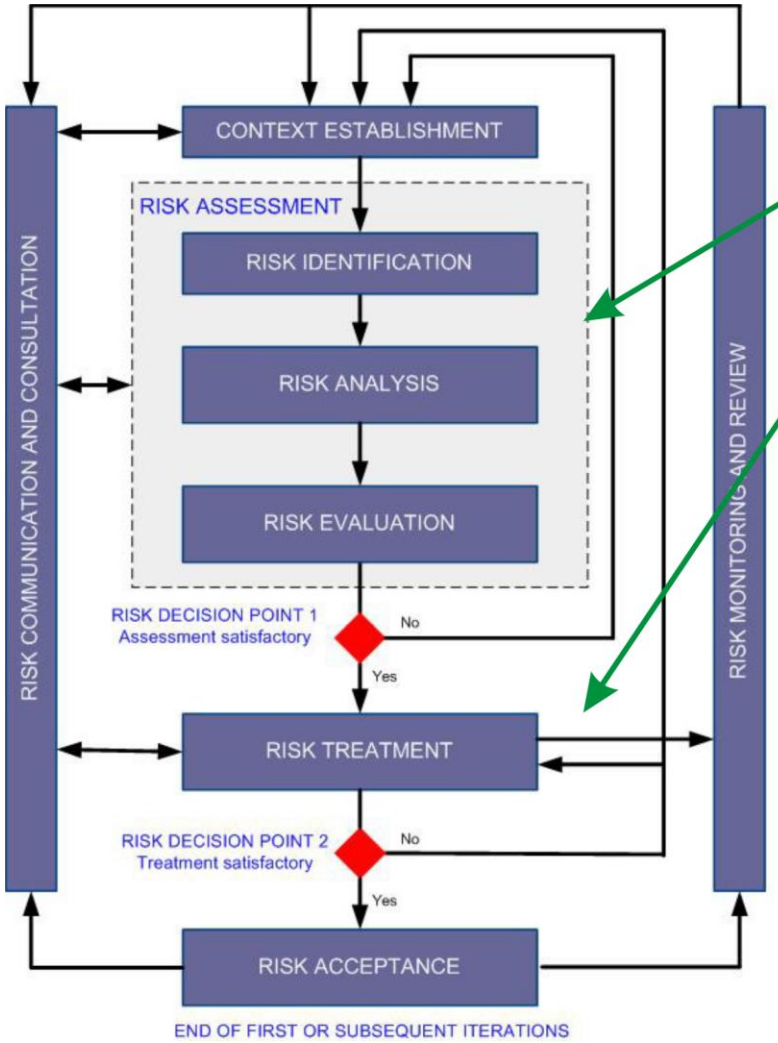
Zvládání rizik

- Rizika se zvládají volbou a uplatňováním vhodných opatření
- Abychom riziko zvládli, tj. eliminovali ho nebo snížili jeho úroveň, musíme ho nejprve ohodnotit, tj. identifikovat a poté analyzovat a vyhodnotit (určit jeho úroveň)
  - Vynakládání velkých nákladů na zavedení opatření chránících aktiva prevencí útoků při nevýznamných rizicích není ospravedlnitelné
- Proces ohodnocení rizik usnadní např. použití **tabulky rizik aktiv** implementující relaci mezi aktivy (řádky tabulky) a faktory určujícími rizika (sloupce)
- Faktory určující riziko:
  - Hrozba, zranitelnosti, id rizika, osoba odpovědná za zvládání rizika, výše možné škody, pravděpodobnost útoku, typ útočníka …

Řízení rizik pro informační bezpečnost

- **ISO/IEC 27005: 2011, Information technology – Security techniques – Information security risk management**
- Identifikace potřeb organizace
  - Z pohledu zajištění vlastní informační bezpečnosti
  - Z pohledu vytvoření účinného (efektivního) ISMS

Procesy řízení rizik (Risk Management)



Ohodnocení rizik a zvládání rizik jsou iterativní procesy

Získala se dostatečná informace pro volbu opatření ?
Pokud ne, musí se upravit kontext
(oblast, kritéria, ...)

Mají zbytková rizika akceptovatelnou úroveň ?

