

doc. Ing. Pavel Šenovský, Ph.D.

Bezpečnost informačních systémů

skripta
4. vydání



Bezpečnost informačních systémů

4. vydání

tento text neprošel jazykovou úpravou

©Pavel Šenovský, Ostrava, 2026

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků	6
Seznam tabulek	7
Úvod	9
1 Systémy řízení bezpečnosti informací	13
1.1 Bezpečnostní dokumentace	13
1.2 Vliv vnitropodnikové kultury na organizaci informační bezpečnosti	16
1.3 Vnitropodniková kultura vs plánování a forma bezpečnostní politiky	20
1.3.1 Vnitropodniková kultura vs plánování	20
1.3.2 Transformační vs provozní dokumentace	22
1.3.3 Formálnost vs schvalovací proces	25
1.3.4 Formálnost vs restrikce v bezpečnostní dokumentaci	26
1.4 Základní principy tvorby bezpečnostní dokumentace	28
1.5 Organizace přijímání, auditu a revize bezpečnostní dokumentace IT	31
2 ISO 27000	37
2.1 ISO 27001 – systémy ISMS	40
2.2 ISO 27002 – bezpečnostní politiky	44
2.3 Vybrané doporučené typy bezpečnostních politik a jejich obsah	49
2.4 ISO 27005 – řízení rizika	54
3 Správa informačních aktiv	63
3.1 Inventarizace aktiv	64
3.2 Management aktiv	68
3.2.1 Pořizování a správa databáze CMDB	69
3.2.2 Správa požadavků	70
3.2.3 Management změn	73
3.3 Správa licencí	73
3.4 Management zranitelností	76
4 Metody a postupy při řízení rizik IT	81
4.1 Obecný postup a odhad velikost dopadů	82
4.2 Identifikace rizik	83
4.3 Model rizika	84
4.4 BRA - Binary Risk Analysis	85
4.5 ARA - Analog Risk Assessment Method	87
4.6 NIST SP 800-30 rev. 1 - Guide for Conducting Risk Assessments	88
4.7 Poznámky k některým běžně používaným metodám analýzy rizik	89
4.7.1 CARVER	89
4.7.2 Ishikawův diagram a myšlenkové mapy	90
4.7.3 Metoda FMEA	91
4.7.4 Paretův graf	91

5	Případové studie bezpečnostní dokumentace ISMS	95
5.1	Politika ISMS	96
5.2	Organizace informací o aktivech IT	100
5.3	Bezpečnostní politika notebooků	103
6	COBIT	111
6.1	Stručná historie norem COBIT	111
6.2	Principy COBIT	113
6.3	Nástroje podpory řízení	114
6.3.1	Balance Score Cards	114
6.3.2	Domény a procesy COBIT	115
6.3.3	Matice RACI	116
6.3.4	Model dospělosti	118
7	ITIL	121
7.1	Stručná historie ITIL	122
7.2	Strategie služeb	122
7.3	Návrh služeb	123
7.4	Přechod služeb	124
7.5	Provoz služeb	125
7.6	Průběžné zlepšování služeb	125
8	Integrace forenzních technik do systému reakce na incidenty	127
8.1	Otázky integrace forenzních technik do systému ISMS	127
8.2	Forenzní proces	130
9	Řešení kontrolních otázek	133
	Literatura	144
	Seznam zkratk	147
	Rejstřík	148

Seznam obrázků

1.1	Celková koncepce bezpečnosti organizace	14
1.2	Překryv pravomocí v oblasti IT	17
1.3	Komu se zodpovídá Chief Information Officer (CIO) (data: průzkum [44])	20
1.4	Plánování v organizaci	21
1.5	Použití informačních systémů pro plánování (převzato z [77])	22
1.6	Hierarchie bezpečnostní dokumentace podle úrovně řízení	24
1.7	Proces tvorby, schvalování a revize bezpečnostní dokumentace	26
1.8	Organizační začlenění Rada pro rozvoj informačních technologií (RRIT)	33
1.9	Organizační začlenění Rada pro koordinaci a strategii ICT (RAKOS)	33
2.1	Certifikační proces Information Security Management System (ISMS) (adaptováno z [47])	41
2.2	PDCA princip	43
2.3	Proces posuzování informačního rizika (převzato z ISO 27005 [10])	59
2.4	Matice rizik	60
3.1	Deployment diagram Moodle	65
3.2	Konstrukty deployment diagramu jazyka UML	65
3.3	Vztah software – hardware a lidé	68
3.4	GUI Evolven – pohled na aktiva (převzato z [14])	69
3.5	OneCMD – screenshot (převzato z [16])	70
3.6	Jira GUI pro projekt Moodle (převzato z [58])	71
3.7	Obrazovka požadavku v Helpdesk VŠB-TU Ostrava	73
3.8	Cyklus kontroly licencí SW	75
3.9	GUI AW Caesar (převzato z [40])	76
3.10	GUI AW Caesar - Analýza SW (převzato z [40])	77
3.11	Secunia Advisory SA51202 (převzato z [18])	78
4.1	BRA - hodnocení pravděpodobnosti (převzato z [2])	86
4.2	BRA - hodnocení dopadů a rizika (převzato z [2])	87
4.3	ARA - pravděpodobnost vs dopady (převzato z [43])	88
4.4	Šablona hodnocení rizik (převzato z [61])	89
4.5	Ishikawův diagram (převzato z [51])	91
4.6	Myšlenková mapa (převzato z [22])	92
4.7	Paretův graf (převzato z [52])	93
5.1	Proces pořízení a počáteční konfigurace notebooku	108
5.2	Proces realizace změn konfigurace notebooku a bezpečnostní incident	109
5.3	Proces vyřazení notebooku z evidence	110
6.1	Evoluce COBIT (adaptováno z Garsoux [42])	112
6.2	Mapování BSC IT cílů na podnikové cíle (převzato z Garsoux [42])	115
6.3	Návaznost domén COBIT	116
6.4	Hodnocení domény COBIT (adaptováno z [46])	117
6.5	Vizualizace modelu dospělosti paprskovým grafem	119
6.6	Porovnání stavu vyspělosti procesu s konkurencí, doporučeními a cíli společnosti.	119

8.1	Základní schéma reakce na incidenty v organizaci	128
8.2	Schéma forenzního procesu (převzato z NIST SP 800-86 [49])	129

Seznam tabulek

6.1	Příklad RACI matice projektového řízení (adptováno z [25])	118
6.2	Srovnání modelu dospělosti v COBIT 4 a 5 (podle ISO 33001)	119

Úvod

Vážený studente, dostává se Vám do rukou učební text Bezpečnost informačních systémů. Tento text je především určen studentům druhého ročníku navazujícího (magisterského) studia Fakulty bezpečnostního inženýrství předmětu Bezpečnosti informačních systémů, který se vyučuje především v oboru **Bezpečnostní plánování (BPL)**, ale mohou si jej zvolit také studenti jiných oborů magisterského studia, zejména **Bezpečnostní inženýrství (BI)** nebo **Inženýrství fyzické bezpečnosti (IFB)**.

Tato skriptu se zaměřují především na oblast systémů řízení informační bezpečnosti (**ISMS**). Z tohoto pohledu tato skriptu logicky navazují na předmět *Počítačové sítě a ochrana dat*. Pokud jste tento předmět absolvovali – budete mít výhodu, protože část teorie tohoto předmětu již znáte a v tomto předmětu si své znalosti v této oblasti pouze výrazně prohloubíte a rozšíříte. Ale ani ti, kteří výše uvedené předměty neabsolvovali nemusí zoufat, protože skriptu obsahují vše potřebné k plnému pochopení probírané látky.

Možná Vás při čtení těchto řádek napadne, proč vůbec takový předmět mít, vyučovat v neinformatických oborech. Ujišťuji Vás, že vím o tom, že nejspíše nikdo z těch, kteří tyto řádky budou číst není a ani nebude „informatikem“ v klasickém pojetí. Důvodem pro zavedení předmětu byly změny ve fungování běžné společnosti, která je stále více závislá na informačních technologiích, které jsou zasíťovány a v každém okamžiku poskytují širokou škálu služeb pro jednotlivce až po nadnárodní obchodní společnosti, od aplikací pro zábavu až po kriticky důležité systémy udržující v provozu výrobní linky, elektrárny.

Pokud hodláte pracovat v oblasti bezpečnosti připravte se na to, že informační technologie Vás budou provázet do konce Vašeho profesního života. Rozdíl bude pouze úhel Vašeho pohledu na problematiku bezpečnosti IT.

Zatímco studenty IFB IT zajímá jako výhodný a efektivní nástroj pro zajištění ochrany (kamerové systémy, zabezpečovací systémy, systémy pro kontrolu vstupu, různé senzory apod.) studenti BPL spíše uvažují o možnostech řešení různých havárií, mimořádných událostí a zotavení z nich, přičemž toto zotavení v sobě nutně musí obsahovat IT složku (IT tvoří jádro fungování všech organizací bez ohledu na obor v rozvinutých státech).

Výše uvedený pohled je pouze příkladem mohli bychom najít celou řadu jiných pohledů v bezpečnostně orientovaných oborech – podstatné ale je, že všechny tyto pohledy mají jeden společný moment a to nutnost řešení procesní stránky věci. Podle čeho budeme provádět analýzy rizik, kontrolu vstupu, navrhování, ale také prosazování ochranných opatření. Právě na formulaci rámců, ve kterých taková opatření mohou fungovat se budeme zabývat.

Bylo by samozřejmě neefektivní, kdyby bylo nutné takové rámce vyvíjet úplně „na zelené louce“ pro různé společnosti, neštěstí existují standardy, které nám naši práci mohou výrazně ulehčit. V praxi se nejvíce používají standardy ISO 27 000, COBIT a ITIL. Všechny tyto tři standardy se dívají na problematiku řízení bezpečnosti z trošku jiných pohledů a proto pokrývají také jiné oblasti IT bezpečnosti. To je také důvodem proč se v těchto skriptech budeme zabývat všemi těmito standardy.

Rozsah předmětu bohužel nedovoluje probrat všechny tři standardy na úrovni podrobností, jak by si zasloužovaly, proto je všechny probereme v obecné rovině a z hlediska praktické aplikace se zaměříme na ISO 27 000, které se v podmínkách České republiky (ČR) používá přece jenom nejčastěji. Tato skriptu obsahují případové studie příkladů bezpečnostních politik, ale také dokumentace inventarizace IT aktiv a jejich rizikových analýz, které slouží jako podklad pro tvorbu těchto politik. Případové studie bezpečnostní dokumentace tvoří druhou část skriptu.

Třetí část je pak zaměřena na bezpečnostní incidenty, jejich pochopení a dokumentace. K tomuto účelu je nutné použití forenzních technik analýzy IT aktiv u nichž máme podezření na narušení bezpečnosti. I tato třetí část je zaměřena primárně na procesy a jejich nastavení v rámci organizací – nikoliv tedy forenzní analýzy použitelné např. v trestním řízení.

Pro zpestvení čtení jsem se také rozhodl zpracovat tento text formou vhodnou pro „distanční vzdělávání“ tak, aby práce s ním byla co možná nejjednodušší. Z tohoto důvodu je text jednotlivých kapitol segmentován do bloků.

Každá kapitola začíná krátkou anotací, ve které se dozvíte, o čem budeme v kapitole mluvit a proč. V bodech se pokusím shrnout, co byste po prostudování kapitoly měli znát a kolik času by Vám studium mělo zabrat. Prosím mějte na paměti, že tento časový údaj je pouze orientační, nebuďte proto smutní nebo naštvaní, když ve skutečnosti budete kapitole věnovat o něco méně nebo více času.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:



Průvodce studiem

Slouží pro seznámení studentů s látkou, která bude v kapitole probírána.



Čas nutný ke studiu

Představuje odhad doby, který budete potřebovat k prostudování celé kapitoly. Jedná se pouze o orientační odhad, neznepokojujte se proto, pokud Vám studium bude trvat o něco déle nebo budete hotovi rychleji.



Vysvětlení, definice, poznámka

U této ikony najdete vysvětlující text, poznámku k probíranému tématu, která problém uvede do širších souvislostí, popřípadě důležitou definici.



Kontrolní otázky

Na závěr každé kapitoly je zařazeno několik otázek, které prověří, zda jste problematice kapitoly dostatečně porozuměli. Pokud nebudete vědět odpověď na některou otázku, je to signál pro Vás, abyste se ke kapitole vrátili.

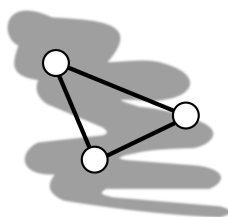


Příklad

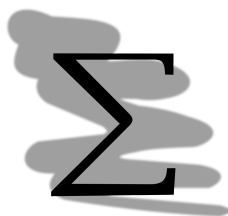
Příklady obsahují praktické demonstrace diskutovaného problému.

Systém ikon, které máte k dispozici v tomto textu není samoúčelný, měl by vám napomoci v efektivnějším studiu problematiky, která v řadě případů je pro Vás nová.

Postupujte proto postupně po jednotlivých tématech a to průběžně (pokud čtete tyto řádky poprvé na konci semestru, pak vezte, že jste nepostupovali správně). Na začátku studia každého tématu ověřte, že Vaše znalosti skutečně pokrývají minimální potřebný rozsah ke zvládnutí daného tématu. Pokud ne, je potřeba se vrátit k předchozím kapitolám nebo dokonce předmětům, kde jste patřičné znalosti

**Návaznosti**

V tomto segmentu budou zmíněny další návaznosti probíraného tématu na další témata tohoto předmětu, ale také dalších předmětů.

**Shrnutí**

Obsahuje základní myšlenky kapitoly, kterým by měl být věnována zvláštní pozornost během studia.

**Přestávka**

Po obtížné části textu, nebo prostě občas jenom tak je nutné si udělat krátkou přestávku, načerpat síly k novému studiu.

mohli (a patrně také měli :-)) vstřebat. Jinými slovy pokud nejsou vstupní předpoklady splněny nemá smysl začínat se studiem daného tématu.

Pro některá témata jsou vstupní požadavky doplňovány také informacemi o používaných softwarech nebo službách. Zde doporučení nepokračovat dále není tak silné. Pokud ale tyto požadavky už vyřešíte preventivně, budete se moci soustředit už jen na studium daného tématu. Na druhou stranu, pokud tak neučiníte, v průběhu studia narazíte dříve nebo později na daný software a sním související úkol narazíte. Budete tedy muset instalovat/zprovozňovat stejně. V tomto případě budete ale vědět co a proč děláte. rozhodnutí je proto na Vás.

Přímo v textu není velké množství úloh. Předmět *Bezpečnost informačních systémů* ale vyžaduje poměrně vysokou aktivitu ze strany Vás studentů a to jednak směrem k prezentaci Vašich názorů k řešení jednotlivých komponent systému **ISMS**, jednak budete jako součást týmu zpracovávat některé klíčové dokumenty v tomto systému řízení.

Po prvotním přečtení textu můžete mít pocit, že všemu dokonale rozumíte a přesto, se Vám třeba projekt vrátí s minimálním počtem bodů a nebo dokonce nebude přijat vůbec. Tuto zpětnou vazbu využijte konstruktivně - hledejte řešení, znovu přečtěte text, kde se probírá dané téma. Buďte aktivní a komunikativní v prezenčně konaných blocích výuky. Pokud máte problém Vy je možné, že někdo ve Vaší studijní skupině jej má také. Sledujte proto, alespoň do jisté míry, dění kolem sebe v těchto blocích. Možná tento problém některý z Vašich kolegů už vyřešil, možná jej konzultuje s vyučujícím. Nebo se svého vyučujícího zeptejte sami.

