VŠB - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

doc. Ing. Pavel Šenovský, Ph.D.

Šablony systému řízení bezpečnosti informací

samostatná příloha skript Bezpečnost informačních systémů

Ostrava, 2026

Šablony systému řízení bezpečnosti informací
tento text neprošel jazykovou úpravou

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Úvod **5**

1 Typologie předpisů a dalších dokumentů v SŘBI **7**

2 Rozsah SŘBI **9**
2.1 Východiska k určení rozsahu SŘBI . . . 9
2.2 Šablona Rozsahu SŘBI . . . 9
2.2.1 Prohlášení o rozsahu . . . 9
2.2.2 Hranice a kontext organizace . . . 9
2.2.3 Vyloučení . . . 10
2.2.4 Relevantní informační aktiva . . . 10
2.2.5 Zákonné a smluvní požadavky . . . 10

3 Politika SŘBI **11**
3.1 Východiska k zpracování Politiky SŘBI . . . 11
3.2 Šablona Politiky SŘBI . . . 11
3.2.1 Úvod . . . 11
3.2.2 Slovník pojmů . . . 12
3.2.3 Cíle politiky . . . 12
3.2.4 Organizace informační bezpečnosti . . . 12
3.2.5 Management aktiv . . . 14
3.2.6 Management rizik . . . 14
3.2.7 Řízení incidentů . . . 14
3.2.8 Inspirace pro další procesy . . . 14
3.2.9 Revize a závěrečná ustanovení . . . 15

4 Management aktiv **17**
4.1 Východiska procesu . . . 17
4.2 Šablona managementu aktiv . . . 17
4.2.1 Úvod . . . 17
4.2.2 Slovník pojmů . . . 17
4.2.3 Organizace . . . 18
4.2.4 stať předpisu <- pouze technický název v rámci šablony, nepoužívejte jej v předpisech . . . 18
4.2.5 Metodika určování aktiv . . . 18
4.2.6 Metodika hodnocení aktiv . . . 19
4.2.7 Revize a závěrečná ustanovení . . . 19

5 Management rizik **21**
5.1 Východiska procesu . . . 21
5.2 Šablona managementu rizik . . . 23
5.2.1 Úvod . . . 23
5.2.2 Slovník pojmů . . . 23
5.2.3 Kontext řízení rizik . . . 23
5.2.4 Identifikace rizik . . . 23
5.2.5 Analýza a hodnocení rizik . . . 23

5.2.6 Postoj k riziku 23
5.2.7 Monitoring a přezkum 24
5.2.8 Komunikace rizik 24

6 Plán na zvládání rizik (RTP) 25

7 Prohlášení o použitelnosti (SoA) 27

8 Bezpečnostní politiky 29

Seznam zkratek 31

Úvod

Tento text vznikl jako pokus o zlepšení výsledků studentů při zpracovávání semestrálních projektů implementujících jednotlivé předpisy v systému řízení bezpečnosti informací (Systém řízení bezpečnosti informací (SŘBI)). Tento dokument je potřeba považovat za doplněk skript do předmětů:

- Počítačové sítě a ochrana dat (Politika SŘBI)
- Bezpečnost informačních systémů (všechny šablony předpisů)

Upozornění: tento text skripta nenahrazuje, neobsahuje žádnou teorii. Doporučený postup je ideálně absolvovat přednášku, popř. i cvičení zaměřené na daný typ předpisu, projít patřičnou pasáž skript a pak teprve studovat šablony poskytované tímto dokumentem.

Dále znovu zdůrazňuji (jako ve skriptech), že systém SŘBI se vždy dělá na klíč, organizace, která tento systém implementuje. Šablonu jako takovou proto NENÍ možné převzít i s „chlupama“! Vždy je nutné s nimi extenzivně pracovat a přizpůsobovat je tak, aby v prostředí organizace byly funkční. V tom je rozdíl proti některým jiným systémům řízení, jako třeba PO nebo BOZP, kde sice u předpisů je také potřeba určitého přizpůsobení, ale obsah předpisů je dán striktně legislativně a tak struktura a z větší části také obsah mohou mezi různými organizacemi zůstat v zásadě zachovány.

Druhým problémem je paradoxně u studentů přesný opak výše uvedeného. Někteří studenti tak chybně vyvozují, že pokud vlastně neexistuje úplně jednotná struktura předpisů a odpovídající šablona, lze do jednotlivých předpisů dávat vlastně všechno. Toto ale také není pravda. Vždy je potřeba zachovat:

- základní filozofii předpisu - řešíme vždy bezpečnost informací, použité technologie, hrozby apod. jsou napříč organizacemi podobné a pak logicky naše přístupy k jejich řešení také.
- základní osnova zůstává také, v zásadě stejná
- základní role mají ustálené názvy - ty chceme držet - jednak tím trefujeme požadavky legislativy, jednak pro pokrytí potřebujeme vytvořit pracovní pozice vyžadující určitou pracovní náplň. Budeme pak hledat jednodušeji pracovní sílu pro obsazení těchto pozic (nebo interně do těchto pozic postupně dovzdělávat stávající zaměstnance).

Šablony tak obsahují spíše komentář k předpokládanému obsahu jednotlivých předpisů, než formulace, které lze využívat přímo v politikách/předpisech.

Kapitola 1

Typologie předpisů a dalších dokumentů v SŘBI

Jaké tedy předpisy a jiné dokumenty v rámci systému SŘBI vedeme?

1. Rozsah SŘBI
2. **Politika SŘBI**
3. **Management aktiv**
4. **Management rizik**
5. Risk Treament Plan (Plán zvládání rizik) (RTP)
6. Statement of Applicability (Prohlášení o aplikovatelnosti) (SOA)
7. **Politiky** - politiky jsou zaměřené na informační aktiva, klíčové procesy, hrozby apod. dle potřeb organizace

Ve výše uvedeném přehledu jsou zvýrazněny typy předpisů, které jsou požadovány jako semestrální projekty v předmětu Bezpečnost informačních systémů (zpracovávány týmově). V předmětu Počítačové sítě a ochrana dat se zpracovává pouze Politika SŘBI.

Je potřeba zdůraznit, že ačkoliv v organizacích jsou obvykle zpracovávány jednotlivé předpisy samostatně, jejich hlavní efekt ve smyslu získání kontroly nad bezpečností informací zpracovávaných organizací vzniká až společným působením všech součástí tohoto systému. Jednotlivé předpisy proto musí být úzce provázány. V opačném případě budou mezi předpisy vznikat rozpory v definicích, úpravách procesů apod., což ve svém důsledku povede k obtížnější vymahatelnosti nastavených opatření.