Procesy řízení rizik (Risk Management)

- **Ustanovení kontextu** (*Context establishment*), stanovení oblasti, kritérií,…
- **Ohodnocení rizik** (*Risk Assessment*) tvoří podprocesy:
  - Identifikace rizik (*Risk Identification*)
  - Analýza rizik (*Risk Analysis*) - určení velikosti rizik
  - Vyhodnocení rizik (*Risk Evaluation*) - určení úrovní rizik porovnáním vůči stanoveným kritériím
- **Zvládnutí rizik** (*Risk Treatment, Risk Mitigation*) - proces modifikující rizika, výběr a implementace opatření snižujících rizika
- **Akceptace rizik** (*Risk Acceptance*) - rozhodování o přijatelnosti rizika dle stanovených kritérií
- **Informování o rizicích** (*Risk Communication*) - sdělení informace o rizicích všem, kdo může rizika ovlivnit či být riziky ovlivněn
- **Monitorování a přezkoumávání rizik** (*Risk Monitoring and Review*) a procesu řízení rizik

Cíle dílčích procesů řízení rizik 1/5

- **Ustanovení kontextu**
  - Vymezení účelu provedení řízení rizik
  - Vymezení spravované oblasti a jejích hranic
  - Zajištění zdrojů (ekonomických, profesních) pro řízení rizik
  - Stanovení kritérií pro vyhodnocení dopadů útoků, úrovní rizik, akceptovatelnosti rizik
  - Stanovení organizačního zajištění a odpovědnostních rolí za řízení rizik

Cíle dílčích procesů řízení rizik 2/5

- **Ohodnocení rizik**
  - Aktiva jsou vystavená hrozbám, hrozby jsou dané existencí útočníků a zranitelnosti, některé útoky jsou pravděpodobnější než jiné, každý útok může mít větší či menší dopad
  - Ohodnocení rizik identifikuje všechny tyto aspekty pro každou hrozbu
  - Jde o získání informací pro účinné určení/volbu opatření potřebných ke změně rizik na přijatelnou úroveň pomocí procesů
    - **Identifikace rizik**
    - **Analýza rizik** - určení velikosti rizik
    - **Vyhodnocení, evaluace rizik** porovnáním vůči stanoveným kritériím
  - Výstupem ohodnocení rizik je
    - Prioritně řazený **seznam ohodnocených rizik**, řazený podle kritérií hodnocení rizik
    - **Prohlášení o aplikovatelnosti** (*Statement of Aplicability)*, vhodných opatření řešících snižování/eliminaci ohodnocených rizik

Cíle dílčích procesů řízení rizik 3/5

- **Zvládnutí rizik**
  - Rizika pro InfoSec organizace lze zvládnout až když jsou identifikovaná, analyzovaná a posouzená rizika pro důvěrnost, integritu a dostupnost informačních aktiv organizace
  - Definuje se **plán zvládání rizik**, který má čtyři související cíle:
    - Určí rizika, která se eliminují
      - Než stavět protipovodňovou hráz, raději serverovnu přemístit na kopec
    - Určí rizika, která nelze eliminovat a sníží se na akceptovatelnou úroveň (zvládnou se) implementací určených opatření
    - Určí tolerovaná rizika, pro která se po zvážení odmítla opatření, která by je udržovala na akceptovatelné úrovni, akceptovatelná rizika
      - Zabudování nákladů na škodní řízení do byznys modelu
    - Určí rizika, která se přenesou smluvně nebo pojištěním na jinou organizaci
      - Řešení sdílením nákladů na škodní řízení

Cíle dílčích procesů řízení rizik 4/5

- **Akceptace rizik**
  - Odsouhlasení plánu zvládání rizika soupisu akceptovatelných rizik managementem organizace

Cíle dílčích procesů řízení rizik 5/5

- **Informování o rizicích**
  - Sdělování výsledků řízení rizik managementu a zaměstnancům
  - Následuje implementace zvolených opatření a zabudování jejich prosazování do procesů organizace
- **Monitorování a přezkoumávání rizik a procesu řízení rizik**
  - Rizika nejsou statická
    - Odhalování změn v kontextu, v rizicích, ve faktorech ovlivňujících úrovně rizik, …
    - Při běžné činnosti organizace

Vzorové ukázky podpůrných materiálů…

- …naleznete na stránkách NUKIB https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