I mimo prezenčně konané bloky výuky lze řadu problémů vyřešit. Použijte diskuzní fórum předmětu, pošlete e-mail s dotazem, kontaktujte vyučujícího přes MS Teams nebo telefonicky.

Na konci Jsou také kontrolní otázky. Ty by Vám měly umožnit rychle kontrolu toho, že jste základní teoretické aspekty kapitoly pochopili. Správné odpovědi jsou doplněny na konec tohoto učebního textu, v poslední kapitole.

Kontrolní otázky ale nikdy nemají schopnost skutečně změřit Vaši úroveň znalostí. Jsou tedy určeny pouze jako jeden ze zpětnovazebních prvků, které mohou identifikovat některé oblasti pro zlepšení/doučení.

Na konci skript naleznete také rejstřík pojmů. Doporučuji, abyste jej v rámci přípravy na zkoušku prošli - zamyslete se nad tím, zda všechny pojmy, které jsem do něj zařadil, chápete a jste je schopni dát do souvislostí. Pokud ne je vedle pojmu odkaz na číslo stránky, kde je pojem probrán a Vy můžete rychle zaplnit případné mezery ve svých znalostech problematiky informačních systémů.

Přeji Vám, aby čas, který strávíte s tímto textem, byl co možná nejpříjemnější a abyste jej nepovažovali za ztracený.

doc. Ing. Pavel Šenovský, Ph.D.

Novinky v 4. vydání skript

- aktualizována skripta podle standardu na studijní opory distančního vzdělávání
- drobné opravy v celém textu
- kapitoly věnované problematice systémů řízení bezpečnosti informací byly zásadním způsobem aktualizovány

Novinky v 3. vydání skript: Třetí vydání vyšlo pouze v angličtině

Novinky v druhém vydání skript

- kapitola věnována ISO 27000 doplněna o specifikace šesti nejpoužívanějších typů bezpečnostních politik
- Doplněna kapitola o **IT Infrastructure Library (ITIL)**
- Přidána kapitola o základech provádění forenzních nástrojích a možnosti zakomponování jejich použití do systému reakce na incidenty a také systému **ISMS** jako takového

Kapitola 1

Systémy řízení bezpečnosti informací



Průvodce studiem

V rámci této kapitoly podíváme na organizaci bezpečnosti informací z hlediska organizačních opatření a základních pravidel která se jí týkají.

Po přečtení této kapitoly budete

Znát

- základní pojmy z oblasti procesní bezpečnosti informací
- souvislost mezi bezpečností a kulturou organizace
- organizační struktury s vlivem na řízení bezpečnosti informací
- souvislost mezi plánováním a bezpečností informací
- proces schvalování předpisů v systémech vnitropodnikových předpisů

Klíčová slova: systémy řízení bezpečnosti informací, SŘBI, ISMS, informační bezpečnost, kybernetická bezpečnost

Požadavky na vstupní znalosti: nejsou, pro rychlejší zvládnutí probírané problematiky ale může být prospěšné, pokud si zopakujete alespoň některá témata z *Bezpečnostní informatiky* [80], popř. *Počítačové sítě a ochrana dat* [79].



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 4 hod.

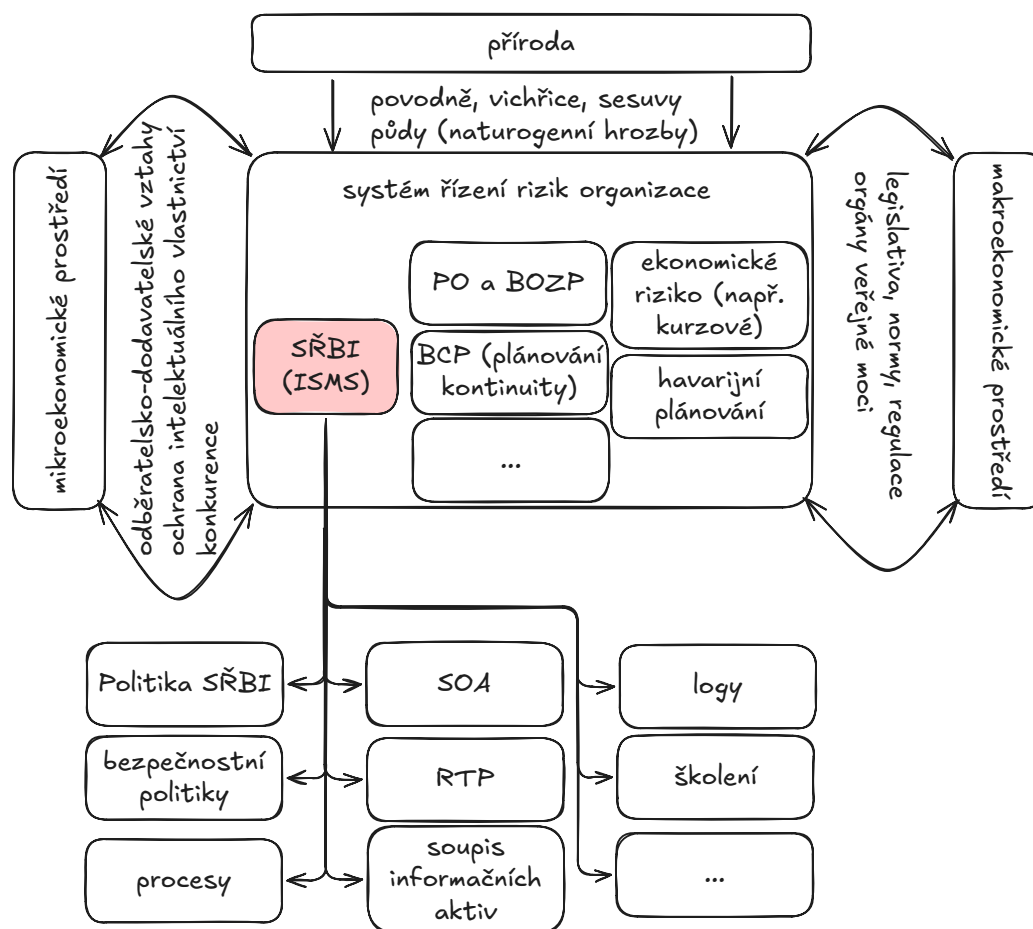
1.1 Bezpečnostní dokumentace

Nepochybně se shodneme na tom, že bezpečnostní aspekty práce s IT organizace je potřeba řídit. Je přitom lhostejné, v jakém oboru organizace působí, jestli se jedná o výrobní nebo nevýrobní podnik, nebo třeba orgán státní správy. V případě, že bezpečnostním hrozbám čelíme pouze realizací náhodně vybraných ochranných opatření a postupů, nemáme zajištěno, že úroveň bezpečnosti organizace dosahuje potřebné výše.

Jediným řešením je proto zavedení celého komplexu postupů, opatření, které jsou pevně zakotveny v bezpečnostní dokumentaci organizace a v ideálním případě jsou integrovány do celkového systému řízení organizace.

Celé prostředí, v rámci kterého organizace působí si můžeme znázornit podobně jako na obr. 1.1.

V těchto skriptech se budeme zabývat primárně bezpečností IT, nicméně je potřeba podotknout, že tuto oblast ve skutečnosti nelze úplně izolovat od běžné bezpečnosti.



Obrázek 1.1: Celková koncepce bezpečnosti organizace

Organizace svojí místní lokalizací (např. polohou poboček) je vystavena lokálním hrozbám přírodního (např. povodně) ale také antropogenního původu. Ačkoliv tyto hrozby běžně chápeme odděleně od IT, jejich souvislost s naší problematikou nelze pominout. Např. v případě, že budova s datovým centrem je v zátopové oblasti, je nutné řešit nikoliv pouze včasnou evakuaci zaměstnanců z budovy, ale také migraci datových služeb centra do bezpečné lokality, což ale nelze realizovat v krátkém časovém horizontu, pokud se s touto možností předem nepočítalo.

Výše uvedený příklad je poměrně extrémní, jelikož zátopové oblasti jsou obvykle předem známy a proto plánování a realizace datového centra v takové oblasti není příliš pravděpodobné. Lze si však představit jiné scénáře které budou mít podobné důsledky (vyřazení služeb datového centra), např. v důsledku dlouhodobého přerušení elektrické energie jako následky vichřice nebo ztráta konektivity k Internetu v důsledku přerušení páteřní sítě **Internet Service Provider (ISP)**.

Na organizaci také působí vlivy mikroekonomického a makroekonomického prostředí. Mikroekonomickým prostředím rozumíme především fungování běžného trhu ve smyslu konkurence, odběratelů a dodavatelů apod.

Z hlediska bezpečnosti nás v mikro úrovni bude zajímat především bezpečnost údajů organizace z hlediska jejich možného úniku (špionáž), bezpečnost osobních údajů zákazníků v systémech elektronických obchodů apod.

Na makro úrovni je organizace vystavena působení vlády (nebo vlád v případě nadnárodního podniku), ale také jednotlivých samospráv a jiných regulačních orgánů. Toto působení se projevuje především v nastavení legislativních požadavků na organizace. Tyto požadavky mohou být obecně platné pro všechny organizace (např. daňové zákony a z nich vyplývající povinnosti archivovat účetní podklady) nebo mohou být spojeny s výkonem určitých povinností nebo poskytováním určitých služeb (např. **poskytovatel certifikačních služeb (PCS)** s povinností certifikovat své kryptografické moduly na úroveň EAL3 (**Evaluation Assurance Level (EAL)**) podle standardu Common Criteria [3]).

Mikro a makro prostředí tedy ovlivňují pozici organizace na trhu a stanovují pravidla, podle kterých na tomto trhu bude působit. Právě toto prostředí se snažíme pro danou organizaci řídit pomocí metod řízení rizika organizace.

Součástí řízení rizik jsou samozřejmě analýzy rizika, ale také další dokumentace a plány, které by vám neměly být neznámé. Jedná se především o havarijní plány, plány kontinuity, plány obnovy, plány pro zvolené typy závažných mimořádných událostí (např. povodně) apod. Všechny tyto plány (se zvláštním důrazem na plány kontinuity) mají své vazby na IT.

Nás však v tomto předmětu (a těchto skriptech) bude zajímat především druhý nástroj pro řízení rizika organizace a to **ISMS**, v češtině se často používá pojem **Systém řízení bezpečnosti informací (SŘBI)**. Jedná se o ucelený filozofický přístup pro řízení bezpečnosti veškerých citlivých informací bez ohledu na to kde a v jaké formě se nacházejí. Formálně se jedná o další systém řízení, který organizace používá pro získání kontroly nad bezpečností zpracovávaných informací.

Předmětem našeho zájmu budou proto informační aktiva ve všech podobách. Intuitivně si v souvislosti s bezpečnostní informací představíme použití výpočetní techniky (IT), ale systém se obvykle neomezuje pouze na tuto oblast. Předmětem jeho zájmu jsou také lidé, archívy, popř. další oblasti dle zaměření a potřeb organizace.

Informačním aktivem přitom rozumíme veškeré informační systémy a další systémy, které zpracovávají informace - tzv. *primární aktiva*, a další aktiva, která zajišťují běh primárních aktiv - tzv. *podpůrná aktiva*.

Předmětem zájmu z pohledu bezpečnosti informací tak nejsou pouze klíčové informační systémy, u kterých bychom to očekávali, ale také další systémy včetně třeba budov ve kterých je např. umístěna infrastruktura, apod.

Na obr. 1.1 jsou zmíněny některé z dokumentů, které se vytvářejí při zavádění a provozu **ISMS**. Jedná se o:

1. politiku **ISMS**
2. různé procesy zpracovávající chránění informace
3. **Risk Treatment Plan (RTP)** - plán zvládnutí rizik
4. **Statement of Applicability (SOA)** - prohlášení o aplikovatelnosti
5. bezpečnostní politiky
6. zprávy z auditů
7. školení, logy a další podpůrné dokumenty
8. a řada dalších

Tento výčet však není v žádném případě úplný. Mohou zde být zařazovány další dokumenty v různé formě. Mohou to být plány na zavádění bezpečnostních opatření, plány pro fúze organizací, plány migrace informačních systémů - obecně transformační plány organizace nebo její části, které mají zohledněno bezpečnostní hledisko.

Mohou zde být dokumenty pokrývající inventarizaci IT aktiv, tedy která IT aktiva jsou ve vlastnictví organizace, kde se fyzicky nacházejí, kdo je spravuje a k jakému účelu se používají.

O tom jaké dokumenty budou ve skutečnosti součástí systému **ISMS** rozhoduje podniková kultura - tedy jakým způsobem je organizována daná společnost, ale také co přesně si od zavedení systému **ISMS** slibuje.



Kontrolní otázky: 1.1 Úvod do prostředí organizace a ISMS

1. Vysvětlete rozdíl mezi mikroekonomickým a makroekonomickým prostředím, ve kterém působí organizace.
2. Zkuste specifikovat mikroekonomické okolí zvoleného úřadu nebo jeho části (např. odbor prevence HZS ČR nebo Registr vozidel).
3. Co je to informační aktivum, uveďte alespoň tři příklady takových aktiv.
4. Zamyslete se nad tím, co je to **ISMS** a k čemu slouží.

1.2 Vliv vnitropodnikové kultury na organizaci informační bezpečnosti

Co je vlastně *vnitropodniková kultura* – rozumíme jí sadu formálních i neformálních pravidel, kterými se řídí každodenní život v dané organizaci. Nejedná se přitom pouze o klasické vnitropodnikové předpisy jako jsou např. předpisy bezpečnosti práce apod., spíše se jedná o standardy komunikace (vizuální styl korespondence, webového sídla), způsob jednání (komunikace) v pracovním kolektivu (familiérní nebo spíše formální), můžeme zde zařadit také tzv. dress code, postoje k určitým otázkám týkající se mise organizace.

Tyto, dalo by se říci, maličkosti mají z hlediska bezpečnosti překvapivě svůj význam. Znalost zvyklostí v dané organizaci může být zneužita útočником pomocí metod *sociálního inženýrství* pro kompromitaci informací v organizaci. Útočník v tomto případě zneužije přímo lidskou komponentu systému.

Vnitropodniková kultura taktéž určuje do určité míry organizační struktury, které se v dané organizaci používají. Některé společnosti využívají spíše maticové organizační struktury, zatímco jiné jsou přísně centralizované, což odpovídá stromové organizační struktuře. Ačkoliv v tomto předmětu primárně není naším záměrem zkoumání různých organizačních struktur s případnými výhodami a nevýhodami (tyto informace jste mohli získat buďto v předmětu *Základy managementu* nebo v takřka kterékoliv učebnici managementu) – zajímat nás bude spíše způsob jak bude organizování informační bezpečnost.

Existuje sice teoreticky možnost, že oblast informační bezpečnosti (nebo dokonce celé informatiky) je zcela rozpuštěna do jednotlivých útvarů organizace, ale v praxi se tento přístup, až na opravdu malé společnosti, nepoužívá. V případě takové (malé) společnosti zase nemá smysl uvažovat o plnohodnotném zavedení systému **ISMS**. Ve výkladu se proto zaměříme zejména na střední a velké společnosti/organizace, které mají alespoň do určité míry vyřešenou centralizaci svých IT služeb.