Z hlediska strategie zpracování semestrálních projektů tak není úplně dobrou strategií snažit se zpracovávat všechny předpisy úplně najednou a zejména je odevzdávat najednou. Identifikované rozpory při hodnocení semestrálního projektu pak mohou indukovat potřebné změny také v dalších předpisech. Optimální strategií je spíše postupné zpracování. Při implementaci v praxi bychom postupovali podobným způsobem.

Tedy nejprve implementujeme Politiku SŘBI. Tato politika bývá implementována obvykle samostatně, jelikož ostatní předpisy systému SŘBI z tohoto předpisu vychází. Následně implementujeme Management aktiv a rizik, často společně, jelikož se jedná o poměrně úzce propojené oblasti, šlo by možná říci, že se jedná o dvě strany téže mince.

Politiky samotné pak mohou být zpracovány v libovolném pořadí. Pro všechny platí, že úzce vycházejí z Politiky SŘBI a výstupů procesů managementu rizik, především pak SOA a RTP. Vzájemná závislost/provázanost mezi těmito politikami pak sice může být přítomna, ale není to tak časté. Důvodem je, že obvykle chceme řešit související problémy na jednom místě a řešení tak nerozdrobovat do samostatných předpisů. Takové rozdrobení mimo jiné zhoršuje naši schopnost proškolování zaměstnanců apod.

Kapitola 2

Rozsah SŘBI

2.1 Východiska k určení rozsahu SŘBI

Základní dokument systému SŘBI, který popisuje, co bude tímto systémem řízeno (co je předmětem jeho zájmu). Rozsah obvykle stanovujeme jako první předpis v systému SŘBI. Jedná se obvykle o velmi krátký předpis, který odpovídá na základní otázky:

- jaké procesy a služby jsou předmětem našeho zájmu
- identifikace primárních informačních aktivech
- koho se systém týká
- a na jaké lokality

SŘBI může být zaveden na organizaci jako celek a všechny její aktivity, což by z pohledu bezpečnosti informací dávalo dobrý smysl, ale organizace se může rozhodnout jinak a zavést SŘBI pouze určité organizační jednotky (útvary, divize, v případě vysokých škol výzkumné ústavy, fakulty, ...). Může se rozhodnout také pro lokalizovanou ochranu např. vymezením budovy nebo patra budovy, nebo určitých vymezených místností, kde jsou zpracovávány citlivé údaje (např. realizován výzkum, analyzovány data, ...).

Informace, které potřebujeme chránit jsou zpracovávány primárními informačními aktivy. Pro účely určení rozsahu je obvykle potřebujeme určit, resp. udělat si alespoň základní představu, kterou později rozšíříme v rámci systému implementací procesů Managementu aktiv. V této fázi postupujeme tak obecně jak je to jen možné.

Primární aktiva jsou obvykle provozována prostřednictví podpůrných aktiv. Podpůrná aktiva ale v rámci rozsahu obvykle pouze shrneme formulacemi jako *... a podpůrná aktiva, pomocí kterých je provozujeme.*

SŘBI se může týkat všech zaměstnanců, pokud ale tento systém nepokrývá celou organizaci, bude se jednat spíše o podmnožinu zaměstnanců.

Výše uvedené otázky nám vedou ke stanovení rozsahu

2.2 Šablona Rozsahu SŘBI

2.2.1 Prohlášení o rozsahu

Stručný, jasný odstavec definující, co SŘBI pokrývá (služby, produkty, procesy ... jinými slovy primární informační aktiva).

Příklad: Systém řízení bezpečnosti informací společnosti ABCD, a.s. se vztahuje na všechny procesy a systémy, které zpracovávají informace o zákaznících společnosti, dále pak procesy personalistiky, výzkumu a vývoje produktů.

2.2.2 Hranice a kontext organizace

Vymezení fyzických, organizačních a technologických hranic. Pokud hranice nejsou, má být pokryta tedy celá organizace, pak je to potřeba specifikovat také.

- **Organizační jednotky**: Která oddělení, útvary, divize, fakulty apod. jsou zahrnuty

- **Fyzické lokality**: Kanceláře, datová centra, budovy, pobočky, ...
- **Technologie a systémy**: Konkrétní aplikace a informační systémy, infrastruktura, Cloud (Software as a Service (Saas), Infrastructure as a Service (Iaas))
- **Procesy**: Výzkum a vývoj, zákaznická podpora, personalistika, finance, apod.
- **Rozhraní a závislosti**: Propojení s třetími stranami (partneři, dodavatelé)

2.2.3 Vyloučení

Opak prvních dvou částí rozsahu, tentokrát postupujeme negativně, tedy ve smyslu, co není součástí SŘBI. Tuto část je potřeba je potřeba definovat pouze pro ty součásti organizace, které by se jinak vlezly do hranic/kontextu tohoto systému. Pokud tedy specifikujeme, že SŘBI se vztahuje pouze na určitý útvar (v hranicích systému), v části vyloučení ostatní útvary už nevylučujeme.

Vyloučené oblasti by měly být zdůvodněny tak, aby v budoucnu bylo možné rozhodnutí o vyloučení přehodnotit, tedy jestli důvod vyloučení trvá.

2.2.4 Relevantní informační aktiva

Přehled primárních aktiv, které má SŘBI chránit.

2.2.5 Zákonné a smluvní požadavky

Výčet legislativy a smluv, kterým systém SŘBI **musí** vyhovět. To musí interpretujeme liberálně ve smyslu musí, protože tím plní povinnost stanovenou legislativou. Požadavky na SŘBI si ale organizace může stanovovat také pro pokrytí interních potřeb organizace.

Typicky se může jednat o:

- Zákon 264/2025 Sb. o kybernetické bezpečnosti (Zákon o kybernetické bezpečnosti (ZKB)) + jeho prováděcí vyhláška 409/2025 Sb. (vyšší režim povinností ... dále v textu označováno jako Vyhláška o kybernetické bezpečnosti (VKB)) nebo 410/2025 Sb. (nižší režim povinností)
- Zákon 110/2019 Sb. o zpracování osobních údajů
- smlouvy s klienty, dodavateli, ...
- ISO 27001:2022
- apod.

Pokud SŘBI má vyhovět zákonu, pak je potřeba specifikovat také patřičnou prováděcí vyhlášku. Tímto způsobem se organizace hlásí k režimu vyšších nebo nižších požadavků, kterým musí vyhovět.

Ochrana osobních údajů může, ale pozor nemusí být součástí SŘBI. Obě rozhodnutí mají své zdůvodnění. Důvodem pro může být, že osobní informace bude potřeba chránit obdobným způsobem jako jiné citlivé informace. Pokud tedy implementujeme systém ochrany informací může být výhodné jím řešit také ochranu osobních údajů. Naopak důvodem proti rozhodnutí zařadit ochranu osobních údajů do tohoto systému může být, že ochranu těchto informací už organizace v minulosti uspokojivě vyřešila a proto nemá potřebu se k této otázce vracet.