HODNOCENÍ RIZIK													
ID	Aktivum	Hodnota dopadu - dostupnost	Hodnota dopadu - důvěrnost	Hodnota dopadu - integrita	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupn	Hodnota rizika - důvěrnc	Hodnota rizika - integrit	Způsob zvládání rizika	Komentář
R43	PO26: Serverovna	3	Nerelevantní	Nerelevantní	Z8: Nedostatečná ochrana aktiv	4	služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	24	Nerelevantní	Nerelevantní	Redukce	oblasti, jedna serverovna (ministerstvo nemá žádnou záložní), blesk/požár
R44	PO26: Serverovna	3	Nerelevantní	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H2: Poškození nebo selhání technického nebo programového vybavení	2	24	Nerelevantní	24	Redukce	skladování hořlavého materiálu v serverovně
R45	PO27: Areál	3	Nerelevantní	Nerelevantní	Z8: Nedostatečná ochrana aktiv	2	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	12	Nerelevantní	Nerelevantní	Akceptace	přírodní katastrofy - požár, záplavy, zemětřesení atd.
R46	PO27: Areál	3	3	3	Z3: Nedostatečná ochrana perimetru	2	H6: Narušení fyzické bezpečnosti	3	18	18	18	Sledování	
R47	PO28: Kabeláž	3	3	3	Z8: Nedostatečná ochrana aktiv	3	H12: Zneužití vnitřních prostředků, sabotáž	2	18	18	18	Sledování	volně přístupné kabely/rozvodny
R48	PO28: Kabeláž	3	3	3	Z8: Nedostatečná ochrana aktiv	3	H11: Pochybení ze strany zaměstnanců a administrátorů	3	27	27	27	Sledování	
R49	PO28: Kabeláž	3	Nerelevantní	3	Z2: Zastaralost aktiv	1	H2: Poškození nebo selhání technického nebo programového vybavení	1	3	Nerelevantní	3	Akceptace	odejdou staré kabely/vadný kus, infrastruktura stará 20 let
R50	PO31: Dodavatel B	3	Nerelevantní	Nerelevantní	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	3	36	Nerelevantní	Nerelevantní	Redukce	stará smlouva - nedostatečné SLA, v případě mimořádné události vypadne důležitá služba, starší smlouva než u dodavatele A
R51	PO31: Dodavatel B	3	2	3	Z7: Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	H5: Působení škodlivého kódu (například viry, spyware, trojské koně)	2	24	16	24	Redukce	dodavatel by měl aktualizovat HW/SW, ale neděllá to tak často, jak by měl - nemáme to ve smlouvě

Typická chybná prohlášení

- „Musíme odstranit všechna rizika…“
- „Nasadíme firewall a antivir (resp. dosaď libovolný nástroj) a jsme v bezpečí…“
- „Tak, systém máme dodělaný, teď tam musíme nějak dodělat tu sekjuritu…“

Politika informační bezpečnosti

Řízení informační bezpečnosti PV017

Kamil Malinka
(využity materiály Doc. Staudka a konzultace Prof. Matyáše)
Verze: podzim 2024

Politika informační bezpečnosti

- **Politika** - pravidla řídící dosažení cílů určenými způsoby
- Politics vs. policy
  - *A policy is a deliberate system of principles to guide decisions and achieve rational outcomes*
  - *A policy is a statement of intent, and is implemented as a procedure or protocol.*

Hierarchie bezpečnostních politik

- Pro oblasti bezpečnosti organizace mají být politiky organizovány hierarchicky
- Na nejvyšší úrovni je **bezpečnostní politika organizace**
  - Souhrn bezpečnostních zásad a předpisů, množina pravidel definujících správu a ochranu aktiv organizace
  - Definuje způsob zabezpečení organizace jako celku
  - Od fyzické ostrahy, přes ochranu soukromí, přes bezpečné plnění cílů činnosti organizace až po ochranu lidských práv
- **Bezpečnostní politika organizace** je podporována řadou dalších specifických politik, mj.
  - Politikou informační bezpečnosti, zásady, pravidla zajištění InfoSec
  - Politikou ISMS, zásady, pravidla chování ISMS
  - Politikou uchování kontinuity činnosti, *Business Continuity Plan*

Politika informační bezpečnosti a politika ISMS

- **Politka InfoSec** - co proti čemu chránit
- **Politika ISMS** - jak navrhovat, vyvíjet, provozovat a hodnotit procesy plnící politiku InfoSec
- ISO/IEC 27001 (standard ISMS) žádá, aby organizace měla jak politiku ISMS tak i politiku informační bezpečnosti
  - Konkrétní vztah mezi těmito politikami nestanovuje, politiku ISMS žádá ISO/IEC 27001, politiku InfoSec ISO/IEC 27002
  - Obě mohou být vytvořeny jako doplňující se politiky, politika ISMS může být podřízena politice InfoSec nebo politika InfoSec může být podřízena politice ISMS