Důvodem pro minimálně střední velikost organizace je také to, že teprve středně velké podniky pro své řízení vyžadují existenci formálních pravidel, které zajistí jednotnost ve způsobu, jakým organizace řeší různé procesy a životní situace. Malé podniky lze za určitých okolností řídit i méně formálními metodami řízení.

Samostatné útvary pro správu a rozvoj IT začaly být zaváděny v 60. letech minulého století. Důvod byl především technický – nepoužívaly se PC, tak jak je známe dnes, ale terminály, které byly připojeny ke vzdálenému sálovému počítači (mainframe). Hardware byl tedy fyzicky centralizován, což si vyžádalo patřičné organizační změny vedoucí k zavádění oddělení IT (dříve v ČR označované jako VT – výpočetní technika), které se o ně staraly.

S rozvojem IT a nástupem nových technologií se naplno začaly projevovat výhody decentralizace. PC je konečně samostatně funkční stroj, se kterým přímo pracuje koncový uživatel. Rychlý vývoj v oblasti software, pak umožnil aby využití počítačů i pro plnění složitých úkolů bylo jednoduché a nevyžadovalo specializované znalosti z oboru informatiky, alespoň od koncového uživatele.

Základní mise IT útvaru se proto změnila z podpory a ošetřování IT prostředků v majetku útvaru na mnohem obecnější podporu zavádění a údržby IT aktiv do organizace. Tato transformace nebyla jednoduchá (rozdílné potřebné portfolio znalostí, setrvačnost postupů apod.), ani levná (nutnost proškolení zaměstnanců na nové technologie, implementace procesů v novém prostředí). V řadě případů transformace proběhla tak, že původní oddělení IT bylo rozpuštěno a následně byl vytvořen útvar nový, který již od počátku byl koncipován pro plnění těchto nových úkolů.

V novém pojetí jsou základní úlohy oddělení IT přibližně následující:

1. centralizace nákupu aktiv IT
2. správa některých aktiv (především servery, aktivní síťové prvky apod., *nikoliv však běžné počítače*)
3. údržba aktiv IT (opravy, reklamace)
4. proškolení a podpora koncových uživatelů při vykonávání jejich pracovní činnosti.

Všimněte si slova přibližně, které jsem uvedl v předchozím odstavci. Důvodem je opět vnitropodniková kultura – rozdílné společnosti, mohou totiž IT organizovat výrazně odlišně. Důvody pro odlišné řešení vycházejí obvykle z historie. Organizace v určitém časovém okamžiku musela řešit problém a hledala nejschůdnější cestu, jak jej vyřešit. Pro řešení se pak obvykle vytipuje součást organizace, která v dané chvíli disponuje schopností problém uspokojivě vyřešit, nebo k vybudování této schopnosti měla nejbližší.

Rozdíly v organizacích tedy vznikají postupně tak, že organizace realizuje řadu relativně malých rozhodnutí, které při dostatečně dlouhém opakování vedou k zásadním rozdílům v organizaci a to jak v organizačních strukturách, tak procesech, které pro plnění úkolů využívají.

Prakticky to znamená, že dvě totožné organizace se vlivem dílčích, v čase rozložených, rozhodnutí začínou postupně od sebe vzdalovat. Z pohledu bezpečnosti informací a systémů jejich řízení je to problém, protože to znamená, že každá organizace je jiná a systém řízení (nejen ISMS/SŘBI) se ji musí přizpůsobovat - musí být vyvinut na míru dané organizace.

Obecně lze říci, že zkušenost z provozu **ISMS** tak může být přenositelná mezi různými organizacemi. Organizace čí stejným hrozbám a možnosti jak se s nimi vypořádat jsou omezené. Tyto obecné poznatky ale musí být přizpůsobeny místním podmínkám. Velmi podobná je i situace s jinými systémy řízení, např. systémy řízení jakosti dle ISO 9000 a dalšími.

Všimněte si také, že v úkolech IT oddělení není ani slovo o bezpečnosti. Důvodem je to, že o bezpečnosti informací a jejím systematickém řešení hovoříme až v několika posledních letech. Do té doby se všeobecně předpokládalo, že k jejímu řešení postačuje pořízení, instalace a údržba antivirového software a běžná údržba IT aktiv organizace.

Tyto úlohy jsou samozřejmě z hlediska bezpečnosti IT stále důležité, zkušenosti však ukazují, že samy o sobě k zajištění zvolené úrovně bezpečnosti nepostačují a je nutné je doplnit o další nástroje, které se zaměří také na „měkkou“ složku IT tedy samotné uživatele jednotlivých systémů a způsobů, kterými jsou tyto systémy využívány, ale také spravovány.

Stále však zbývá velké množství úkolů, které spadají do oblasti bezpečnosti informací, ale nejsou pokryty IT oddělením, které jsme definovali výše. Možné řešení, co do organizace oblasti zájmů je znázorněno níže, na obr. 1.2.



Obrázek 1.2: Překryv pravomocí v oblasti IT

Pojmenování jednotlivých oddělení prosím berte s rezervou - reálné pojmenování v praxi vychází z lokálních zvyklostí dané organizace (vnitropodnikové kultury). Berte jej proto spíše jako určité nálepky, které můžeme použít pro zastřešení určitých problémových oblastí. Zájmové oblasti jsou přitom tři:

1. správa IT v klasickém pojetí
2. bezpečnost IT
3. fyzická bezpečnost (technická bezpečnost osob a majetku ve správě organizace)

Správu IT v klasickém pojetí jsme alespoň ve stručnosti probrali výše, jaké úkoly ale plní zbývající dvě oddělení. Bezpečnost IT by se mohla starat o následující problémové oblasti.

1. nástroje pro detekci a prevenci průniků (**Intruder Detection System (IDS)** a **Intruder Prevention System (IPS)** systémy)
2. správa firewallů
3. správa síťové infrastruktury (často zůstává v ve správě běžného oddělení IT)
4. vývoj a vymáhání bezpečnostních politik týkajících se IT aktiv
5. řešení bezpečnostních incidentů
6. pořizování, nasazení a údržba bezpečnostních nástrojů dle potřeb organizace

Oddělení pro technickou bezpečnost (bez ohledu jak je nazveme) se pak stará o:

1. fyzické zabezpečení objektů organizace (ostraha)
2. instalace, provoz a údržba kamerových systémů, reakce na detekované události
3. instalace, provoz a údržba zabezpečovacích systémů, reakce na události zaznamenané senzory těchto systémů
4. reakce na události detekována systémy **elektrická požární signalizace (EPS)**

5. instalace, údržba a provozování systémů na kontrolu vstupu (elektronické turnikety, čtečky karet a pod.)

Pokud má být zajištěna bezpečnost, musí být logicky zajištěny všechny tyto funkce. Situace může být také komplikovaná nákladovou optimalizací poskytovaných služeb, kdy část portfolia služeb může být outsorcována externím firmám. Charakteristiky služeb (jejich obsah, rozsah a zaručená kvalita) jsou upraveny smlouvami mezi dvěma nebo více subjekty. Organizačně je zaručení určité požadované úrovně poskytovaných služeb pak těžší.

Na organizační strukturu se můžeme dívat také z pohledu funkcí manažerů, jak jsou definovány v různých pracovních nabídkách. V této souvislosti existuje celá řada vedoucích pozic:

- **Chief Executive Officer (CEO)** - generální ředitel
- **Chief Information Security Officer (CISO)** - manažer informační bezpečnosti
- **CIO** - manažer IT
- **Chief Security Officer (CSO)** - manažer bezpečnosti
- **Chief Operation Officer (COO)** - provozní ředitel (manažer)

Manažer informační bezpečnosti je senior level pozice, která je obvykle z organizačního hlediska hodně vysoko (jedná se o tzv. C-level pozici, která je obvykle přímo podřízena **CEO**). V tomto kontextu lze také uvažovat o dalších pozicích jako je finanční ředitel **Chief Financial Officer (CFO)**, technologický ředitel **Chief Technological Officer (CTO)**, případně další manažerské pozice.

Z pohledu bezpečnosti informací je zcela nezastupitelná pouze jediná role a to je role **CEO**, který nese vždy vrcholovou odpovědnost za organizaci jako takovou a to včetně bezpečnosti informací.

Ačkoliv je manažerská odpovědnost nepřenositelná, neznamená to, že v oblasti bezpečnosti informací pracuje **CEO** sám. Pro zajištění procesů je možno delegovat pravomoc konat na existující organizační struktury, nebo pro potřeby práce vytvářet struktury nové. Tyto struktury pak budou reprezentovány vedoucími pracovníky těchto struktur (např. **CSO**, **CIO**, **CISO**, atd.).

Pokud je v organizaci ustanovena samostatná pozice **CISO** je nutné, aby v organizační struktuře měla přímý přístup k **CEO**, se kterým v otázce bezpečnosti informací musí velmi úzce spolupracovat. Z hlediska povinností může **CISO** zabezpečovat např. následující:

- informační bezpečnost a ručení za informace (**information assurance (IA)**)
- soulad s legislativními požadavky na informační bezpečnost
- řízení informačního rizika
- důvěrnost informací
- **Computer Emergency Response Team (CERT)** / **Computer Security Incident Response Team (CSIRT)**
- **identity management (IDM)** v organizaci
- Architektura bezpečnosti informací
- řešení bezpečnostních incidentů (zkoumání důkazů apod.)
- Zotavení po bezpečnostním incidentu a řízení kontinuity poskytovaných IT služeb
- **Information Security Operations Center (ISOC)**

Výše uvedená náplň práce je opět pouze orientační a v realu se bude v různých společnostech více či méně lišit. Možná několik málo slov k některým bodům.

Ručením za informace se rozumí různé postupy, které mají za cíl zaručit správnost informací, se kterými organizace pracuje.

CERT/CSIRT týmy, jsou více či méně formální týmy mající v dané organizaci za úkol detekovat a reagovat na různé druhy bezpečnostních incidentů. Prosím neplést s národními resp. vládními **CSIRT** týmy, jejichž úloha je trochu jiná (viz skript *Bezpečnostní informatika 3* [81]).

IDM rozumíme realizaci jednotného systému pro správu identit uživatelů v rámci dané organizace. Systémy **IDM** reagují na fakt, že většina různých informačních systémů se realizuje vlastní správou identit svých uživatelů, v případě, že je ale v organizaci velké množství takových systémů vedlo by vedení identit samostatně pro tyto systémy ke zvýšené složitosti údržby.

Zavedením **IDM** proto organizace buduje jedinou databázi svých uživatelů, ze které se dle potřeby přelévají údaje o jednotlivých uživateli do provozovaných systémů organizace, v potřebném rozsahu. O **IDM** jsme se již bavili také v předmětu *Počítačové sítě a ochrana dat* [79].

Operační centra **ISOC** se budují především ve velkých společnostech s tisíci počítačů. Jedná se o centrum, které sjednocuje činnosti a vylepšuje podmínky pro prevenci, detekci a zvládání bezpečnostních incidentů.

ISOC centra používají často:

- nástroje pro průzkum sítě (network discovery)
- systémy pro hodnocení zranitelností
- **Governance, Risk and Compliance (GRC)** systémy (systémy pro zajištění shody s legislativními požadavky)
- monitoring webových sídel
- skenery databází a aplikací
- systémy **IDS** a **IPS**, firewally, antiviry
- nástroje pro penetrační testování
- systémy pro management logů
- SIEM systémy (systémy pro podporu řízení bezpečnosti informací a událostí)
- UTM systém (unified threat management – sjednocené řízení hrozeb)

ISOC si je tedy možné do určité míry představit podobně jako třeba operační střediska OPIS HZS, která jsou ale zaměřena pouze na bezpečnost IT. Shromážďují se zde tedy veškeré informace potřebné k detekci bezpečnostních incidentů a jsou zde lidé, kteří tyto informace průběžně vyhodnocují a v případě nutnosti aktivují další osoby (například vlastníky jednotlivých aktiv IT zasažených bezpečnostním incidentem).

Architektura informační bezpečnosti je v případě CISO ale myšlena její praktická realizace. Pro návrh architektury organizace vytvářejí samostatnou pozici (nemanažerskou) *architekta kybernetické bezpečnosti*. Ne všechny organizace ale tuto pozici obsazují.

Pokud jsou pozice CISO a architekta kybernetické bezpečnosti obsazeny, pak se předpokládá, že se musí jednat o osoby odborně způsobilé k této práci. Pro tyto práce ale neexistuje jednotný systém certifikace. Existuje ale řada kurzů, kde může prokazatelně absolvent potřebné znalosti získat. Organizace si pak např. podmínkami výběrového řízení na obsazení pozice může přesně nastavit očekávaný odborný profil.

CIO je někdy také označován jako ředitel IT (information technology director). Jedná se tedy o vedoucího pracovníka majícího na starosti klasické IT tak jak jsme si je definovali na předchozích stránkách. Z hlediska organizační struktury, ale vnímání významu pozice **CIO** jsou výsledky průzkumu toho, komu se **CIO** zodpovídají [44]. Průzkum proběhl v roce 2010 na vzorku 729 pracovníků v pozici označované **CIO**. Pro srovnání se můžete podívat na starší výsledky z průzkumu, který proběhl v roce 2007 [45].

Zdaleka největší podíl přímé podřízenosti připadá na **CEO** (44 %) a teprve daleko za ním je podřízenost pod **CFO** (20 %).

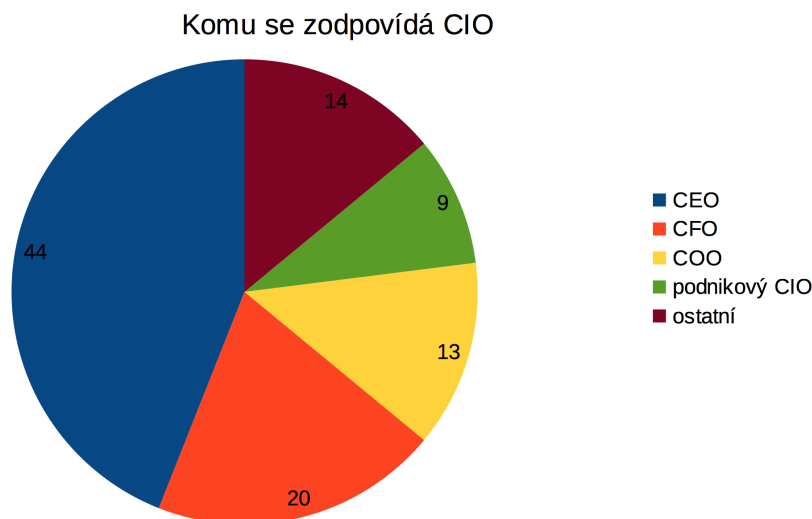
Graficky jsou podíly přímé podřízenosti znázorněny na obr. 1.3.

CSO je ředitel, který přímo zodpovídá za bezpečnost. Jedná se o osobu, která je v dané organizaci zodpovědná za vývoj, implementaci a údržbu bezpečnostní vize organizace a jejích bezpečnostních strategií a programů. **CSO** funkce je přitom zaměřena na fyzickou bezpečnost, nicméně vzhledem k tomu, že informační a fyzická bezpečnost spolu souvisí, existují případy, kdy **CSO** má na starosti zároveň také bezpečnost IT (spojení s funkcí **CISO**). Na druhou stranu funkce **CSO** a **CIO** se prakticky nepřekrývají a proto ke slučování funkcí **CIO** a **CSO** obvykle nedochází.