Organizace podle toho, co přesně potřebuje chránit může být vázána libovolnou kombinací výše uvedeného (nebo také jiná legislativa, normy nebo naopak nic z tohoto).

Kapitola 3

Politika SŘBI

3.1 Východiska k zpracování Politiky SŘBI

Tato politika představuje základní předpis systému SŘBI, který definuje způsob, jakým je tento systém organizován. Politiku vytváříme na základě Rozsahu SŘBI. Informace z rozsahu se využívají extenzivně už v úvodu, kde se organizace hlásí k řízení bezpečnosti informací a specifikuje, koho se systém týká stejně jako legislativu/normy, na základě kterých je implementován.

Oproti rozsahu, Politika systému je předpisem, který již vytváří vymahatelná opatření, ustanovuje procesy a organizační struktury, které umožní celému systému fungovat. Jelikož je ale tato politika vrcholovým předpisem činí tak spíše v obecné rovině. Předpokládá se přitom, že v systému budou existovat specializované předpisy, které budou v Politice SŘBI nastavené procesy podrobně řešit. Pro proces je tak v Politice nastavována obvykle jen základní účel a manažerskou odpovědnost za tento proces.

Některé organizace spojují Rozsah a Politiku SŘBI do jednoho předpisu. Příkladem tohoto přístupu je třeba Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti, resp. jeho Příloha č. 3: Politika systému řízení - bezpečnosti informací (vzor), která je dostupná ve formátu [docx].

Tento postup ale nedoporučujeme. Je vždy lepší mít v řídící systému menší, jasně zaměřené předpisy, které úplně řeší určitou problematiku. Takový systém se také následně lépe udržuje.

Z jiných příkladů, ze kterých bychom se mohli inspirovat, je možno zmínit např. také Vrcholovou bezpečnostní politiku systému řízení bezpečnosti informací Ministerstva průmyslu a obchodu (MPO) ke stažení ve formátu [docx]. Tato politika sice také propojuje Rozsah a Politiku systému SŘBI, ale má lépe zpracované bezpečnostní role systému.

Svůj vzor Politiky SŘBI má také Svaz měst a obcí: také ve formátu [docx]. Tato politika je celkem dobře zpracována - obsahuje základní strukturu systému řízení bezpečnosti informací, včetně ustanovení základní rolí, ale bez nastavení procesů. Politika MPO také nemá samostatně řešené procesy, ale jednotlivé role jsou v ní specifikovány mnohem podrobněji až na úroveň procesů. Což je jedna z cest, kterou lze přijmout.

Zkusme tedy výše uvedené shrnout do koherentní šablony takové Politiky

3.2 Šablona Politiky SŘBI

3.2.1 Úvod

Filozoficky vychází z Rozsahu SŘBI. Úvod obsahuje především:

- přihlášení se společnosti k řízení bezpečnosti informací v organizaci nebo její části. Tato část je někdy zpracováváno formou závazku vedení.
- specifikace okruhu osob, kterých se politika resp. SŘBI týká
- podle čeho je Politika zpracována - ve smyslu zákonných a smluvních požadavků, norem apod. - opět viz Rozsah SŘBI

Forma může být různá. Může se jednat o běžný odstavcový text nebo jednotlivé části mohou být rozděleny do samostatných podkapitol podle toho, jak formálně potřebuje daná organizace postupovat.

Pozor způsob jakým úvod napíšete bude mít dopad na celkovou kompozici předpisu. Např. pokud SŘBI má pokrýt také přístup smluvních partnerů, tedy externích subjektů, k chráněným informacím. V úvodu uvedeme, např. že ustanovení politiky: *... jsou povinná pro zaměstnance společnosti a externí subjekty s jakýmkoliv přístupem k ...* [chráněným informacím]. Tento požadavek nám ale ovlivní také obsah politiky v stati politiky, protože budeme muset tuto vymahatelnost vynutit smluvně. Text politiky pak musí tento požadavek zohlednit.

Dalším příkladem mohou být legislativní požadavky. Pokud se např. přihlásíme k požadavkům zákona o kybernetické bezpečnosti v režimu vyšších povinností bude to mít přímé dopady na existenci konkrétních bezpečnostních rolí a organizačních struktur.

3.2.2 Slovník pojmů

Pro zajištění pochopitelnosti a vymahatelnosti politiky je potřeba nadefinovat některé pojmy. Vybíráme takové pojmy, u kterých předpokládáme, že by je osoby, které se mají Politikou řídit neznají, nebo takové, které mohou být vykládány výrazně odlišným způsobem, což by mohlo následně omezit naši schopnost vymáhat ustanovení Politiky z důvodu nejednoznačnosti jejích požadavků.

Použité pojmy **musí** být použity v Politice. Slovník pojmů tedy není univerzálně použitý napříč všemi politikami nebo jinými předpisy systému řízení bezpečnosti informací nebo dokonce celkového systému řízení organizace.

Formálně je slovník pojmů obvykle realizován jako seznam, tedy formou odrážek nebo číslovaný seznamu. Pro lepší čitelnost pak vysvětlovaný pojem obvykle zvýrazňujeme tučným písmem nebo kurzívou. Vysvětlení pojmu samotné by mělo být stručné a mělo by se týkat pouze pojmu. Seznam samotný pak řadíme obvykle podle abecedy.,

V rámci slovníku pojmů naopak nevytváříme žádné požadavky, organizační struktury, procesy - toto si ponecháváme na stať předpisu.

Vybrané pojmy, které se v politikách objevují často:

- bezpečnostní incident
- bezpečnostní událost
- informační aktivum
- systém řízení bezpečnosti informací
- Confidentiality, Integrity and Avalilability (Důvěrnost, integrita a dostupnost) (CIA)

3.2.3 Cíle politiky

Základní cíle systému SŘBI se jsou obvykle odvozovány z bezpečnostní triády CIA - Confidentiality (důvěrnost), Integrity (integrita) a Availability (dostupnost), které charakterizují bezpečné použití informací v rámci organizace. Tato triáda je také základem bezpečnostních požadavků ZKB a jeho prováděcích předpisů.

Kromě nich ale organizace si může stanovit libovolné množství dalších cílů, které hodlá implementací SŘBI dosáhnout. Zde hodně závisí na tom, jak byl nastaven Rozsah SŘBI.

3.2.4 Organizace informační bezpečnosti

Tato sekce Politiky obsahuje organizační struktury, bezpečnostní role a ostatní role které plní nějakou úlohu v SŘBI. Jako základ úvah o obsahu sekce politiky bereme VKB v režimu vyšších povinností, popisující základ plnohodnotného SŘBI.

Organizace, které tomuto režimu nepodléhají pak mohou vyjít z těchto rolí a organizačních struktur a upravit si je vzhledem ke svým potřebám.