Politika informační bezpečnosti (IT Security Policy, InfoSec)

- Má vyhovovat celkové bezpečnostní politice organizace
- Definuje bezpečné používání IT v rámci organizace
- Stanovuje koncepci informační bezpečnosti organizace v horizontu 5-10 let
- Stanovuje co jsou citlivá informační aktiva, jejich klasifikaci a odpovědnosti za jejich stav
- Stanovuje bezpečnostní infrastrukturu organizace
  - Nutná je nezávislost výkonných a kontrolních rolí
- Definuje třídu (sílu) útočníků, vůči kterým se informace organizace zabezpečují
- Je nezávislá na konkrétně použitých IT

Systémová bezpečnostní politika

- Také bezpečnostní politika IS, systémová bezpečnostní politika, …
- Podle ISO/IEC 27000 - **Plán zvládání rizik**
  - Detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v oblasti vymezené systémem pro zpracování informací organizace
  - Specifikace bezpečnostních opatření, způsobu jejich implementace a určení způsobů jejich použití zaručujících přiměřenou bezpečnost
  - Musí splňovat politiku informační bezpečnosti organizace
  - Musí respektovat konkrétně použité IT
  - Určuje způsob zabezpečení informací v daném systému v horizontu 2–5 let , tj. definuje
    - Konkrétní cíle co se proti čemu chrání
    - Konkrétní opatření
    - Použité mechanismy pro implementaci opatření
    - Obsahuje havarijní plán a plány činnosti po útocích

Bezpečnostní procedury (postupy), role

- Připomínka z popisu dokumentace systému Provozní procedury
  - Popisy (krok po kroku) jak se systém provozuje v konkrétní organizaci
  - Kdo je odpovědný za provedení jednotlivých úkolů, …
- Složitost a rozsah procedur je daná stupněm potřebné interakce lidského činitele se systémem a požadavky na záruku spolehlivosti, důvěryhodnosti, …
- Typické role osob vystupujících v bezpečnostních procedurách
  - Chief Security Officer (CSO) - manažer, který je odpovědný za fyzickou, informační i personální bezpečnost v organizaci
  - Chief Information Security Officer (CISO) - manažer, který je odpovědný za informační bezpečnost v organizaci
  - Security architect, bezpečnostní architekt
  - Security manager, bezpečnostní správce,
    resp. Security officer, bezpečnostní administrátor/úředník
  - Operátor, správce, administrátor systému
  - Auditor, nezávislá osoba na exekutivě bezpečnosti

Modelový příklad bezpečnostní politiky

- Deklarovaná bezpečnostní politika při výuce nepovoluje podvod opsáním domácí úlohy (plagiát)
- Politikou stanovený bezpečný stav (bezpečnostní cíl) - nikdo nevlastní kopii domácí úlohy jiného studenta
- Studenti si uchovávají své domácí práce na školním počítači
- Alice soubor se svou domácí úlohou neoznačí jako chráněný proti čtení jinou osobou
- Bob úlohu opíše
- Kdo se choval v rozporu s bezpečnostní politikou ?
  - Alice ?? Bob ?? oba ?

Modelový příklad bezpečnostní politiky

- Odpověď - bezpečnostní politiku nedodržel pouze Bob
  - Politika zakazuje opisování domácích úloh
  - Bob opisoval
  - Systém se dostal do jiného než bezpečného stavu, Bob vlastní kopii Aliciny úlohy
- Alice si svoji domácí úlohu nechránila proti čtení
- To ale bezpečnostní politika to nepožadovala
- Alice nijak nenarušila definovanou bezpečnostní politiku
- Pokud by politika studentům předepisovala povinnost chránit své domácí úlohy před opsáním, pak by Alice bezpečnostní politiku porušila

Tvorba politiky informační bezpečnosti

- Definice politik InfoSec a ISMS je 1. krok při budování ISMS
  - Tvorba politiky je obvykle iterativní proces
  - Finální verze politiky musí odrážet výsledek **ohodnocení rizik** daný obsahem **prohlášení o aplikovatelnosti** (specifikace vhodných opatření) - dokument vzniklý jako výsledek ohodnocení rizik
- Politika je konceptuální dokument, který má
  - Respektovat charakteristiky činností, lokalit a aktiv organizace a technologií použitých organizací pro zpracování informací
  - Definovat systém stanovení cílů a strategií řízení organizace a rizik
  - Ustanovit kontext, ve kterém bude působit
  - Ustanovit kritéria pro evaluaci rizik a strukturu procesu hodnocení rizik
- Politika musí být
  - Schválená vedením organizace
  - Pravidelně přezkoumávaná (např. ročně) a aktualizovaná