Vraťme se ještě k souvislosti mezi **CISO** a **CSO**. Bezpečnost IT je, pokud se jí organizace hodlá věnovat v plné šíři (což by ve vlastním zájmu měla), složitá oblast, která v sobě zahrnuje prvky z oborů informatika, technická bezpečnost, telekomunikace, ale také managementu a další. **CISO** se proto svým portfoliem znalostí adaptuje většinou buďto z řad klasických informatiků s tím, že si doplní znalosti z oblasti bezpečnosti (technická bezpečnost, management rizik), nebo naopak se adaptuje z oblasti technické bezpečnosti a logicky pak doplňuje znalosti z oblasti IT. CISO tedy není pracovní pozice pro čistého informatika.

Konečně **COO** je manažer, který je zodpovědný za běžný, každodenní, provoz organizace a jako takový nemá přímou odpovědnost za IT ať už z pohledu provozního nebo bezpečnostního. Vzhledem k tomu, že IT je v současnosti nedílnou součástí prakticky všech činností je možné s nadsázkou říci, že **COO** je závislý na funkčnosti IT a proto vyvíjí tlak na to, aby IT fungovaly tak jak mají (efektivně a zároveň bezpečně).

COO přitom není informatikem, a požadavky z tohoto hlediska nejsou „informatické“, definuje spíše jaké funkce mají mít provozované systémy a jaké mají být parametry jejich provozu.



Obrázek 1.3: Komu se zodpovídá CIO (data: průzkum [44])



Kontrolní otázky 1.2: Organizační struktura a manažerské pozice

1. Vyjmenujte jednotlivé zkratky vedoucích pozic, které mají vztah k informační bezpečnosti (alespoň 3) a zkuste si představit pracovní náplň těchto funkcí.
2. Jaký je vztah mezi CIO a CSO a proč?
3. Zkuste najít jakým způsobem je formálně organizována informační bezpečnost na VŠB-TUO a uvažujte o tom, proč tomu tak je?
4. Definujte organizaci informační bezpečnosti z hlediska jednotlivých oddělení a jejích představitelů pro svůj semestrální projekt.
5. Mohli byste se stát (někdy v budoucnu) CISO? Pokud ano, které znalosti Vám chybí, pokud ne tak proč?

1.3 Vnitropodniková kultura vs plánování a forma bezpečnostní politiky

1.3.1 Vnitropodniková kultura vs plánování

Možná Vás napadne otázka – proč bychom se vůbec v souvislosti s vnitropodnikovou kulturou a jejím vlivem na bezpečnost informací měli zabývat plánováním? Důvod je ten že plánování budoucích činností organizace je běžnou součástí fungování všech organizací bez ohledu na obor, ve kterém působí. Plánování přitom ovlivňuje budoucí směřování organizace a projeví se prakticky v dlouhodobých (strategických) plánech. Plány pak umožňují organizaci efektivně mobilizovat zdroje pro dosažení plánem stanovených cílů i pro zajištění běžných funkcí organizace.

Dlouhodobé plány tedy stanovují dlouhodobé cíle a také způsoby jejich dosažení. Výsledkem realizace dlouhodobých plánů jsou tak mohou být rozsáhlé změny v organizačních strukturách, nasazení nových technologií nebo systémů, fúze s jinou společností apod. Tyto změny s sebou nesou nutnost řešit bezpečnostní aspekty, protože každá změna s sebou může přinést také nové hrozby nebo ovlivnit zranitelnost provozovaných systémů, popř. následek předpokládané realizace hrozby. Z tohoto důvodu je potřeba všechny změny řídit také z pohledu bezpečnosti.

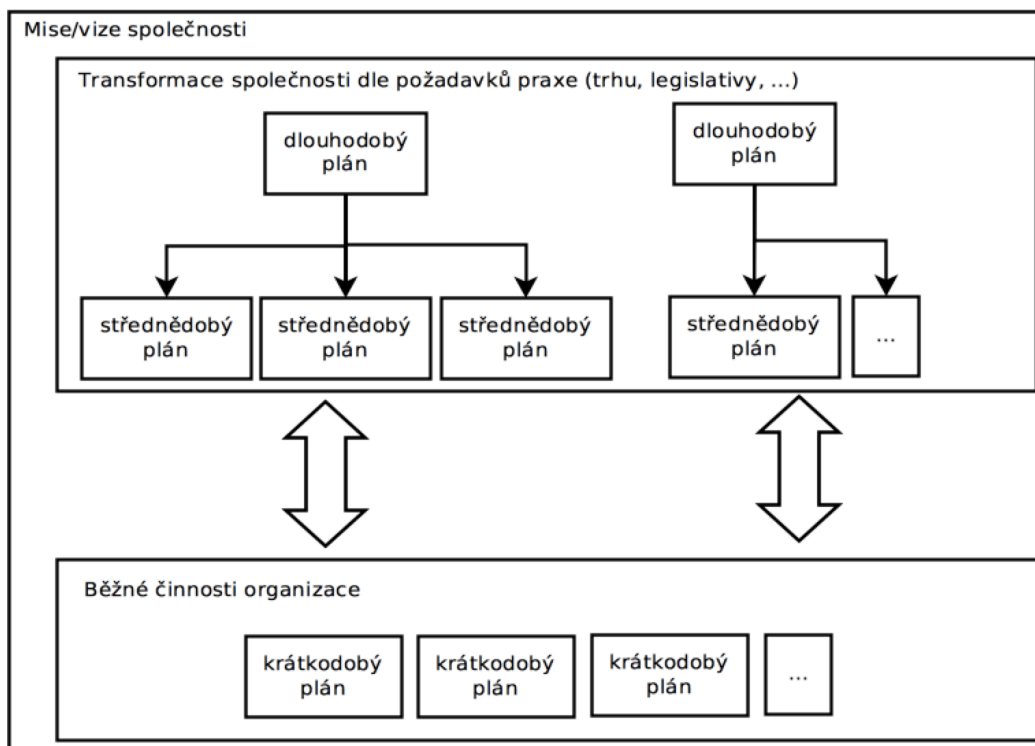
Cílem je, aby se realizací změny nebylo spojeno nepřiměřené riziko.

Z hlediska plánovacího horizontu platí, že čím jsou plány na delší dobu, tím méně jsou konkrétní/specifické. Tedy zatímco dlouhodobé plány určují pouze základní obrysy věcí budoucích, plány krátkodobé již musí být velmi konkrétní a podrobné.

Střednědobé plánování slouží jako podklad pro realizaci menších změn, ale i ty je nutné z hlediska bezpečnosti ošetřit.

Konečně krátkodobé plány slouží pro zajištění běžného fungování organizace. Pokud mají být

zajištěna funkčnost bezpečnostních řešení – musí na ně být uvolněny dostatečné zdroje (personální, finanční, apod.). Schematicky bychom si mohli představit celou situaci podobně jako na obr. 1.4.



Obrázek 1.4: Plánování v organizaci



Poznámka

Všimněte si, že plánování se neděje náhodně, ale sleduje určité základní, společné cíle, které jsou sepsány v základních dokumentech společnosti obvykle nazývaných **mise a vize**.

Účelem stanovení mise je definice samotné podstaty existence organizace, tedy proč vůbec byla zřízena, jaký účel má plnit.

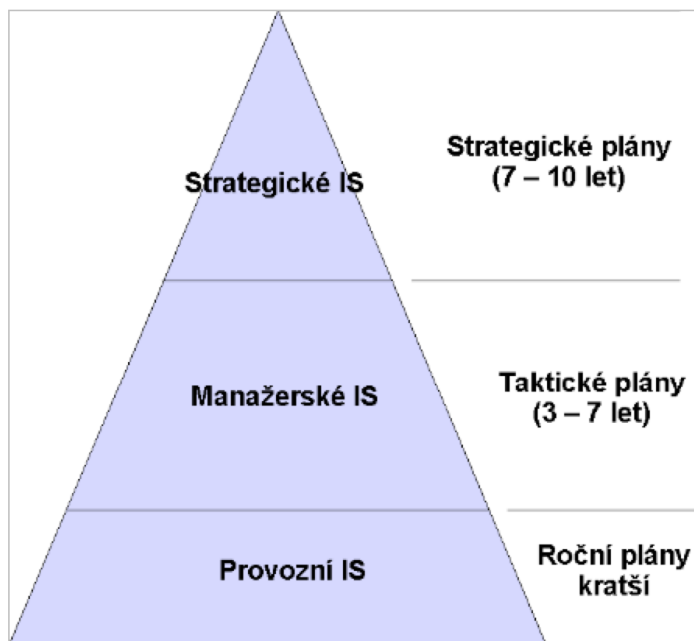
Vize oproti tomu stanovuje, kam se společnost má ubírat. Ale počkat – není toto účelem dlouhodobého plánování? Ano v obecné rovině je, vize je ale specifický dokument, který není obvykle pevně zakotven v čase a jeho formulace jsou obecné, specifikující hlavní cíl společnosti. Tím může být například: *chceme se stát leaderem v oblasti XYZ a podobné formulace*.

Z hlediska časového, tedy na jak dlouhý časový horizont je zaměřeno dlouhodobé, střednědobé a krátkodobé plánování, neexistuje jednoznačná odpověď. Plánovací horizont si jednotlivé organizace určí samy pro sebe na základě poznatků o fungování prostředí, ve kterém musí organizace působit.

Obecně platí, že plánovací horizont je delší v oborech, kde jsou inovace spojovány s nutností realizace velkých investic nebo oborů, které se z pohledu stavu poznání příliš nevyvíjí. Naopak kratší plánovací cykly budou mít firmy ve vysoce inovativních oborech, často se silnou vazbou na IT apod.

Dokonce i pojmenování jednotlivých plánů může být různé. Na obr. 1.5 níže například používám pro dlouhodobé plány pojmenování strategické, pro střednědobé taktické a pro krátkodobé roční.

Toto pojmenování odpovídá lépe zdrojům dat, které jsou potřeba pro efektivní stanovení, ale také plnění těchto plánů. Všimněte si také, že samotný časový horizont je řešen časovým intervalem. Ani hranice tohoto intervalu ale nejsou pevně zakotveny a mohou být menší nebo větší dle potřeb dané organizace.



Obrázek 1.5: Použití informačních systémů pro plánování (převzato z [77])

Kontrolní otázky: 1.3 Plánování, mise a vize



1. Vysvětlete rozdíly mezi krátkodobými a dlouhodobými plány.
2. Co je to mise a vize společnosti a jaký účel plní?
3. Co ovlivňuje nastavení délky jednotlivých plánovacích cyklů?

1.3.2 Transformační vs provozní dokumentace

Z pohledu plánování lze bezpečnost zkoumat z několika různých směrů. Plány, jelikož stanovují konkrétní činnosti, které organizace podnikne v budoucnu jsou samy o sobě cenné např. pro konkurenci a proto jsou samy o sobě předmětem ochrany (jako citlivé dokumenty). Chráněny by přitom měly být plány jak v tištěné, tak elektronické verzi.

Kromě toho, plány na delší časové úseky v sobě často obsahují transformační kroky, které je potřeba bezpečnostně ošetřit. Jednotlivé transformace, jako např. zavedení nového informačního systému, mají obvykle charakter projektu.

Připomeňme si z *Managementu* popřípadě *Modelování rozhodovacích procesů* [78] co to vlastně projekt je. Zjednodušeně se jedná o na sebe navazující sled činností, které sledují určitý společný cíl. Pro projekt je typické, že má stanoven datum počátku realizace a také datum, kdy má být projekt dokončen (cíl projektu je splněn). Zároveň jsou již před zahájením pro projekt stanovené zdroje, které budou k dispozici pro jeho řešení. Zdroji přitom rozumíme zdroje časové, personální, finanční, přenosová kapacita apod. Tyto zdroje nesmí (neměly by) být překročeny.

Projekt je tedy jednorázovou záležitostí, která se po dokončení již nebude opakovat. Oproti tomu klasický management/řízení, je ze své podstaty cyklický. Tedy opakujeme stále stejné činnosti, aplikujeme stále stejné nástroje řízení, s cílem udržet řízený systém (organizaci) v chodu a to na optimální úrovni výkonu.

Jelikož projekty mají transformační charakter, budou bezpečností opatření s nimi spojené spíše dočasného charakteru - po dobu trvání projektu nebo jeho etapy. IT v tomto ohledu není nijak výjimečné, protože podobně se postupuje v oblasti bezpečnosti obecně. Pokud např. zjistíme, že v budově není funkční zařízení EPS (nebo obecně vyhrazené požární zařízení) provozovatel objektu přijímá po dobu nefunkčnosti náhradní opatření jako např. posílení požárních hlídek apod.

V praxi lze nalézt celou řadu příkladů IT projektů:

- pořízení nového IS

- sloučení informačních a datových základů různých společností při fúzi
- zavádění nové majoritní verze informačního systému, programu nebo operačního systému, apod.
- realizace opatření vyplývajících ze změn v legislativě
- a řada dalších

V okamžiku, kdy informační aktivum přejde do běžného provozu, pak by jeho činnost z hlediska bezpečnosti měla řídit běžná provozní bezpečnostní dokumentace. Platnost této dokumentace není obvykle časově omezena, často se ale do ní napevno zavádějí revizní lhůty tak, aby byla zajištěn maximální soulad mezi v organizaci používanými informačními aktivy a bezpečnostní dokumentací, která je ošetřuje.

Dokumentaci si přitom nepředstavujte jako třeba dokumentaci software - tedy obecný popis toho, jak daný software funguje. V kontextu bezpečnosti informací máme na mysli především **politiky**. Politiky jsou schvalovány na strategické úrovni, tedy nejvyšším vedením organizace. Definují co a proč se v organizaci má dělat.

Na taktické úrovni jsou politiky rozpracovávány do podoby **směrnic**. Politiky jsou obvykle obecné, směrnice jsou naopak konkrétní.

Na taktické úrovni fungují také **metodiky**. Ty popisují jak systematicky postupovat při řešení určité agendy, postupu nebo problému. Metodiky se obvykle stanovují pro složitější, často se opakující procesy. Cílem je, aby postup, který má být použit, byl normalizován, byl dlouhodobě udržitelný na zvolené úrovni kvality a byl opakovatelný. Jako příklad můžeme uvést třeba metodiku analýzy rizik, metodika klasifikace aktiv, metodika řízení bezpečnostních incidentů, apod.

Metodika, podobně jako směrnice nebo politika, má charakter vnitropodnikového předpisu. Pro své adresáty je proto závazná.

Na operativní úrovni pak specifikujeme **postupy** a **procedury**. Tyto nám popisují přesný proces realizace určitého postupu nebo úkonu a říkájí kdo, kdy, co a jak má udělat. Příkladem může být postup zřízení uživatelského účtu, postup zálohování apod. Pokud bychom porovnali postup a metodika, pak metodika je obecnější. Postup řeší problém detailněji. Může proto platit, že na jednu metodiku bude navázáno hned několik postupů.