Bezpečnostní role:

- Manažer kybernetické bezpečnosti (VKB §5 odst. 1)
- Architekt kybernetické bezpečnosti (VKB §5 odst. 2)
- garant aktiva (VKB §5 odst. 3)
- auditor kybernetické bezpečnosti (VKB §5 odst. 4)

Pro Manažera KB studenti mají tendenci používat jiné názvy, zejména pak Manažer ISMS nebo Manažer SŘBI - toto označení je ale jednoznačně chybné! Úloha Manažera KB je totiž širší než pouze správa SŘBI. Označení manažer informační bezpečnosti nebo manažer bezpečnosti informací

je o něco lepší a pokud organizace nespadá pod ZKB, může být přijatelné. Reálně, ale pro odlišné pojmenování není důvod. Manažer KB je ustálené označení role, které má oporu v legislativě a s ustálenými požadavky na odbornost včetně případných certifikací apod. Neexistuje tedy dobrý důvod, proč bychom měli znovu vymýšlet kolo.

Výše uvedené role dle VKB určuje vrcholné vedení (všimněte si formulace vrcholné, nikoliv vrcholové vedení). Toto je záležitostí, se kterou studenti mají také problém. VKB v §4 říká: *Statutární orgán povinné osoby nebo jiná osoba anebo skupina osob v obdobném řídícím postavení u povinné osoby (dále jen „**vrcholné vedení**“) s ohledem na systém řízení bezpečnosti informací.* VKB tedy používá tuto definici proto, aby pokryla různé typy úřadů, firem různé velikosti a zaměření, které mohou být velmi různě vnitřně organizované z hlediska mechanismů odpovědnosti a rozhodování. Vrcholné vedení je v kontextu VKB tedy zástupný pojem, který všechny tyto situace pokrývá.

Pozor: v kontextu konkrétní organizace tato nejistota neexistuje a nemůže existovat! Rozhodování je proto vždy spojeno s konkrétní pozicí nebo organizační strukturou. Tuto je potřeba v této sekci Politiky nadefinovat a dále v textu politiky používat.

Z hlediska výkladu, zejména pokud jako zdroj inspirace používáte umělou inteligenci nebo zahraniční literaturu je také *garant aktiva*. V angličtině se tato role označuje jako asset owner a do češtiny je pak někdy překládána jako vlastník aktiva. Toto označení ale v kontextu českého překladu je nekorektní - protože evokuje, že role řeší vlastnický vztah vůči aktivu, v systému SŘBI nás ale zajímá především vztah odpovědnostní - tedy osoba, která je zodpovědná za aktivum. To je poměrně významný rozdíl.

Roli garanta aktiva také nelze nahradit rolí, administrátora, popř. technického správce aktiva a to z tohoto důvodu, že podle charakteru aktiva nemusí taková role mít smysl. Např. administrátora budou mít pouze technická aktiva, typu informační systém, databáze, atd., ale třeba budovy. V SŘBI ale potřebujeme jednu roli, kterou pokryjeme všechny typy aktiv.

Další role, které může mít smysl v SŘBI ustanovit:

- Manažer IT - může zde být odpovědnost za provoz technických aktiv, které zpracovávají informace item Manažer bezpečnosti - pokud v rámci SŘBI řešíme také některé oblasti fyzické bezpečnosti jako perimetrová ochrana, kontrola vstupu, ...
- ...
- doporučujeme také ustanovit koncového uživatele (je možno pojmenovat libovolně), jako "catch all"roli, do které spadnou všechny osoby které jsou pouze příjemci ustanovení předpisů SŘBI

Jak je to s organizačními strukturami? Původní legislativa vyhláškou 82/2018 Sb. (§6 odst. 2 a 7) pracovala s *Výborem kybernetické bezpečnosti*, jako kolektivním orgánem rozhodování, který hraje velkou úlohu v SŘBI. Nová legislativa s touto organizační strukturou nepracuje a odpovědnost dává jen a pouze do rukou managementu, zejména pak Manažerovi KB a vrcholnému vedení dané organizace. Přesto bychom doporučovali tuto organizační strukturu v politice zřídit.

Výborem lze elegantně pokrýt problematiku existence struktury řízení bezpečnosti, odpovědnosti, přidělování rolí a dohled vedení tak, jak je požadováno ISO 27001 ... pokud je výbor správně nastaven. Výbor může také schvalovat předpisy v systému SŘBI apod.

Další organizační struktury, které mohou, ale nemusí být implementovány v kontextu organizace:

- **Computer Security Incident Response Team (CSIRT)/Computer Emergency Response Team (CERT) tým** - reakce na incidenty. Tento tým by pro střední a velké organizace měl být implementován.
- komise pro řízení rizik - pokud tuto činnost nevykonává výbor KB
- Změnový výbor - pro řízení změn v IT (právě změny (nebo jejich absence :-) jsou častou příčinou bezpečnostních incidentů)
- dodavatelský výbor - z důvodu řízení bezpečnosti dodavatelů
- výbor pro kontinuitu a obnovu - pokud je řízení kontinuity v rámci organizace formálně implementováno
- Výbor pro datovou a informační správu - pokud organizace má formálně implementován systém data governance
- případně další podle toho, co organizace vykonává, jaké systémy řízení má implementovány a jaké cíle si v oblasti bezpečnosti informací klade.

Role a organizační struktury definujeme vždy v kontextu systému SŘBI. Proto pokud třeba definujeme roli generálního ředitele, tak nás nezajímá obecné postavení ředitele v organizaci (že organizuje a řídí a je v důsledku odpovědný za vše), ale co specifického vykována v SŘBI.

U rolí se často specifikují také přímo procesy, za které daná role zodpovídá. V případě, že definujete text těchto odpovědností dostatečně podrobně, může být dostatečný i z hlediska nastavení základních procesů tohoto systému. Z hlediska přehlednosti ale toto doporučuji řešit spíše samostatně.

Tento názor vychází z duálního možného použití Politiky. Jeden pohled se na Politiku dívá optikou role - např. Manažer KB a potřebou zjistit, za co zodpovídám. V takovém případě budu odpovědi hledat v sekci organizace bezpečnosti. Co ale, když mám spíše otázku o tom, jak je nastaven z pohledu bezpečnosti určitý klíčový proces? V takovém případě je výhodou, pokud takový proces bude mít samostatnou sekci, kterou následně uživatel bude snadněji hledat než v případě, že informace bude ukryta v někde v textu.

Následující sekce šablony obsahují vybrané procesy s krátkým komentářem, které často v Politikách SŘBI vídáme.

Řešení těchto procesů v Politice SŘBI je obvykle velmi obecné, ve smyslu nastavení základního cíle procesu a odpovědnosti za jeho realizaci namapovanou na role, které jsme určili v této sekci Politiky. Úmyslně se vyhýbáme implementačním detailům, protože předpokládáme, že budou existovat další předpisy, které daný proces vyřeší podrobně. Takový předpis může být v textu odkázán a to i v případě, že dosud reálně neexistuje (nebyl sepsán, nebo byl sepsán ale nebyl schválen a není tudíž platný).