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Deklarace politiky informační bezpečnosti**
  - Maximální rozsah 2 až 5 stran A4
  - Odpovědi na klíčové otázky „Pro koho?“ „Kde?“ „Co?“ „Proč?“
  - Deklaruje vrcholový management, podepisuje „šéf“ organizace
- **Pro koho** bude politika informační bezpečnosti závazná?
  - Odpovědnost za politiku (za každou revizi) má vrcholový management, musí existovat důkaz, že tomu tak je - zápisy z vedení, …
  - Vrcholový management/řídicí výbor musí zvážit a vymezit dopad politiky na konkrétní okruhy zaměstnanců, zákazníků, dodavatelů, … vč. přínosů/negativ pro byznys, …
  - Vytvářená politika má být maximálně srozumitelná, úplná (samostatně použitelný dokument) a evidentní (nezpochybnitelná), aby se v průběhu implementace nemusely opakovaně odsouhlasovat všechny dílčí alternativy politiky

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Kde** bude oblast působnosti politiky informační bezpečnosti?
  - Nutno přesně vymezit podle organizačního řádu / geograficky / funkčně / …
  - Špatně se prosazuje politika v oblasti, která nepodléhá jednotnému řízení
  - Mnohdy nestačí jednostranné vymezení např. na bázi organizační struktury či geografické lokality, do oblasti musí být zahrnuty všechny související kritické funkce
- **Co** politika informační bezpečnosti chrání ?
  - Specifikace informačních aktiv pokrytých politikou
  - Specifikace relevantních rysů bezpečnosti chráněných aktiv (důvěrnost, integrita, dostupnost)
  - Stanovení kritérií pro akceptování rizik a identifikace úrovně akceptovatelného rizika

Tvorba politiky informační bezpečnosti, iniciální dokument

- **Proč** se politika informační bezpečnosti zavádí ?
  - Srozumitelné vyjádření podstaty hrozeb pro organizaci
  - Srozumitelné vyjádření výše škod způsobených narušením bezpečnosti informací (ve finančních i nefinančních pojmech)
  - Ilustrační příklady důsledků incidentů podporující zavedení ISMS

- Tak, jak jsou následně získávané dílčí výsledky z hodnocení rizik, se deklarace politiky informační bezpečnosti může rozšiřovat a upřesňovat

Deklarace politiky informační bezpečnosti, šablona - příklad

- Vedení organizace ….. provozující činnost v oblasti ….. , umístěné v ….. , se rozhodlo chránit důvěrnost, integritu a dostupnost všech svých relevantních fyzických a elektronických informatických aktiv
- Cílem ochran je udržení dobrého stavu konkurenčních výhod, hotovostních toků, ziskovosti, vyhovění zákonným a smluvním omezením a zachování dobré pověsti organizace.
- Cíle ochran, požadavky na informace a na bezpečnost informací budou vyhovovat cílům organizace v oblasti stanovených politikou informační bezpečnosti a jako zmocňovací mechanismus pro sdílení informací v elektronických operacích, pro e-komerci a pro redukci rizik vázaných na zpracování informací na akceptovatelnou úroveň se použije systém řízení informační bezpečnosti (ISMS).
- Zaměstnanci organizace činí v oblasti ….. jsou povinni plnit požadavky bezpečnostní politiky a ISMS, který tuto politiku implementuje. Totéž platí pro třetí strany definované v ISMS.
- Tato politika bude přezkoumávaná alespoň jednou ročně.
- Odpovědností za bezpečnostní politiku a ISMS je pověřen odbor …..

Politiky a systém řízení informační bezpečnosti

- Většina organizací vytváří **politiku informační bezpečnosti** podle standardu ISO/IEC 27002
  - Politika správy informační bezpečnosti založená na řízení rizik
  - Použití standardu ISO/IEC 27002 byl věnovaný vesměs dosavadní obsah
- Důvěryhodná bezpečnostní politika zpracování informací je **základní kámen systému řízení informační bezpečnosti** (*Information Security Management System*, ISMS).