Pro metodiku jsme uváděli příklad metodiky analýzy rizik. Řekněme že v této metodice bychom měli specifikován obecný postup. Řekněme, že pro identifikaci rizik bychom použili metodu brainstormingu následovanou Ishikawovým diagramem. Pro samotnou analýzu rizik bychom použili třeba metody FMEA, Attack Tree a CARVER. Ve finále bychom konsolidovaly rizika do jedné matice rizik pro účely lepší komunikace rizik. Toto vše by bylo v metodice. Pro každou z výše uvedených metod bychom pak mohli vytvořit postup, který bude pro danou metodu detailně rozebírat, jak se má při jejím nasazení postupovat.

Pracovní instrukce jsou ještě detailnější než postupy. Velmi často jsou psány pro konkrétní roli nebo dokonce nástroje, které se pro daný postup využívají. Postupy a instrukce nemají charakter vnitropodnikových předpisů, představují spíše standard, popř. doporučení podle kterého se postupuje.

Jelikož se nejedná o vnitropodnikový předpis, vznikají tyto dokumenty už na úrovni jednotlivých pracovišť a nevyžadují formální schvalování ze strany vedení organizace.

Zcela mimo výše uvedenou hierarchii dokumentů pak spadají různé další dokumenty a záznamy, které bychom mohli označit jako **podpůrné**. Do této kategorie řadíme **záznamy** jako jsou logy, prezenční listiny školení, evidence informačních aktiv, bezpečnostních incidentů, apod.

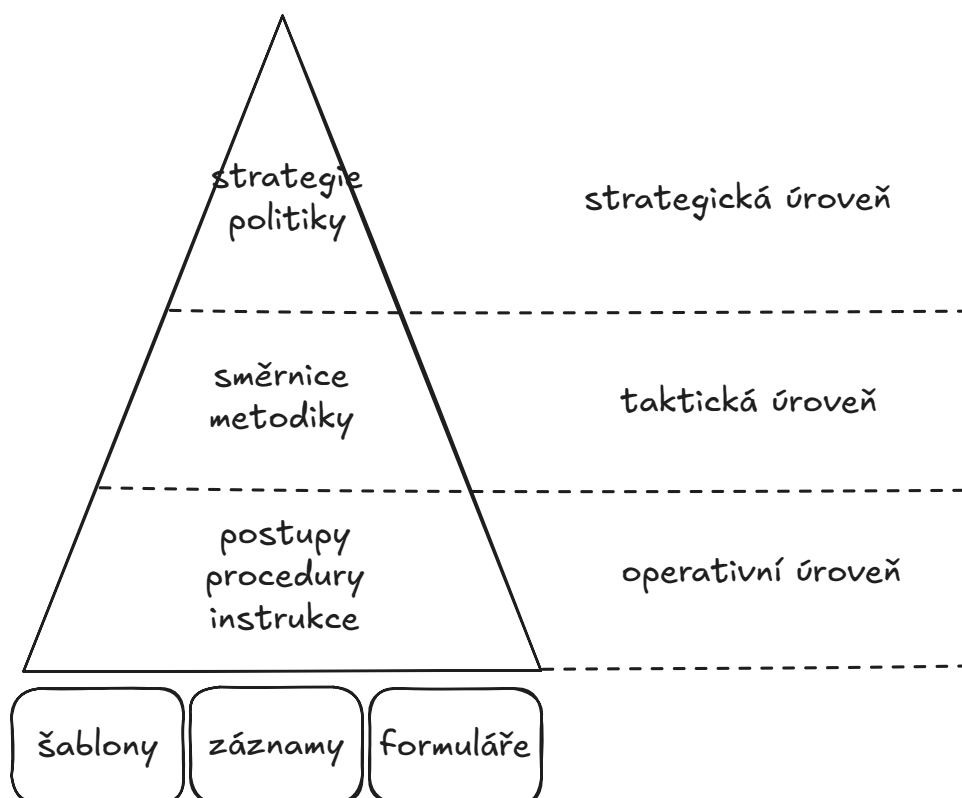
Do podpůrných dokumentů řadíme také různé formuláře a šablony, u kterých očekáváme, že budou používány při plnění úkolů vyplývajících z bezpečnostní dokumentace.

Graficky je celá hierarchie bezpečnostní dokumentace znázorněna na obr. 1.6.

Všimněte si, že výše uvedené označování dokumentů a jejich zařazení do jednotlivých úrovní řízení je pouze jedním z možných řešení tohoto problému. V anglicky psané literatuře se velmi často používá model jiný:

1. *politiky* - specifikují co a proč
2. *standards* - specifikují parametry politik
3. *procedures* - specifikují postupy
4. *návody* - podrobně řeší jak postupovat, ale nejsou závazné

ISO 27001 pak neřeší hierarchii bezpečnostní dokumentace vůbec. Norma ale používá pojem *dokumentované informace*, pro které rozlišuje zda jsou *udržované* (např. politiky, směrnice a postupy) nebo pouze *uchovávané* (např. různé záznamy, logy, apod.). Norma je v tomto ohledu úmyslně vágní, aby organizace mohla použít svůj stávající model struktury vnitropodnikových předpisů.



Obrázek 1.6: Hierarchie bezpečnostní dokumentace podle úrovně řízení

Typologie použitých předpisů, jejich pojmenování, ale také forma je závislá čistě na vnitropodnikové kultuře. Vnitropodniková kultura ovlivňuje zejména:

- pojmenování jednotlivých dokumentů
- jejich organizaci (např. v kolika dokumentech bude problém řešen - je preferován menší počet specializovaných předpisů nebo menší počet předpisů s širším zaměřením?)
- ve stanovení rolí a zodpovědnosti
- ve formálnosti dokumentace

Z hlediska pojmenování se v praxi můžete setkat s dokumenty jako je:

- Provozní řád (např. počítačové učebny)
- bezpečnostní politika
- bezpečnostní zásady použití
- provozní bezpečnostní dokumentace
- a řada dalších pojmenování

Pojmenování je tedy čistě na tvůrci dokumentu. Při pojmenování by ale vycházet z místních zvyklostí tak, aby označení dokumentu logicky zapadalo do schématu pojmenovávání dokumentů dané organizace. Konzistence ve jménech zvyšuje čitelnost dokumentu jako celku – čtenáři je již po přečtení názvu jasné o čem dokument bude.

Organizací dokumentace rozumíme především způsob jakým dokumentaci řešíme. V zásadě existují dva extrémní přístupy:

- monolitická dokumentace
- samostatný dokument na všechno

Oba tyto přístupy jsou extrémní a v praxi se nepoužívají. Organizace tak oscilují někde mezi těmito dvěma extrémy. *Monolitickou* dokumentací rozumíme systém, kdy veškerá bezpečnostní opatření jsou shromážděna v jediném dokumentu. O monolitické dokumentaci lze teoreticky uvažovat pokud IT v organizaci je velmi malé - v takovém případě se ale formální bezpečnostní dokumentace IT často vůbec nezpracovává.

Druhým extrémem je systém, kdy každé informační aktivum a každá procedura má svůj vlastní bezpečnostní dokument. Ani k tomuto systému se většinou nepřikláníme. V zájmu zvýšení efektivity se spíše snažíme identifikovat podobná informační aktiva v majetku organizace a související procesy a tyto řešit společně (např. Bezpečnostní politika provozu WWW serverů společnosti ABC s. r. o.).

Zaměření se spíše na jednotlivé třídy IT aktiv také odpovídá snaze IT oddělení co možná nejvíce unifikovat jednotlivé IT prostředky tak, aby byly od stejných výrobců (ideálně i stejného typu), obsahovaly stejný operační systém a programové vybavení. V takovém prostředí se výrazně zvyšuje pravděpodobnost, že takto podobná zařízení budou čelit velmi podobným rizikům a je tedy výhodné je z hlediska bezpečnosti vyřešit najednou.

V neposlední řadě se taková bezpečnostní dokumentace také lépe udržuje a je také levnější.

Získání kontroly na aktivity by z pohledu bezpečnosti mělo nepřímě vést také k lepšímu provozu takového aktiva a tím také vyšším benefitům, které organizaci budou vyplývat z použití těchto aktiv.

Kontrolní otázky: 1.4 Bezpečnostní dokumentace



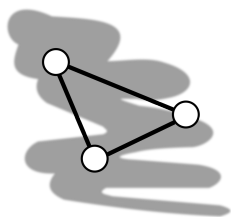
1. Co je to projekt?
2. Jak se liší provozní a projektová bezpečnostní dokumentace?
3. Co rozumíme monolitickou dokumentací?
4. Vysvětlíte rozdíl mezi politikou a postupem?

1.3.3 Formálnost vs schvalovací proces

Konečně se dostáváme k *formálnosti dokumentace*. Přístup k tvorbě dokumentace může být výrazně rozdílný právě v této oblasti. Obvykle se s bezpečnostní dokumentací začíná v čistě neformální rovině. Bezpečnostní opatření v takovém případě nejsou psaná nebo jsou psána neformálním jazykem jako určitá doporučení, podle kterých se dá řídit.

Seznamování s dokumentací pak probíhá také neformálně, většinou tak, že méně zkušení pracovníci se ptají těch zkušenějších „jak se věci dělají“. Dokumentace vzniká spontánně, což znamená že bez jakýchkoliv nároků na kvalitu jako soubor dokumentů, které mají napomoci především ve vyhnutí se různým problémům a to obvykle motivuje jednotlivé pracovníky, aby se těmito pokyny řídili.

Vzhledem k neformálnosti takové dokumentace však nemůžeme očekávat jakoukoliv vymahatelnost těchto zásad, nebo možnost je použít jako základ pro nějaké kárné řízení při jejich porušení. Takováto dokumentace je tedy udržovatelná ve funkční podobě pouze v menších kolektivech, kde jsou spolu jednak všichni v přímém kontaktu, jednat na pracovištích používajících takovou dokumentaci musí panovat atmosféra vzájemné důvěry a respektu. Stačí přitom jediný člověk, který takovéto předpoklady nesplňuje, aby se celý model neformální bezpečnosti zhroutil.



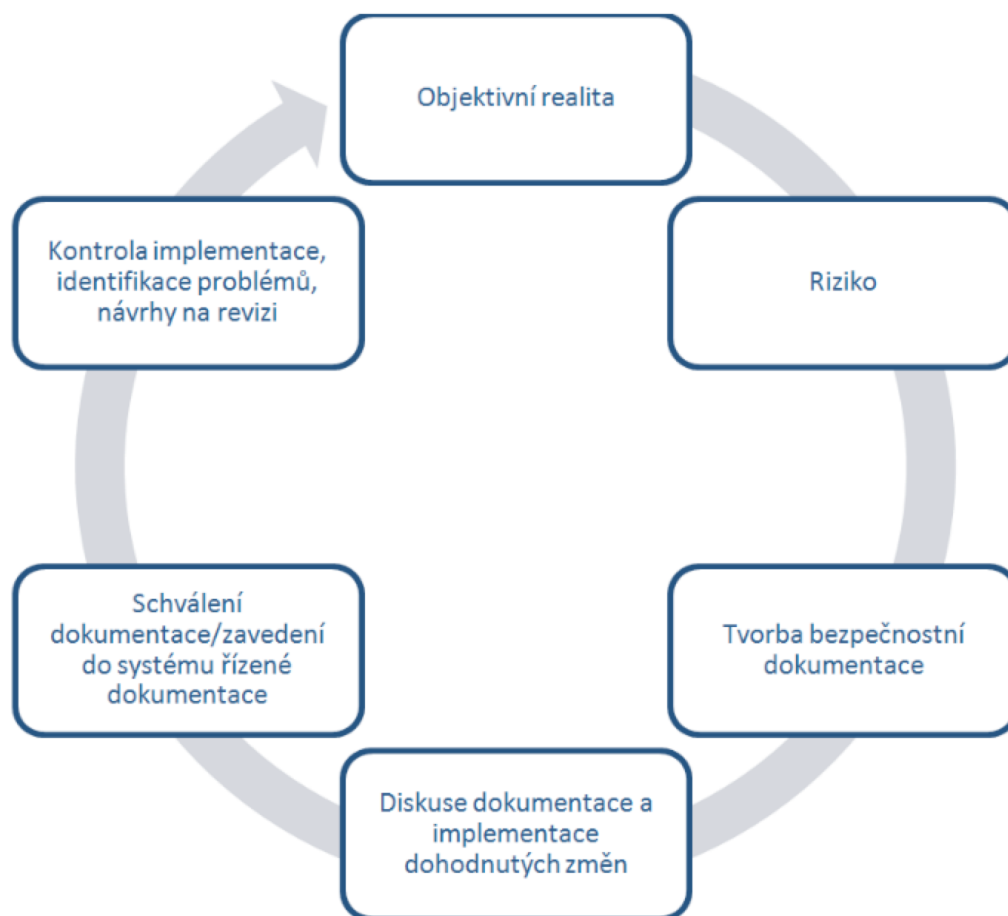
Hodnocení procesů

Hodnocení procesů je možno provádět i formálně. V jedné z následujících kapitol věnující se systému IT governance COBIT se budeme tímto procesem zabývat a to dokonce dvěma odlišnými způsoby - hodnocením tzv. *dospělosti procesů* a také se blíže podíváme na způsob hodnocení dle ISO 15504 [12].

Čím větší je organizace, tím vyšší obvykle má nároky na formalizaci procesů, které používá pro svou činnost. Tento poznatek platí obecně, nikoliv pouze pro oblast počítačové bezpečnosti. Velké společnost často zavádějí celé systémy řízení dokumentace a oblast řízení bezpečnosti informací a IT prostě berou jako další blok v celém systému. Ten pak sice může být do určité míry brán samostatně, avšak z formálního hlediska bude se zbytkem běžné dokumentace mít společné znaky (stejný způsob identifikace, hlavička/patička popř. titulní list, ale také způsob tvorby, schvalování a revize dokumentace).

Proces tvorby, schvalování a revize bezpečnostní dokumentaci si můžeme představit podobně jako na obr. 1.7.

Bezpečnostní dokumentace nejen bezpečnost informací by tedy neměla být mrtvým cárem papíru, ale měl by odrážet aktuální obraz práce s riziky v daném časovém okamžiku. Bezpečnost je z tohoto



Obrázek 1.7: Proces tvorby, schvalování a revize bezpečnostní dokumentace

pohledu pouze jedním z nástrojů, které dané organizace používá pro dosažení svých cílů. Bezpečnost tedy obvykle sama o sobě není cílem dané organizace.

Připomeňme si základní cíl organizace - je definován v misi organizace a tam obvykle nejsou formulace typu: firma ABC má ambice využívat nejzabezpečenější informační systém. Zabezpečení je pouze funkcí, která umožnit naplnění cíle, za kterým daný informační systém nasazujeme.

Úroveň bezpečnosti IT (podobně jako úroveň bezpečnosti obecně) je tedy vždy do určité míry záležitostí kompromisu. Kompromis může být finančního charakteru: kolik finančních prostředků do opatření můžeme a chceme investovat? Kompromis ale může být ve smyslu pohodlnosti pro koncového uživatele - pohodlí práce koncového uživatele v chráněném systému je obvykle nepřímě úměrné výši zabezpečení.

Zvolená úroveň zabezpečení může mít ale širší souvislosti - např. v nutnosti používat určité postupy nebo programy, vyžadované legislativou apod.