V takovém případě se řídíme principem *policy first*, tedy ustanovení politiky je závazné. Pokud se odvolává na neexistující dokument, pak se očividně jedná o rozpor, který bude při revizích identifikován a pokud je správně nastaven Plan, Do, Check, Act cyklus (PDCA) cyklus, měla by existence odkazu vynutit vznik chybějícího předpisu nebo revize Politiky a odstranění tohoto požadavku.

3.2.5 Management aktiv

Pro získání kontroly nad bezpečností informací v organizaci musí daná organizace nejprve získat kontrolu nad tím, jaká aktiva vlastně pro zpracování informací využívá. Základním cílem procesu je identifikovat aktiva a jejich garanty.

Manažerskou odpovědnost za proces (garantovat proces) může Manažer IT (nejčastěji) nebo Manažer KB.

3.2.6 Management rizik

Vychází z managementu aktiv, zejména pak soupisu informačních aktiv a informací poskytovaných garanty těchto aktiv. Základním cílem procesu je identifikovat míru rizika identifikovaných aktiv a přijmout rozhodnutí (RTP, často schvaluje Výbor KB) o způsobu jejich zvládnutí. jedná se o periodickou aktivitu. Tedy postoj k riziku je periodicky přehodnocován.

Manažerskou odpovědnost za proces obvykle nese manažer KB.

Při zpracování této sekce textu politiky dbejte na to, aby jste nezaměňovali management rizik a analýzu rizik. Analýza rizik je relativně malou částí celkového systému managementu rizik. Pozor, toto je častá chyba.

3.2.7 Řízení incidentů

Z textu by mělo vyplynout že bezpečnostní události je potřeba detekovat a bezpečnostní incidenty je potřeba řešit. Za řešení incidentu je odpovědný garant aktiva. CSIRT/CERT tým (pokud jej organizace má zřízen) pak detekuje a poskytuje garantovi podporu při zvládnutí incidentu.

Manažerskou odpovědnost za proces jako takový (ale ne nutně za zvládání jednotlivých incidentů!) nese manažer KB.

3.2.8 Inspirace pro další procesy

Pro případné další procesy se lze inspirovat VKB v paragrafech 9+:

- Řízení dodavatelů (§9)
- bezpečnost lidských zdrojů (§10)
- řízení změn (§11)
- akvizice, vývoj a údržba (§12)
- řízení přístupu (§13)
- řízení kontinuity činností (§15)

- **audit** (§16)

Jako nejzajímavější a nejčastější je *audit*, který v Politikách SŘBI se objevuje také velmi často. Ostatní procesy se přímo v Politice SŘBI objevují spíše méně často. To neznamená, že je systém SŘBI neřeší, pouze to, že je neřeší ve svém vrcholovém předpisu. Pro každý z těchto procesů musí být pak následně zpracován samostatný předpis, který proces plnohodnotně ustanoví a dá do souladu s požadavky na bezpečnost informací dané organizace.

3.2.9 Revize a závěrečná ustanovení

Pro politiku SŘBI je potřeba nastavit interval revizí. Obvyklý interval je 1 - 2 roky. Pozor nastavený interval bude považován za základní interval revizí také pro ostatní předpisy v systému SŘBI.

Závěrečná ustanovení obsahují věci, které se do jiných částí předpisu nevlezly. U ustanovení, která zde dáváme, bychom se měli ptát, zda by logicky neměly být umístěny v jiné části politiky. Teprve, pokud si odpovíme, že ne a zároveň, že vzhledem k rozsahu nemá smysl vytvořit novou samostatnou sekci k řešení daného problému vkládáme ustanovení do závěrečných.

Závěrečná ustanovení neslouží také k tomu, abychom věci opakovali. (To je kupodivu také častou chybou studentů.)

Kapitola 4

Management aktiv

4.1 Východiska procesu

Při zpracování vycházíme z Politiky SŘBI, která definuje (velmi stručně) základní cíl procesu a vrcholovou odpovědnost za něj. Tato politika dále tento cíl rozpracovává do plnohodnotného předpisu, který upraví všechny aspekty tohoto procesu po celou dobu, kdy budou informační aktiva využívána pro zpracování chráněných informací.

Z tohoto pohledu potřebujeme především:

- identifikovat aktiva (všech typů)
- určit jejich garanty
- určit jaké informace zpracovávají
- popsat vztahy mezi aktivy
- určit způsob evidence.

Postup vypadá přímočaře, podívejme se proto přímo do navrhované šablony.

4.2 Šablona managementu aktiv

4.2.1 Úvod

Organizace stanovuje základní cíl a stručně jej zdůvodňuje. Základní cíl lze převzít z Politiky SŘBI, pokud zde byl správně určen.

Jelikož management aktiv je také předpis, musíme určit koho se týká, kdo se jím musí řídit. Množství osob v tomto případě bude výrazně nižší než v případě Politiky SŘBI. Tento předpis je zaměřen především na osobu odpovědnou za proces a garanty aktiv. Můžeme zde přidat nějakou administrativní roli, ale většinou to neděláme a tiše předpokládáme, že Manažer je odpovědný, ale samotnou práci bude realizovat prostřednictvím svých podřízených.

Východiskem pro zpracování je Politika SŘBI, mohou zde být ale další předpisy/normy. Pokud např. organizace podléhá ZKB a podléhá vyšší formě regulace, pak je potřeba odkázat §7 vyhlášky VKB, která nám pak zároveň specifikuje, co potřebujeme předpisem vyřešit. To nám může posloužit jako osnova statě předpisu.

Než se ale do ní pustíme je potřeba nastavit pojmy a celý proces zorganizovat.

4.2.2 Slovník pojmů

Pojmy volíme dle potřeby předpisu. Obvykle je potřeba vysvětlit minimálně:

- podpůrné aktivum
- primární aktivum
- technické aktivum
- garant aktiva
- ...