Zdroje informací pro tvorbu politiky informační bezpečnosti

- Zdroje návodů k postupu budování politiky informační bezpečnosti a ISMS v prostředí IS0 27000
  - http://www.itil.cz/ , ITIL - IT Governance
  - http://www.iso27001security.com/html/iso27000.html

Příklady z praxe

- Viz annexes.zip

- Používají se dva koncepty:
  - Jeden velký všeobjímající dokument (Annex A)
  - „Deštník“ – zastřešující dokument, pod kterým je mnoho dalších, menších, konkrétněji zaměřených (Annex B.1 – B.6)

Legislativa informační bezpečnosti

Řízení informační bezpečnosti PV017

Pavel Loutocký

Verze: podzim 2024

Dodatek

Tvorba politiky informační bezpečnosti 1/3

- Politika informační bezpečnosti má pokrývat/obsahovat:
  - Prohlášení, že vedení organizace bude podporovat ISMS a periodicky přezkoumávat politiku informační bezpečnosti
  - Nástin přístupu k řízení rizik (určení metodiky)
  - Kritéria evaluace (vyhodnocení) rizik
  - Strukturu procesu ohodnocení rizik
  - Kdo bude za ohodnocení rizik odpovědný
  - Stručnou identifikaci požadavků na soubory opatření zajišťujících vyhovění politice, např.
    - plán(y) reakcí na incidenty,
    - plán zachování činností,
    - plán zálohování dat,
    - plán ochran před viry,
    - politika řízení přístupu,
    - zpravodajství o bezpečnostních incidentech, …

pokrač .

Tvorba politiky informační bezpečnosti 2/3

pokrač.

- Srozumitelnou deklaraci toho, že požadavky na informace a bezpečnost informací budou vyhovovat cílům organizace a že relevantní ISMS bude předmětem trvalého vylepšování.
- Jasné vyjádření, že všichni zaměstnanci budou podrobováni školení a trénování v bezpečnostním uvědomění a specialisté budou absolvovat specializovaná školení.
- Ideálně by politika měla deklarovat vyhovění standardu ISO/IEC 27002 (tj. prohlášení, že se uplatňují standardní opatření), případně by politika měla deklarovat cíl získat certifikátu ISO/IEC 27001 (tj. certifikátu, že se uplatňují validní procesy ISMS).

Tvorba politiky informační bezpečnosti 3/3

- Náklady na budování politiky InfoSec
  - Vedení organizace má požadovat doložení návrhu politiky
    - Odhadem ceny vybudování ISMS a zdrojů pro vybudování ISMS
    - Hodnocením a kvantifikací potenciálních zisků
    - Návrhem plánu implementace a odpovědnosti za implementaci
- Monitorování postupu budování politiky InfoSec
  - Klíčové okamžiky pro přezkoumání postupu tvorby politiky jsou
    - Vypracování návrhu **Prohlášení o aplikovatelnosti** (specifikace vhodných opatření) v rámci ohodnocování rizik
    - Implementace iniciální sestavy procedur aplikujících opatření identifikovaná v Prohlášení o aplikovatelnosti
    - Provedení prvního auditu ISMS
    - Následně pak ročně, v termínech pravidelného přezkoumávání ISMS, určených v politice informační bezpečnosti

12 tipů pro tvorbu politiky informační bezpečnosti 1/2

- Bezpečnostní politika je nejefektivnější, když si ji organizace napíše sama.
- Politika informační bezpečnosti by měla být klíčovým faktorem při všech rozhodnutích o činnosti organizace, není pravda, že ovlivňuje činnost pouze IT oddělení.
- Zaměstnanci musí být školení pro dodržování bezpečnostní politiky.
- Bezpečnostní politika nebude organizaci chránit před všemi možnými hrozbami.
- Účinná bezpečnostní politika je bezpečnostní politika, která se trvale aktualizuje a reviduje.

12 tipů pro tvorbu politiky informační bezpečnosti 2/2

- Bezpečnostní politika má zahrnovat sledování výkonu.
- Co nemůžete obhájit/dokázat u soudu, není ani spolehlivé ani užitečné pro bezpečnost.
- Všichni musí dodržovat bezpečnostní politiky nebo čelit důsledkům.
- Účinnost a přijatelnost bezpečnosti jsou dva neoddělitelné faktory.
- Bezpečnostní politika musí být jasná, čtivá, srozumitelná.
- Předpisy a dosažení souladu s nimi jsou nutná zla.
- Když jste na pochybách, konzultujte standardy.