V praxi toto můžeme ilustrovat třeba pro operační systém Windows 11 a v něm obsaženou technologii **User Access Control (UAC)**, která způsobuje, že systém vyžaduje potvrzení o provedení činnosti vyžadující zvýšená práva k systému. Někteří uživatelé hlášení **UAC** akceptují jako nutné zlo, jiní tuto technologii vypínají nebo potvrzují automaticky veškeré žádosti o navýšení práv, aniž by zkoumali oprávněnost takových požadavků.

UAC přitom má potenciál výrazným způsobem zvýšit bezpečnost systému a zabránit efektivně i řadě neznámých hrozeb, které ještě není schopen rozeznat antivirový program.

1.3.4 Formálnost vs restrikce v bezpečnostní dokumentaci

Z výše uvedeného vyplývá, že nastavení restrikcí je velmi vážné rozhodnutí, které na jedné straně má vliv na úroveň bezpečnosti, kterou dokumentace má zajistit, na straně druhé vyšší restrikce vedou k omezování uživatelů a to vede ke zvyšování odporu k zavádění a udržování takových pravidel.



Kontrolní otázky: 1.5 Schvalovací procesy

1. Co je účelem schvalovacího procesu bezpečnostní dokumentace?
2. Kdy můžeme považovat bezpečnostní dokumentaci za dokončenou (nevyžadující další revize)?
3. Popište vztah mezi bezpečností a cíli organizace.

Z hlediska restriktivnosti rozlišujeme čtyři stupně¹:

- promiskuitní
- liberální
- racionální
- paranoidní

Promiskuitní přístup znamená, že všichni uživatelé mohou vykonávat v chráněných systémech všechny činnosti a to i takové, které by z titulu své funkce vykonávat nemuseli nebo dokonce neměli.

Prakticky si tento přístup můžeme představit tak, že uživatel chráněného systému dostane k tomuto systému maximální možná práva (tedy práva administrátora). Tento přístup tak klade vysoké nároky na znalosti a zodpovědnost svých uživatelů. Administrátor totiž svým konáním může vážně narušit fungování administrovaného systému, z tohoto důvodu je obvykle na činnosti spojené s administrací speciálně školen (vzděláván). Takovými školeními obvykle běžný uživatel neprochází, je proto na jeho sebeovládání, aby některé činnosti v rámci systému nevykonával a nechával je na specialistech ačkoliv technicky má práva k výkonu těchto činností.

To je poměrně silný požadavek na uživatele, protože po něm chceme, aby sám rozhodl, které činnosti z pohledu bezpečnosti by měl vykonávat, a které ne. Tedy chceme, aby uživatel sám identifikoval funkce systému a činnosti, které nebude z důvodu bezpečnosti vykonávat. Technicky to samozřejmě jde, ale je potřeba říci, že takové rozhodnutí jde proti lidské přirozenosti. Člověk je od přírody nastaven tak, že pokud narazí na problém, tak se jej pokusí překonat a my mu dáváme do rukou práva, aby tak mohl skutečně učinit. Zároveň ale říkáme, aby tak nečinil.

Udržitelnost takového přístupu je možné zaručit pouze v situaci kdy se jednotliví uživatelé vzájemně neformálně dohodnou a tuto dohodu dodržují. Aby toto mohlo fungovat musí organizace přizpůsobit tomuto modelu své chování a také organizaci.

Z praktického pohledu se jednotliví uživatelé:

- musí vzájemně znát a ideálně také respektovat,
- musí spolu komunikovat a být dostupní pro řešení různých problémů spojených s provozem systému.
- Ideálně by uživatelé systému měli být lokalizováni na jednom místě (v jedné budově nebo dokonce v jedné místnosti).
- Preferovány jsou neformální modely řízení.

Výše uvedené předpoklady je bohužel možné zajistit pouze v malých pracovních kolektivech. Čím větší kolektiv, tím vyšší jsou nároky na formalizaci všech procesů a bezpečnost v tomto ohledu není výjimkou.

Mimochodem je zajímavé, že tento přístup je u jeho uživatelů velmi oblíben pro svou neformálnost i přes problémy, které jsou s ním spojeny. Příznivci tohoto přístupu se dokonce často snaží o jeho udržení i v situaci, kdy se podmínky v organizaci výrazně změnily, např. se společnost rozrostla a bylo by vhodnější použití restriktivnějšího přístupu.

Změna v jednou nastoleném směru tedy není úplně jednoduchá a o to důležitější je vhodně nastavit přístup k řešení bezpečnosti již od počátku.

Liberální přístup umožňuje uživateli dělat vše, co není explicitně zakázané. U liberálního přístupu organizace akceptuje fakt, že promiskuitní přístup je příliš volný a je nutné zavést určitá pravidla. Tato pravidla jsou založena obvykle na přísném oddělení objektů systému (tabulek, formulářů, funkcí)

¹V předmětech Bezpečnostní informatika 2 [77] a Počítačové sítě a ochrana dat [79] jsme u těchto přístupů požívali označení politiky (např. promiskuitní bezpečnostní politika). Jedná se ve skutečnosti o totožný problém. V těchto skriptech, ale chápeme problematiku bezpečnosti mnohem širěji, a proto spíše používám pojmy jako bezpečnostní dokumentace nebo přístup (např. liberální přístup).

od subjektů systému (uživatelé). Jinými slovy toto znamená, že vytváříme databázi uživatelů a jejich rolí a využíváme je pro řízení přístupu uživatelů k různým částem systému.

Účelem je přitom identifikace činností, které by daná role neměla vykonávat. Takové činnosti jsou pak zakazovány.

Abychom si to shrnuli: při vytvoření nového uživatele má tento uživatel stejná práva jako administrátor a postupně tato práva omezujeme. Tomuto způsobu počáteční konfigurace uživatele říkáme *allow all* (dovol vše).

Tento přístup je samozřejmě bezpečnější než přístup promiskuitní, umožňuje nám však dosáhnout zaručené úrovně zabezpečení? Abychom mohli odpovědět na tuto otázku musí se podívat na o stupeň přísnější přístup k bezpečnosti.

Racionální přístup zakazuje dělat vše, co není explicitně povoleno. I v rámci této politiky je nutné provést klasifikaci všech objektů BP (dat, serverů, nástrojů ...) a subjektů BP (uživatelů) a na základě této klasifikace přidělit práva.

Oproti liberálnímu přístupu používáme ale odlišnou počáteční konfiguraci, která je popsitelná pomocí slov *deny all* (odepřít/zakázat vše). Nově vytvořený uživatel tedy má nulová práva v systému a administrátor zkoumá, jaká práva nutně uživatel potřebuje pro výkon svých pracovních povinností.

Rozdíl mezi oběma přístupy se jasně projeví pokud začneme uvažovat o možných chybách v konfiguraci. V případě, že liberální administrátor udělá chybu, výsledkem bude účet, který bude mít vyšší práva než je nutné, chyba racionálního administrátora vede k účtu, který má nižší než potřebná práva. Liberální administrátor má tak při chybě bezpečnostní problém, zatímco racionální administrátor má při chybě nespokojeného uživatele, který svůj problém musí aktivně řešit, pokud chce pracovat - problém je tedy identifikován a vyřešen.

Pokud se tedy nad těmito přístupy zamyslíme, tak zjistíme, že racionální přístup k ochraně je z výše jmenovaných přístupů prvním z hlediska restriktivnosti, u kterého lze garantovat určitou míru bezpečnosti. Logicky liberální přístup nedovoluje zaručit zvolenou úroveň bezpečnosti.

Je potřeba poznamenat, že ani liberální, ani racionální přístup není odolný vůči přílišné aktivitě administrátora. Obvykle se ale sází na rčení, že lenost je dobrou vlastností administrátora a tak se aktivita administrátora nad rámec zajištění hladkého chodu systému nepředpokládá.

Ve skutečnosti o administrátorech koluje celá řada rčení, z nichž jedno se pro tento okamžik obzvláště hodí: paranoia je dobrou vlastností administrátora nebo to že jsem paranoidní ještě neznamená, že mě nesledují. Prosím berte tato rčení s nadhledem - skutečná paranoia není dobrou vlastností u nikoho ani u administrátora. Tím se však hezky oklikou dostáváme k poslednímu přístupu.

Paranoidní přístup zakazuje dělat vše, co je potencionálně nebezpečné včetně toho, co by nemuselo být nutně explicitně zakázané. Jedná se tedy o logický krok směrem k vyššímu stupni zabezpečení ve srovnání s racionálním přístupem.

Paranoidní přístup explicitně předpokládá, že „tam venku“ jsou lidé, jejichž jediným úkolem je nám škodit a z tohoto důvodu je nutné systémy zabezpečit obzvláště důkladně po všech stránkách. Oproti racionálnímu přístupu zkoumáme samotnou funkční základnu chráněného systému a hledáme komponenty, které nejsou nutné k provozu systému, popřípadě by mohly být zneužity k útoku na systém. Tyto komponenty se pak odstraňují nebo alespoň vypínají.

Omezování funkčnosti kromě pozitivních efektů z hlediska bezpečnosti má také své negativní důsledky. Odstranění funkčnosti totiž mohla přinášet uživatelům prospěch při práci se systémem → odstranění pak nutně vede k znesnadnění práce. Negativem tohoto přístupu také možné výrazné omezení počtu cest vedoucích ke splnění cíle práce uživatele se systémem. Toto omezení nemusí některým uživatelům vyhovovat a mohou se proti němu bránit.

Vzhledem k těmto negativním efektům se paranoidní způsob zabezpečení využívá prakticky pouze p případech obzvláště citlivých IT aktiv. V ostatních případech je preferován především racionální přístup.

1.4 Základní principy tvorby bezpečnostní dokumentace

V předchozích podkapitolách jsme se o bezpečnostní dokumentaci dozvěděli toho spoustu. Víme, že má vztah k cílům organizace, že souvisí s vnitropodnikovou kulturou (tím, jak se věci v dané organizaci dělají) a že dokumentace může mít velmi různou podobu. Otázka zní: *může mít bezpečnostní dokumentace libovolnou podobu?*

Pokud má být bezpečnostní dokumentace závazná a vymahatelná pak nikoliv - v takovém případě je potřeba, aby bezpečnostní dokumentace splňovala určitá kritéria, řídila se určitými pravidly. Právě tato pravidla probereme v této podkapitole.



Volba přístupu k zabezpečení

Organizace obvykle provozují celou řadu IT aktiv pracujících s různě citlivými údaji, z toho však také vyplývá, že také nároky na zabezpečení těchto aktiv budou různé. Tedy v rámci jedné organizace mohou být pro různá IT aktiva aplikovány různé přístupy.

Např. experimentální vývojové prostředí pro IS vyvíjený in-house (vlastními silami) může být přijatelný promiskuitní přístup k zabezpečení, ale stejný IS, který je již nasazen do ostrého provozu může vyžadovat racionální nebo dokonce paranoidní přístup k zabezpečení.



Kontrolní otázky: 1.6 Formálnost a restrikce politik

1. U kterého nejnižšího možného přístupu lze garantovat určitou úroveň bezpečnosti?
2. Za jakých okolností může fungovat promiskuitní přístup k bezpečnosti?
3. Vysvětlete rozdíl mezi principem allow all a deny all.
4. Který z přístupů k zabezpečení je odolný vůči přílišné aktivitě administrátora?

Tedy jaké principy je vhodné při tvorbě bezpečnostní dokumentace dodržet? Jedná se především o princip:

- adresné odpovědnosti,
- znalosti,
- integrity,
- aktuálnosti a periodického hodnocení,
- úměrnosti
- apod.

Co tedy jednotlivé principy znamenají? *Princip adresné odpovědnosti* vychází z toho, že pokud dojde k bezpečnostnímu incidentu vinou porušení pravidel a organizace chce nastavenou úroveň bezpečnosti v praxi prosazovat, pak musí být v dokumentaci zakotvena odpovědnost a to způsobem, aby bylo možné odvodit spojení mezi určitým pravidlem a konkrétní osobou.

Tedy pokud dojde k bezpečnostnímu incidentu musíme vědět, kdo za to může. Následnou zodpovědnost je možné často zjistit i při absenci bezpečnostní dokumentace, problém je ale v tom, že v takovém případě jsme schopni většinou pouze ukázat prstem bez možnosti použití dalších kárných prostředků, protože nejsme schopni dokázat, že daný člověk něco dělat měl a nedělal nebo naopak dělal něco co dělat neměl.

Adresnost obvykle neřešíme zavedením konkrétních jmen do bezpečnostní dokumentace, ale spíše přiřazením pravidel určitým rolím nebo funkcím. Pro funkce přitom existují obvykle jmenovací dekrety a pro role můžeme sestavit třeba jmenné seznamy, které ale vedeme jako samostatné dokumenty.

Samostatnost jmenného seznamu je důležitá, protože lidé se mění a udržování dokumentace v aktuální podobě by bylo při integraci seznamu přímo do bezpečnostní dokumentace velmi náročné a to jak časově, tak i finančně.

Princip znalosti nám říká, že pokud mají být ustanovení bezpečnostní dokumentace účinná (vy-mahatelná) musí být všichni, kterých se týká, prokazatelně seznámeni s jejím obsahem. To je logický požadavek - pokud nevím, že něco mám/nemám dělat, šance, že to splním se limitně blíží nule.

Existuje celá řada způsobů, jak požadavku znalosti dostat. Můžeme zvolit čistě třeba byrokratické řešení. To obvykle spočívá v tom, že v nějakém obecném vnitropodnikovém předpisu stanovíme všem uživatelům povinnost seznámit se a dodržovat všechny předpisy organizace. Jelikož bezpečnostní dokumentace má také charakter předpisu, je problém vyřešen, tedy alespoň „papírově“. Tento způsob často využívají organizace se zavedenou řízenou vnitropodnikovou dokumentací.

Řízená dokumentace se zavádí většinou jako součást zavádění některého ze systémů řízení, např. ISO 9 000, tedy řízení jakosti. Součástí řízené dokumentace je také rozhodnutí o způsobu zveřejňování nových nebo revidovaných dokumentů. To se provádí jednak prostřednictvím k tomu určených intranetových portálů, jednak lze k tomuto účelu použít třeba běžný email a hromadně rozeslat upozornění na nové/revidované dokumenty s odkazem na plný text nacházející se na portálu. Tento způsob využívá

např. VŠB.

Realizace tohoto řešení je po technické stránce jednoduše realizovatelná a proto také levné. Portál pro zveřejňování dokumentace lze zrealizovat v prakticky jakémkoliv **Content Management System (CMS)**, jako je třeba Joomla [15], Drupal [23] nebo stovky dalších. Pro velké společnosti může být výhodné využití systémů jako je Microsoft SharePoint nebo dokonce specializovaných systémů pro řízení dokumentů **Document Management System (DMS)**. Rozesílání mailu ať už ručně nebo prostřednictvím distribučních seznamu (mailing listů) je technologie, která se v prakticky nezměněné podobě využívá již 40 let.

Tento způsob zveřejňování má však jednu zásadní vadu – zveřejněné dokumenty totiž prakticky nikdo nečte. Důvody k tomu jsou různé. Studium dokumentů nikdo nekontroluje, resp. v podstatě neexistuje způsob jak tuto kontrolu zajistit. Teoreticky lze sice vyžadovat na portálu přihlášení a následně kontrolovat, jestli daný uživatel k danému dokumentu skutečně přistoupil a pokud se zjistí, že ne, tak problém řešit. Obrana proti tomuto postupu ze strany koncových uživatelů je ale jednoduchá – mohou např. tvrdit, že dokument četli na monitoru kolegy, nebo v papírové podobě.