4.2.3 Organizace

Podobně jako v případě Politiky SŘBI i zde použijeme role a organizační struktury, které mají být aktivní v procesu. Musí zde být minimálně:

- role odpovědná za proces (obvykle Manažer IT nebo Manažer KB)
- garant aktiva
- Architekt KB - protože je autorem celkového konceptu KB organizace, který tím pádem přímo vede na identifikaci aktiv
- role která schvaluje seznamy aktiv - pokud už není v seznam výše. Může se jednat např. o Výbor KB
- další role dle potřeby

4.2.4 stať předpisu <- pouze technický název v rámci šablony, nepoužívejte jej v předpisech

§7 VKB specifikuje povinnosti organizace následovně:

a) stanoví metodiku pro určování aktiv,
b) stanoví metodiku pro hodnocení aktiv včetně stanovení úrovní aktiv, alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,
c) eviduje garanty aktiv podle § 4 odst. 4 písm. c),
d) hodnotí primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),
e) posuzuje při hodnocení primárních aktiv alespoň oblasti uvedené v příloze č. 1 k této vyhlášce,
f) určuje a eviduje vazby mezi aktivy, která mají vliv na bezpečnost regulované služby,
g) hodnotí podpůrná aktiva a vychází přitom zejména z určených vazeb na primární aktiva a
h) pro jednotlivé úrovně aktiv podle písmene b) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti, která obsahují alespoň
   1. přípustné způsoby používání aktiv,
   2. pravidla pro manipulaci s aktivy, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
   3. pravidla pro klasifikaci informací,
   4. pravidla pro označování aktiv,
   5. pravidla správy výměnných médií a
   6. pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 2 k této vyhlášce.

Body a) - c) a f) lze vyřešit pravděpodobně jednou sekcí předpisu *Metodika určování aktiv*.
Body d) a e) sekcí *Metodika hodnocení aktiv*.
Bod h) pak musí být řešen samostatnými předpisy/politikami. Požadované procesy jsou příliš složité na to, aby je bylo možné zrealizovat jedním předpisem nebo dokonce jeho částí.

4.2.5 Metodika určování aktiv

Obsahuje podrobnější popis toho, co je:

- primární a
- podpůrné aktivum

Technické aktivum je speciálním případem podpůrného aktiva a může být proto ošetřeno společně s ním.

Specifikujeme odpovědnost za identifikaci a hodnocení - tedy kdo identifikuje. Manažer KB/Manažer IT, architekt KB, garanti aktiv. U podpůrných aktiv aktiv by měla být jasná vazba na primární aktivum. Postup je v tomto případě takový, že máme identifikovaná primární aktiva a ptáme se, jaká další (podpůrná a podpůrná) aktiva potřebujeme k tomu, aby primární aktivum mohlo poskytovat své funkce.

Jako výstupem celého procesu je Evidence aktiv - tedy dokumentace popisující aktiva, jejich typ, garanty a vzájemné vazby. Je potřeba, aby tuto evidenci někdo vedl.

4.2.6 Metodika hodnocení aktiv

Jako vstup slouží Evidence aktiv. Hodnocení realizuje garant aktiva. Rozumí se jím hodnocení aktiva v základních rozměrech bezpečnosti tedy CIA - důvěrnosti, integrity a dostupnosti. Posuzuje se jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv. Pokud je organizace ve vyšším režimu požadavků, pak k účelu hodnocení musí použít minimálně 4-stupňovou stupnici (dostupné v příloze 1 VKB). Organizace, ale použít vlastní systém hodnocení, ovšem s tím, že úroveň zjištěných informací hodnocením musí být minimálně stejná.

V případě, že vyšší úrovni regulace nepodléhá, může způsob hodnocení volit bez omezení. Z praktického pohledu představuje výše uvedený postup představuje rozumné minimum z hlediska komplexnosti hodnocení.

Postup musí být formálně popsán (ideálně v tomto předpisu) včetně použitých stupnic tak, aby postup byl dokumentovaný a opakovatelný.

Výstupem je dokument obsahující zhodnocení aktiv - tento dokument je potřeba nějak pojmenovat, bude někde uložen ...

Upozornění k pojmenování a formě výstupů obou metodik - může být libovolná. Tedy může se jmenovat libovolně a může být realizovaná libovolně. Může se tedy jednat o tabulky např. v MS Excel, nebo se může jednat o sofistikovaný informační systém určený pro pohodlnou práci s těmito informacemi. Organizace si volí formu evidence dle svých vlastních potřeb. Pozor: tato volba bude mít významné dopady za způsob jak musí být předpis napsán.

4.2.7 Revize a závěrečná ustanovení

Filozofie je totožná s postupem v rámci Politiky SŘBI.

Kapitola 5

Management rizik

5.1 Východiska procesu

Při zpracování můžeme vyjít ze základní filozofie managementu rizik, kterou nám představuje ISO 31000, viz následující obrázek.

Tady je ale potřeba doplnit, že z ISO 31000 bereme pouze tento základní proces, pojetí (definice) rizika je v ISO 31000 a SŘBI (např. dle ISO 27005) zásadně odlišná, jelikož ISO 31000 vnímá riziko jako jakoukoliv odchylku od normální úrovně - tedy negativní nebo pozitivní, zatímco v SŘBI se soustředíme pouze na negativní odchylky.

V praxi management rizik téměř nikdy nebudujeme na zelené louce a není tomu tak ani v případě systému SŘBI. Ve skutečnosti je tento řídící systém postaven na snaze získat kontrolu nad informačním rizikem. Z tohoto pohledu do jisté míry lze třeba Politiku SŘBI a také celý Management aktiv vnímat jako nástroje, kterými určujeme celkový kontext řízení. V managementu rizik proto extenzivně pracujeme s výstupy dalších procesů, především evidencí a hodnocením aktiv.

Management rizik samotný v předpise řešíme obecně. Proces tedy musí být aplikovatelný na všechna informační rizika. Z pohledu výstupů vede v obecné rovině ke specifikaci SOA a RTP. Zvládání rizik tak z hlediska předpisu končí rozhodnutím o rizicích, tedy přijetím SŘBI.

Implementace opatření dle RTP je pak záležitostí dalších předpisů. Lze předpokládat, že opatření povedou na nutnost zavádění specializovaných politik, standardů, apod. nebo jejich úpravu.

Z hlediska analýzy rizik (prosím neplést analýzu, posuzování a management rizik, viz obr. 5.1 můžeme volit jakoukoliv metodu, je tady ale několik ale.