Druhým důvodem, pro který většina lidí takovou dokumentaci nečte, je fakt, že takových dokumentů mohou být měsíčně klidně desítky a prostě není čas je prostudovat všechny. Koncový uživatel většinou nezkoumá, které dokumenty by mu byly užitečné, prostě upozornění maže všechny.

Druhou možností, kterou máme je realizace nějaké formy školení. Je přitom pouze na nás jakou formu toto školení bude mít a jaké cíle jím budeme sledovat. Školení může být chápáno jako seznámení se s obecnými principy bezpečnosti nebo jako školení na užívání informačního systému. Podobně se můžeme rozhodovat o tom, zda školení budeme provádět vlastními silami nebo si na něj najmeme externího lektora, jestli bude v pracovní době nebo mimo ni, jestli bude stačit účast nebo je vyžadována i aktivita ze strany školených, popřípadě zda budeme testovat znalosti nějakou formou testu nebo zkoušky. Zejména poslední dobou je populární také realizace školení distanční formou.

Organizace školení bez ohledu na formu a obsah je významná sama o sobě, naznačuje totiž zaměstnancům, že organizace na určité téma klade důraz dostatečně veliký, aby ji stálo za to do školení investovat čas a prostředky, zejména, pokud je školení realizováno v pracovní době.

Samozřejmě zvolená forma a obsah bude mít vliv na to, jak školení bude úspěšné. Obecně lze říci, že úspěšnější jsou školení v pracovní době než mimo ni, zejména pokud se nekonají na pracovišti. Osoba školitele je důležitá, ale obecně nelze říci zda externí lektor bude lepší než interní zaměstnanec – i uvnitř firem lze nalézt zdatné řečníky a výhodou může být také určité osobní souznění s ostatními zaměstnanci (možná lepší volba tématu, bodů na které je potřeba klást důraz apod).

Formálnost účasti ovlivní také procento informací, které utkví školenému v paměti. Pokud je vyžadováno, aby si účastník školení odeseděl bez interaktivních prvků, které by jej aktivně zapojily procesu výuky, zle podobně jako při běžné výuce předpokládat zapamatování maximálně 20 % informací (mluvené slovo + prezentace v PowerPointu). Při uvažování interakce lze toto procento i zvýšit ale celkově nelze očekávat, že se přiblížíme byť 50 %.

Pokud školení vyžaduje testování znalostí může, ale také nemusí to mít pozitivní vliv na množství zapamatované látky. Pokud provedeme školení, za kterým okamžitě následuje test pak vliv testu je prakticky zanedbatelný. Školení stimuluje krátkodobou paměť nebo jsou odpovědi školeným dokonce diktovány a po opuštění školící místnosti je zahájen rychlý a nevratný proces zapomínání.

U rozsáhlejších školení je mezi školením a testem přestávka, která nutí účastníky, aby se připravili na vykonání testu, prostudovali studijní materiály látku se učili. Tímto způsobem se stimuluje také dlouhodobá paměť – účinky školení jsou pak samozřejmě větší, na druhou stranu je také takové školení časově náročnější a proto i podstatně dražší.

Prezenční i distanční forma školení může být účinná, záleží ale na způsobu, jakým zejména distanční formou školení zrealizujeme. Dostanou školení příručku a budou se doma učit, nebo jim připravíme zajímavé úkoly a budeme je nutit aby je společně s ostatními školenými realizovali? Otázkou je také cíl školení. Školení obvykle chápeme jako jednorázovou záležitost. Při využití **Virtual Learning Environment (VLE)** prostředí můžeme vytvořit prostor, v rámci kterého se budou jednotliví zaměstnanci dlouhodobě scházet a diskutovat/řešit problémy, se kterými se při využití systému nebo technologie setkávají.

Realizace tohoto způsobu řešení však vyžaduje vysokou angažovanost organizace samotné (lektor musí v podstatě neustále monitorovat **VLE**) a jednak o to musí mít jednotliví zaměstnanci zájem.

Principem integrity rozumíme zajištění souladu mezi opatřeními uplatňovanými v bezpečnostní dokumentaci a cíli, které si organizace stanovila. Účelem je zajištění toho, aby přijímaná ochranná opatření nesnižovala schopnosti organizace plnit svou funkci. Princip integrity tedy plní regulační

úlohu mající za účel zachování nebo zvýšení efektivity vykonávaných činností.

V úvahu přitom bereme jednak základní cíle organizace tak, jak je definuje mise, jednak bereme v úvahu také dílčí cíle, které byly definovány při zavádění technologií a systémů (obecně IT aktiv).

Princip aktuálnosti a periodického hodnocení nás upozorňuje na fakt, že bezpečnost je pohyblivý cíl. Obor IT je vysoce inovativní – mění se technologie samotné, pravidelně se objevují nové systémy nebo jejich nové verze, nástroje, postupně se také mění samotný způsob jakým IT prostředky využíváme (např. v poslední době tablety). Všechny tyto změny společně přispívají k vývoji hrozeb, které tato aktiva ohrožují. Z tohoto důvodu nelze očekávat, že jednou napsaná bezpečnostní dokumentace si bude udržovat konstantní schopnost chránit aktivum, kterého se týká. Z toho logicky plyne, že bezpečnostní dokumentaci je potřeba aktualizovat. Doba, po které má k revizi dojít však může být pro různá aktiva a také různě společnosti různá.

Časový interval revize se často zavádí přímo do znění daného dokumentu větou podobné této: tento dokument musí být revidován minimálně 1x za ... (můžeme doplnit libovolný časový interval). Interval revize dokumentu je pouze málokdy kratší než 6 měsíců, nejčastěji se používá interval jeden nebo dva roky podle citlivosti údajů, se kterými se pracuje, nebo rychlosti inovací v dané oblasti.

Platí také, že čím výše jsme v hierarchii dokumentů (viz předchozí podkapitola a obr. 1.6), tím je daný dokument obecnější. Proto, ze své podstaty, bude např. strategie obsahově stálejší než běžné provozní předpisy nebo dokonce podpůrné dokumenty, které může být potřeba aktualizovat i několikrát do roka v důsledku běžných aktualizací verzí řízeného systému.

Po uplynutí tohoto intervalu by dokument měl být znovu přezkoumán a mělo by být zhodnoceno, zda obsah odpovídá bezpečnostním nárokům, které budou na chráněný systém kladeny v následujícím období. Výsledkem revize tedy nemusí být změna – revizní interval pouze zajišťuje, abychom nutnost zapracovávat změněné bezpečnostní požadavky úplně nezapomněli. Tedy revize může skončit zjištěním, že změny v dokumentu není potřeba dělat.

Principem úměrnosti rozumíme to, že investicí do bezpečnostních opatření, která pokrýváme bezpečnostní dokumentací, dostaneme odpovídající protihodnotu ve schopnosti organizace dosahovat své cíle.



Podobnost principů

Možná jste si všimli, že některé z výše uvedených principů jsou si podobné. Tato podobnost není náhodná, protože výše uvedené principy ve všech případech směřují ke splnění základních cílů bezpečnostní dokumentace tedy vymahatelnost bezpečnostních opatření a jejich efektivita. Jednotlivé principy jsou proto pouze různým pohledem na stejný problém.

V literatuře (např. [50]) lze najít ještě řadu dalších principů, které se doporučuje dodržovat, ale vzhledem k omezenému prostoru se tady jimi zabývat nebudu.



Kontrolní otázky: 1.7 Základní principy bezpečnostní dokumentace

1. Vyjmenujte alespoň tři principy, kterými se řídí tvorba bezpečnostní dokumentace.
2. Vysvětlíte princip znalosti.
3. Proč je tak důležitá vymahatelnost bezpečnostní dokumentace?
4. Podle čeho volíme interval revize bezpečnostní dokumentace?

1.5 Organizace přijímání, auditu a revize bezpečnostní dokumentace IT

Tohoto problému jsme se již dotkli rámcově v předchozích podkapitolách. Náš úkol však byl trochu jiný - dívali jsme se na organizaci z hlediska vnitropodnikové kultury nikoliv z pohledu organizace celého procesu (v jiné než obecné rovině). To se brzy změní, protože v této kapitole nás bude zajímat právě organizační proces tentokrát oprostěný od specifik vnitropodnikové kultury.

My už toho víme o bezpečnostní dokumentaci poměrně hodně, víme že se její tvorba řídí určitými obecnými principy a také, že opatření musí být akceptována koncovými uživateli dokumentace (jsme schopni kárně řešit excesy nikoliv situaci, kdy k porušování opatření bude docházet masově).

Pro zajištění informační bezpečnosti se většinou doporučuje (např. ISO 27 000, viz další kapitola), aby za tuto oblast zodpovídal jediný člověk. Z předchozích podkapitol víme, že organizace bezpečnosti může být různá a že oblast bezpečnosti IT může spadat do kompetenci **CIO**, **CISO**, **CSO** nebo dokonce někoho úplně jiného, proto je potřeba, abychom zvolili pro účely této kapitoly jediné označení popisující náplň práce a tomu nejlépe odpovídá **CISO**. Může tedy existovat **CIO** s pravomocemi **CISO**, ale v této podkapitole nás to nebude zajímat :-).

Svou pracovní náplní je **CISO** ideální osobou, která zastřešuje celou práci s bezpečnostní dokumentací, proto ji:

- předkládá ke schválení,
- spolupracuje s jednotlivými zájmovými skupinami na implementaci přijatých opatření,
- kontroluje implementaci,
- řeší bezpečnostní incidenty,
- apod.

CISO, ale vše nezvládne sám. Jelikož jeho vzdělání je obvykle specificky zaměřené na oblast bezpečnosti, popřípadě IT nemusí (a také obvykle není) **CISO** odborníkem v oboru, ve kterém organizace působí. Z tohoto důvodu není **CISO** sám (a se svými podřízenými) schopen sestavit bezpečnostní dokumentaci tak, aby bez problémů vyhověla principům integrity a úměrnosti. Problém může pak mít i se všeobecným přijetím opatření koncovými uživateli.

Velké společnosti tento problém řeší zřizováním formálních platforem, které slouží pro diskusi problémů v oblasti IT a také má svou funkci při schvalování a revizích bezpečnostní dokumentace IT.

Různé společnosti nazývají tuto platformu různě. Nejčastěji používaným názvem je ale jednoznačně *Vábor kybernetické bezpečnosti*. Tento název vycházel z původního zákona O kybernetické bezpečnosti (181/2014 Sb.), resp. jeho prováděcí vyhlášky (82/2018 Sb.), která s tímto označením pracuje.

Nový zákon O kybernetické bezpečnosti (264/2025 Sb.) ani jeho prováděcí vyhlášky (408 a 409/2025 Sb.) ale s tímto výborem nepracují. Dávají pouze hlavní odpovědnost za bezpečnost vedení organizace a je na organizaci samotné, jak této odpovědnosti vyhoví. Z logiky věci ale vyplývá, že organizace při implementaci systému ISMS budou potřebovat nějakou obdobnou organizační strukturu. Označení Výbor KB je pak již ustálené a proto se používá nadále.

Změny ve specifických potřebách organizací také mohou vést ke změnám v zadání této rady a to třeba včetně změny v organizačním zařazení. Dobrým příkladem může být řešení na VŠB. Původní **RRIT** byl organizován jako poradní orgán rektora. Jako takový měl svůj statut, v jeho čele stál **CIO** (ředitel **Centrum informačních technologií (CIT)**). Účelem pak bylo radit rektorovi v otázkách směřování IT na univerzitě. Z hlediska organizačního začlenění byl **RRIT** začleněn podobně jako na obr. 1.8.

Z tohoto pohledu **RRIT** stál mimo běžné organizační struktury, zato měl přímý přístup k statutárnímu zástupci univerzity.

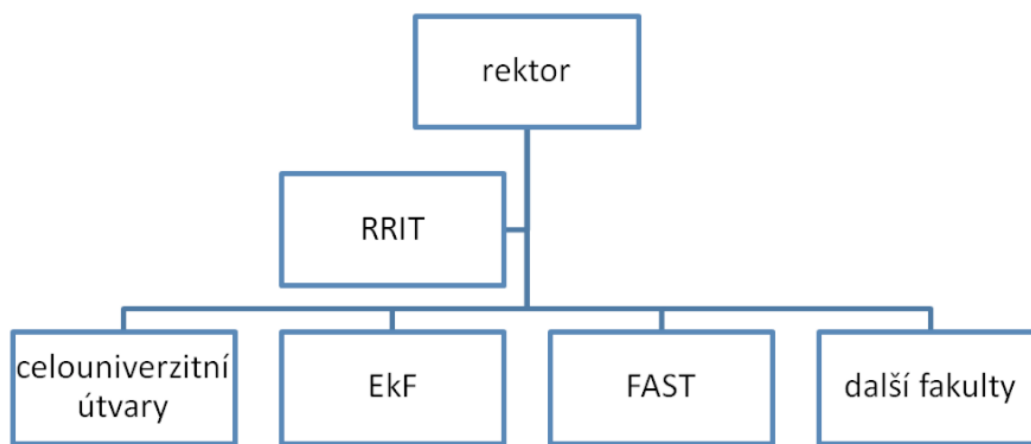
RAKOS je proti tomu organizován odlišně, viz obr. 1.9.

RAKOS podle tohoto začlenění není poradním orgánem rektora, ale ředitele **CIT**. **RAKOS** jako takový odpovídá spíše neformálnímu způsobu organizace. Jednotliví členové **RAKOS** musí totiž věřit, že ředitel **CIT** bude schopen záležitosti, dokumenty, strategie apod. prosadit na Kolegiu rektora, jehož je členem. Ředitel **CIT** v tomto ohledu musí spoléhat na zástupce fakult v **RAKOS**, aby přesvědčili „své“ děkany (kteří jsou členy Kolegia rektora), aby tyto záležitosti schválili.

V současnosti pak VŠB-TUO opustila i model **RAKOS** a místo něj v rámci implementace systému ISMS vytvořila plnohodnotný Výbor KB, jehož předsedou je rektor a dalšími členy pak architekt KB, **CISO**, **CIO** a ředitelé pro počítačovou síť a informační systémy. Úkolem výboru je projednávat otázky kybernetické a informační bezpečnosti, včetně projednávání a schvalování bezpečnostních předpisů.

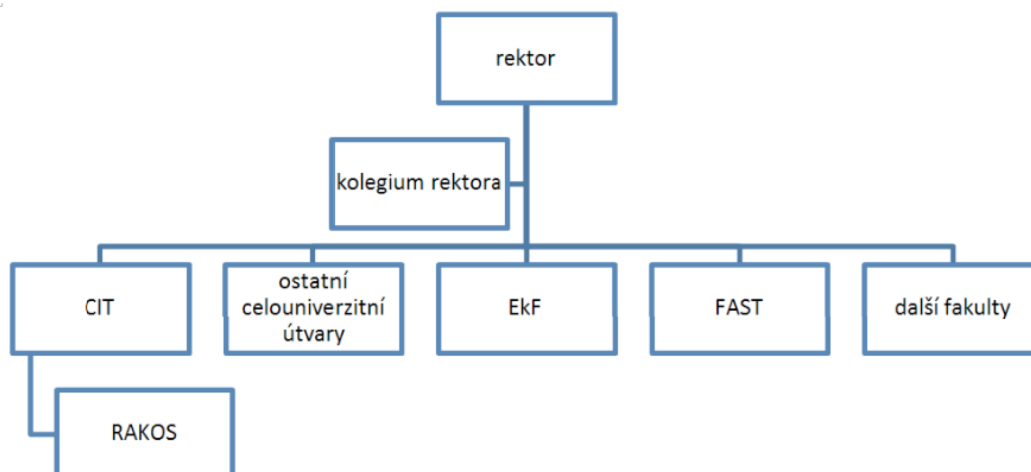
Ostatní otázky okolo IT pak řeší skupina pro strategii ICT. Předsedou je prorektor pro strategii, místopředsedou je **CIO** a členy jsou pak zástupci jednotlivých fakult a výzkumných infrastruktur.