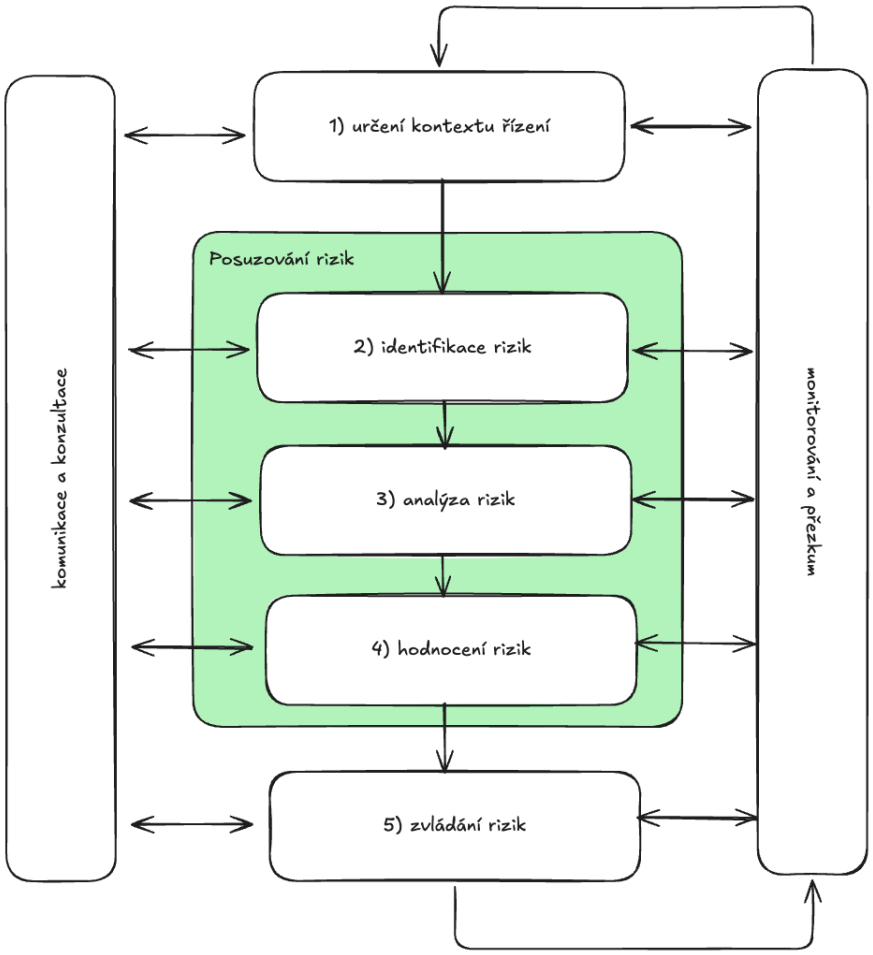
První ale je, *ale tvoříme předpis.* Dokumentace metod analýzy rizika je ale obvykle koncipována, jako obecný postup nasazení metody a odvození výsledků, případně interpretace výsledků. Jenomže předpis funguje jinak. Prostřednictvím předpisu specifikujeme kdo má co kdy a jak dělat. Jednotlivé kroky proto musí řešit časově, mapovat je na role. Pokud jsou zde nějaká dílčí rozhodnutí, musíme nastavit kdo je bude provádět atd.

Dalším ale je, *ale pokud používáme více metod analýzy rizik, musíme jejich výsledky konsolidovat.* Důvodem pro použití více metod mohou být různé vlastnosti metod, které potřebujeme využít. Např. existují metody lépe použitelné pro identifikaci rizik. V takovém případě řešíme jak různé metody budou na sebe navazovat (výstup jedné poslouží jako vstup druhé metody).

Důvodem pro použití více metod ale může být také snaha lépe pochopit určitý specifický aspekt rizika. Dobrým příkladem může být použití dobře známe a studenty relativně oblíbené metody CARVER. Tato metoda je určena pro hodnocení úmyslných antropogenních rizik a umožňuje nám dívat se na chráněný systém optikou útočníka, což může být velmi cenné. Zároveň ale nemůžeme ignorovat rizika neúmyslná a naturogenní. Abychom je zohlednili zvolíme proto také jinou metodu, řekněme FMEA (ale může být jakákoliv jiná).

Ve výsledku budeme mít naturogenení a neúmyslná antropogenní rizika hodnocená pouze pomocí FMEA, všechna ostatní pak pomocí CARVER a FMEA. Obě metody poskytují diametrálně odlišné výsledky a celý proces vede k jednomu dokumentu RTP. Potřebujeme tedy výsledky analýz sjednotit, jelikož metody samotné obvykle mechanismus pro tuto operaci neobsahují, budeme jej proto muset vyvinout sami.

Posledním ale je, *ale pokud podléháme režimu vyšší regulace dle VKB musíme vyřešit také mapování na minimální požadavky kladené touto vyhláškou.* Toto by neměl být tak velký problém. Model rizika



Obrázek 5.1: MAangement rizik dle ISO 31000

ve VKB (příloha 4) prezentovaný jako bezpečnostní minimum je:

Riziko = hodnota aktiva x hrozba x zranitelnost.

Přičemž se používají čtyř stupňové škály pro jednotlivé rozměry rizika.

Přesto tuto otázku mapování je nutno vyřešit, protože organizace musí prokázat soulad s požadavky legislativy.

Zkusme se přesunout k obsahu předpisu samotného.

5.2 Šablona managementu rizik

5.2.1 Úvod

Jako obvykle (už je to 3-tí předpis, tak už bychom si mohli zvykat) popíšeme základní motivace k realizaci této aktivity a specifikujeme okruh osob, kterých se předpis bude týkat. Podobně jako u managemenetu aktiv to nebudou všichni zaměstnanci ale především garanti aktiv a osoby, které o rizicích budou rozhodovat.

Východiska budou představovat Politika SŘBI, Management aktiv (prostřednictvím výstupů evidence a hodnocení aktiv). Odkázána může být také vyhláška VKB, pokud ji organizace podléhá.

5.2.2 Slovník pojmů

volíme dle potřeby

- pojmy z oblasti rizikologie (informační riziko, analýza rizik, management rizik, posuzování rizik)
- zvolené metody analýzy rizik
- garant aktiva
- podpůrné aktivum
- ...

5.2.3 Kontext řízení rizik

Vycházíme z Politiky SŘBI, přejímáme výstupy z Managementu aktiv, tedy evidenci aktiv a hodnocení aktiv.

5.2.4 Identifikace rizik

Identifikaci rizik realizujeme na podpůrných aktivech. Riziko se tedy na primárních aktivech neprojevuje přímo, ale právě prostřednictvím podpůrných aktiv.

Sekce obsahuje popis zvolené metody identifikace rizik. Metoda ale musí být zapracována přímo do předpisu a napsána „jazykem předpisu“. Tedy ustanovení musí být adresná, namapovaná na role a vymahatelná. Pozor toto není přirozený jazyk, jakým jsou obvykle metody popisovány.

5.2.5 Analýza a hodnocení rizik

Dále analyzujeme identifikovaná rizika. Předpis musí zdokumentovat postup tak, aby bylo zajištěno, že organizace bude schopna celý proces dlouhodobě držet a ideálně, že výsledky budou porovnatelné.

Popsány musí být všechny metody analýzy rizika včetně specifikace kdy, kterou je potřeba použít. Při použití více než jedné metody je pak potřeba popsat také postup, jak výsledky hodnocení realizovaného různými metodami konsolidovat do jednoho výstupu.

Riziko a jeho hodnocení se eviduje obvykle do Registru rizik.

5.2.6 Postoj k riziku

Ke každému zhodnocenému riziku musí organizace přijmout určitý závěr, tedy rozhodnout se, co s ním bude dělat. Portfolio strategií, které organizace může nasadit je omezené:

- akceptovat riziko - riziko je akceptováno ve své současné podobě

- ošetření rizika - organizace implementuje opatření s cílem zmenšit pravděpodobnost, že riziko nastane a nebo jeho dopad
- přenesení rizika - organizace se rozhodne přenést riziko na jiný subjekt, např. formou outsourcingu služby

Proces rozhodnutí by měl být formálně stanoven předpisem. Postoj k riziku je konsolidován v RTP, které také musí být jako celek schváleno. Schvalování provádí obvykle Výbor KB, pokud jej má organizace zřízen. Organizace ale může mít zřízenu speciální organizační strukturu (výbor) jen pro tento účel.

RTP by mělo obsahovat:

- riziko a jeho stručný popis
- aktivum, které postihuje
- garanta aktiva
- dokumentaci opatření
- termín pro realizaci
- potřebné zdroje

(Inspiraci lze také najít v šabloně RTP v textu dále.)

Poznámka - výsledek hodnocení rizik nutně nemusí odpovídat tomu, jak je sestaven RTP. Analýza rizik nám umožňuje zhodnotit informační riziko napříč organizací a seřadit je podle závažnosti. RTP by mělo dávat priority těm rizikům, které vyšly v analýzách hůře. V praxi ale nelze jednoznačně říci, že tato rizika nutně budou řešena jako první. Rozhodnutí o opatřeních je manažerské rozhodnutí, které bere v úvahu riziko jako takové, ale také např. náklady (popř. jiné zdroje), které je nutno vynaložit na realizaci daného opatření. Za určitých okolností tak organizace nemusí mít k dispozici dostatečné množství prostředků. V takovém případě se realizace opatření obvykle odkládá.

5.2.7 Monitoring a přezkum

Název je poměrně samodokumentující. Rizika by měla být dlouhodobě sledována a přehodnocována, aby organizace byla schopna zachytit jednak nová, do té doby pro organizaci neznámá rizika také změnu postoje organizace k riziku.

Studenti někdy mají tendenci přezkoumávat rizika několikrát do roka ... to je ale přehnané. V praxi i perioda 1x za rok bývá pro některé organizace problém.

5.2.8 Komunikace rizik

Měla by zajistit, že garant aktiva je informován o rizicích aktiva, které mu bylo svěřeno a opatřeních, která se jej týkají.

Kapitola 6

Plán na zvládání rizik (RTP)

Dobře zpracovaný tutoriál je v viz Cyber Arrow.

RTP je obvykle vedený tabelární formou s rizikem na každém řádku:

- ID rizika - identifikátor rizika odpovídající identifikátoru rizika v Registru rizik
- popis rizika - krátký popis rizika, např. neautorizovaný přístup k osobním údajům zaměstnanců
- vlastník rizika - osoba zodpovědná za riziko a jeho řešení
- strategie zvládnutí - akceptovat/redukovat/přenést
- kontrola - jaké kontroly jsou aplikovatelné na dané riziko, např. kontrola přístupu, MFA, ...
- opatření - popis zvoleného opatření, např. implementace multifaktorové autentizace do SSO (single-sign on) systému
- termín - specifikace data, ke kterému má být opatření dokončeno
- stav - např. v řešení/dokončeno, lze také řešit třeba procenty
- zbytkové riziko - např. nízké/střední/vysoké
- schválení - kdo přijal rozhodnutí o riziku

Ačkoliv výše uvedený seznam poskytuje dobrý strukturální rámec pro úvahy o tomto klíčovém dokumentu, není to seznam vyčerpávající. Může zde být také klasifikace významu. Mohou zde být mapovány procesy. Používané stupnice mohou být jiné apod.

Organizace si tedy přizpůsobuje podobu RTP také svým potřebám.

Kapitola 7

Prohlášení o použitelnosti (SoA)

Je klíčový dokument, který umožňuje organizaci zmapovat jakým způsobem aplikuje kontroly obsažené v příloze A ISO 27001.

Základní struktura dokumentu je:

- ID
- název kontroly
- aplikovatelné/neaplikovatelné
- jak/kde implementováno

SOA může obsahovat řadu dalších informací.

Kapitola 8

Bezpečnostní politiky

Z hlediska jedné šablony je v podstatě nemožné vytvořit jednu. Tedy alespoň tak, aby byla skutečně použitelná.

Bezpečnostní politiky jsou totiž zaměřeny na řešení konkrétního problému v systému řízení bezpečnosti informací. Běžný systém SŘBI může mít klidně implementovány desítky různých politik a každá bude jiná.

Existují šablony zpracované různými skupinami:

- Pro technické problémy existují šablony zpracované SANS institute
- Center for Internet Security má politiky pro některé své bezpečnostní kontroly
- Ministerstvo spravedlnosti Velké Británie poskytuje bezplatně šablony

Takže k obsahu Vám mohu říci - studujte dostupné šablony. Inspirujte se prací, kterou již odvedli jiní. Mějte ale vždy na paměti, že žádná z těchto šablon není použitelná bez úprav a to v tomto případě nemám na mysli, nutnost překladu šablony.

Pokud máte představu o problému, který Bezpečnostní politika má řešit, ale výše uvedené odkazy neobsahují šablonu, kterou by šlo použít jako východisko pro Vaši práci, nevěště hlavu. Výše uvedený seznam není vyčerpávající a tak existuje celá řada dalších zdrojů, které budou mít možná jiné šablony.

Na závěr ještě si dovolím zdůraznit, že pro Bezpečnostní politiky, jelikož jsou již relativně blízko technologiím platí, že pro úspěšné zpracování politiky musíte rozumět podstatě problému, který se snažíte řešit. Není proto od věci při zpracovávání spolupracovat s experty na problémovou oblast. Nemusí se přitom jednat pouze o experty na IT. V rámci bezpečnostní politik řešíme často třeba politiku sociálních médií (ta upravuje bezpečné použití sociálních sítí) ...

Dbejte na to, aby výsledkem Vaší práce byl vždy předpis. Text by proto neměl být obecný popis, ale měl by obsahovat konkrétní, vymahatelná opatření u kterých je jasné koho se týkají.

Slovník

CERT Computer Emergency Response Team.

CIA Confidentiality, Integrity and Avalilability (Důvěrnost, integrita a dostupnost).

CSIRT Computer Security Incident Response Team.

Iaas Infrastructure as a Service.

PDCA Plan, Do, Check, Act cyklus.

RTP Risk Treament Plan (Plán zvládání rizik).

Saas Software as a Service.

SOA Statement of Applicability (Prohlášení o aplikovatelnosti).

SŘBI Systém řízení bezpečnosti informací.

VKB Vyhláška o kybernetické bezpečnosti.

ZKB Zákon o kybernetické bezpečnosti.