Co si z toho vzít? Potřeby organizací se v průběhu času mění. Tyto změny postupně indukují potřebu realizace změn také v organizačních strukturách. Neexistuje přitom jedno řešení, které by vyhovovalo všem organizacím. Dále úkoly, které pomocí takových výborů řešíme jsou různé. Pokud zřídím Výbor KB podle filozofie vycházející z původní legislativy, bude složení výboru takové, že v podstatě znemožní, aby se sešel (a jednal) více krát než jednou za několik měsíců, tedy např. čtvrtletně.



pozn: Ekonomická fakulta (EkF)
Stavební fakulta (FAST)

Obrázek 1.8: Organizační začlenění **RRIT**



Obrázek 1.9: Organizační začlenění **RAKOS**



Organizace rady IT

Organizace rady, její pojmenování stejně jako její poslání může být velmi různorodé v závislosti na vnitropodnikové kultuře. Řešení rady může být více či méně formální (viz příklad s VŠB) – existují však činnosti, které musí být formálně řešeny vždy a to je rozhodnutí:

- kdo zodpovídá za oblast bezpečnosti IT
- jak (jestli) bude organizována samotná Rada IT
- kdo bude schvalovat bezpečnostní dokumentaci a jakým způsobem.

Jak je již zmíněno musí toto rozhodnutí být formální – tedy stanovené patřičným vnitropodnikovou normou^a.

^aV tomto předmětu předpokládáme potřebu vést vnitropodnikovou dokumentaci (tedy nutnost formálně řídit bezpečnost IT).

V takovém případě, ale výbor bude moci projednávat pouze předem připravené a projednané návrhy předpisů, které pak následně bude schvalovat.

Vyvodit z toho pak lze to, že bude potřeba ustanovit, ať už formálně nebo neformálně, další organizační strukturu, která bude „akčnější“ a bude vytvářet a předjednat tyto návrhy.

V obecné rovině organizace musí řešit:

- schvalování bezpečnostních politik (dokumentace)
- hodnocení účinnosti politik
- měl by obrušovat třecí plochy mezi jednotlivými útvary organizace, které by se týkaly bezpečnosti IT
- schvalování zprávy o činnosti útvaru odpovědného za bezpečnost IT
- tvorba strategie rozvoje IT
- a další.

Každá organizace si ale sama určí, zda tyto úkoly bude realizovat jedinou organizační strukturou a nebo jich bude využívat více. Rozhoduje také o formálnosti takových struktur. Přitom platí, že minimálně jedna z takto vytvořených struktur a to konkrétně ta, která schvaluje vnitropodnikové předpisy a jiné strategické dokumenty v oblasti bezpečnosti informací, musí být ustanovena formálně. Důvodem je kontrolovatelnost procesu schvalování předpisů.

Z hlediska složení by alespoň na té nejvyšší úrovni (Výbor KB) měl být statutární zástupce dané organizace předsedou. Z hlediska dalších členů by zde měli být minimálně CIO, CISO a architekt KB. Dle potřeby pak organizace mohou jmenovat další členy, jako např. **CTO**, žádoucí zejména u startupů, **CSO**, zástupce právního oddělení, apod.

Naopak oficiálním členem výboru **nemůže** být **auditor**. Důvodem je, že auditor by měl být nezávislý vůči auditovanému systému. Vzhledem k tomu, že Výbor projednává a schvaluje předpisy, které budou podléhat auditu. Přímá účast auditora jako člena výboru na schvalování by automaticky znamenala ztrátu nezávislosti. Auditor ale může být přizván na jednání výboru, např. aby představil výsledky auditu.

Pro organizační struktury, které pro takový výbor připravují podklady, je již volnější. Tuto organizační strukturu obvykle vede CISO, ale do práce se obvykle přímo nezapojují vedoucí pracovníci. Pro identifikaci problémových míst předpisů a politik jsou jejími členy zástupci jednotlivých útvarů popřípadě skupin uživatelů IT tak, aby rada tvořila reprezentativní zájmový vzorek organizace s ohledem na IT.

Další skupinou důležitou pro implementaci a zajištění bezpečnosti IT jsou správci zájmových systémů. Jedná se o běžné administrátory, jejichž základním úkolem je udržení systému v takovém stavu, aby byly schopny poskytovat služby. Právě tato skupina pracovníků je velmi důležitá z hlediska bezpečnosti, protože právě oni prakticky implementují bezpečnostní opatření a kontrolují jejich účinnost. Zároveň v případě bezpečnostního incidentu, tento incident řeší a přijímají opatření k zamezení jeho opakování.

Vzhledem ke svému pracovnímu zaměření by zástupci administrátorů měli být taktéž zastoupeni v Radě pro IT. V případě tvorby bezpečnostní dokumentace vztahující se k IT aktivům nebo jejich skupinám by se pak na tvorbě této dokumentace měli tito administrátoři podílet také a to bez ohledu na to jestli jsou nebo nejsou členy rady pro IT. Minimálně by tuto dokumentaci měli dostat k připomínkování.

Poslední skupinou, která má vztah k organizaci bezpečnosti v daném podniku jsou auditoři. V tomto případě se přitom bavíme pouze o auditu bezpečnosti IT nikoliv o auditu obecně (např. jakosti apod.). Účelem auditu je zkontrolovat, že bezpečnostní opatření jsou implementována a také vymáhána v souladu se schválenými předpisy. Auditoři poskytují tedy další úroveň kontroly nad rámec běžné, provozní kontroly zajišťované běžnými administrátory jednotlivých IT aktiv.

Audity mohou být organizovány jednak interně a jednak externě. Jejich účel je přitom jiný, stejně jako náklady, které jsou s takovými audity spojeny.

Interní audit je zajišťován interními auditory organizace. Tito auditoři jsou speciálně proškoleni pro provádění auditů, zároveň v dané organizaci vykonávají jiné činnosti – tedy nejsou až na výjimky zaměstnání pouze na provádění auditů bezpečnosti IT.

Výhodou interního auditu je jeho relativně nízká cena – provádějí ji interní zaměstnanci, kteří by si měli na sebe „vydělat“ ve zbytku běžné pracovní doby. Další výhodou je relativní rychlost provedení auditu. Interní auditoři jsou totiž obvykle podrobně seznámeni s fungováním organizace i přijatelných bezpečnostních opatření a nehrozí proto nebezpečí z prodlení vyplývající z nutnosti podrobně se seznámit s bezpečnostní situací.

Tato výhoda však může být z určitého pohledu také nevýhodou. Interní auditor totiž obvykle ví o bezpečnostní situaci v organizaci podstatně více než je nutné pro provedení auditu. Nebezpečné jsou zejména znalosti o genezi opatření - tedy důvodu, proč se opatření implementovala zrovna tímto

způsobem. Tyto „nadbytečné“ informace mohou auditora motivovat k přijetí kladného rozhodnutí bez toho aby u daného opatření si kladl otázku, zda je to tak správně nebo ne. Tomuto problému říkáme *provozní slepota*.

Externí audit takovými problémy netrpí - externí auditor nemá vztah k hodnocené organizaci, je proto nestranný a může proto lépe přijímat autoritativní rozhodnutí o skutečném stavu bezpečnosti IT.

S externím auditem jsou ale také spojeny některé problémy, zejména:

- je časově náročnější, protože auditori potřebují čas pro seznámení se s bezpečnostní situací organizace
- je finančně náročnější – audit je dodáván jako služba externí firmou a je proto patřičně zpoplatněn.
- auditori mají přístup k interním dokumentům a systémům společnosti, což představuje bezpečnostní riziko v případě, že je zvolena nedůvěryhodná auditorská firma.

Z hlediska optimality kontroly bezpečnostních opatření proto většina organizací volí kombinaci interních a externích auditů, kdy interní audity jsou častější, externí audit pak slouží jako zpětná kontrola nastavení interních auditů z hlediska jejich důvěryhodnosti.

Existují však problémy, které interním auditem není možno řešit. Interním auditem samotným nelze vyřešit certifikaci na zvolenou normu nebo kodex norem pro řešení bezpečnosti IT, např. podle ISO 27 000. Hodnocení souladu s požadavky norem musí zhodnotit externí auditorská firma k tomuto účelu certifikovaná a teprve ona je oprávněna udělit patřičný certifikát. Podobně pak fungují i následné audity, které mají za cíl zaručit, že daná organizace se od požadavků norem neodchýlila. V tomto je ISO 27 000 podobné třeba kodexu norem ISO 9 000.

Externí audit je také nenahraditelný v okamžiku, kdy organizace nalezne problém, se kterým dosud neměla žádné zkušenosti. Externí auditori v tomto ohledu mohou výrazně pomoci, jednak mohou zhodnotit celkový rozsah problému, jednak mohou navrhnout kroky vedoucí k nápravě.

Výhodou externích auditorů je to, že nepracují pouze pro jedinou firmu a proto mají obvykle rozsáhlé zkušenosti s provozem různých systémů v řadě odlišných prostředí, což jim dává lepší zázemí pro poradenskou činnost. Další výhodou je možnost využití specializovaných programů a systémů, které mohou pomoci s auditem. Stejně tak, jako portfolio šablon, postupů a zkušenost s jejich aplikací. Specializované nástroje, informační systémy. jsou často velmi drahé, a proto si je organizace které auditní činnost v oblasti IT nemají jako základní poslání, nemohou většinou dovolit.

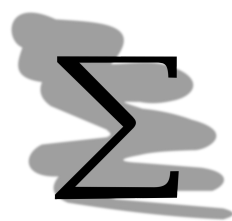
Zprávu auditorů ať už interních nebo externích by měl schválit, popř. vzít na vědomí Výbor KB. S výsledky auditů by se mělo dále pracovat zejména pokud byly nalezeny neshody mezi nastavením jednotlivých procesů a jejich skutečnou implementací, nebo mezi fungováním systému a reálných potřeb vyplývajících z legislativy, norem nebo prosté bezpečnostní situace.

Výsledky auditu by proto měly sloužit jako jeden z podkladů pro provedení revize bezpečnostní dokumentace, popřípadě dalších vnitropodnikových norem.

Kontrolní otázky: 1.8 Audit a revize politik



1. Které skupiny pracovníků se podílejí na tvorbě bezpečnostní dokumentace?
2. Jaký je rozdíl mezi interními a externími auditory?
3. Existují činnosti, které interní audit ve srovnání s externím nemůže provést?
4. Jako jsou úkoly CISO?
5. Jaké jsou úkoly Výboru KB?
6. Jaké jsou úkoly administrátora IT aktiva?



Shrnutí

Tato kapitola se věnuje Systémům řízení informační bezpečnosti (ISMS / SŘBI) z pohledu organizačního řízení a systematické práce s riziky. Popisuje koncepci bezpečnosti, která musí reagovat na hrozby z vnějšího mikroekonomického (trh, konkurence) i makroekonomického (legislativa, regulace) prostředí. Text podrobně rozebírá vliv vnitropodnikové kultury na organizaci IT útvarů, na zavádění specifických bezpečnostních pozic (CISO, CIO, CSO, COO) a na formálnost a strukturu samotné bezpečnostní dokumentace. V neposlední řadě se kapitola zabývá principy plánování (vize, mise, plánovací cykly), základními přístupy k nastavení uživatelských práv (promiskuitní, liberální, racionální, paranoidní), pravidly tvorby dokumentů (např. adresná odpovědnost, úměrnost) a mechanismy kontroly v podobě Výboru kybernetické bezpečnosti a interních či externích auditů.

Kapitola 2

ISO 27000



Průvodce studiem

V této kapitole se podíváme na jedny z nejpožívanějších norem v oblasti bezpečnosti IT – ISO 27000.

Po přečtení této kapitoly budete

Znát

- členění kodexu norem ISO 27000
- základní principy řízení informační bezpečnosti

klíčová slova: ISO 27000, ISMS, bezpečnost informací, PDCA, SOA, RTP

požadavky na vstupní znalosti: K pochopení této kapitoly potřebujete zvládnout kapitolu předchozí. Pokud jste se již v minulosti setkali s nějakým systémem řízení, je jedno jakým (např. řízení jakosti dle ISO 9000, odpadů dle ISO 14000, rizik dle ISO 31000) zkuste si před započítím studia této kapitoly osvěžit základní filozofii přístupu k řízení. ISO 27000 používá filozofii stejnou.



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 3 hod.

ISO 27000 je kodex norem, který je zaměřen na systémové řízení bezpečnosti informací. Tedy jedná se o podobný koncept jako je ISO 9000 pro řízení jakosti nebo ISO 14000 pro systémy environmentálního managementu, jen je změřen do oblasti řízení informační bezpečnosti.

Samotný kodex je tvořen normami níže (přehled 26.6.2026). Tento seznam by Vám měl poskytnout základní přehled o tématech relevantních z pohledu řízení informační bezpečnosti.

- ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary
- **ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements** - hlavní norma kodexu norem ISO 27000
- **ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management**
- ISO/IEC 27003 Information technology - Security techniques - Information security management system implementation guidance
- ISO/IEC 27004 Information technology - Security techniques - Information security management - Measurement
- **ISO/IEC 27005 Information technology - Security techniques - Information security risk management**

- ISO/IEC 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 Information technology - Security techniques - Guidelines for information security management systems auditing
- ISO/IEC 27008 Information technology - Security techniques - Guidelines for auditors on information security management systems controls
- ISO/IEC 27009 Information technology - Security techniques - Sector-specific application of ISO/IEC 27001 - Requirements
- ISO/IEC 27010 Information technology - Security techniques - Information security management for inter-sector and inter-organisational communication
- ISO/IEC 27011 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013 - Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ITU-T Recommendation X.1054 a ISO/IEC 27014 Information technology - Security techniques - Governance of information security
- ISO/IEC TR 27016 - IT Security - Security techniques - Information security management - Organizational economics
- ISO/IEC 27017 / ITU-T X.1631 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
- ISO/IEC TR 27019 - Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- ISO/IEC 27021 - Information technology — Security techniques — Competence requirements for information security management systems professionals
- ISO/IEC 27022 - Information technology — Guidance on information security management system processes
- ISO/IEC TR 27023 Information technology - Security techniques - Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002
- ISO/IEC 27031 Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27032 Information technology - Security techniques - Guidelines for cybersecurity
- ISO/IEC 27033 Information technology - Security techniques - Network security - sada norem obsahující doporučení pro implementaci protipatření, vztahujících se k bezpečnosti sítí.
 - ISO/IEC 27033-1 Information technology - Security techniques - Network security - Part 1: Overview and concepts
 - ISO/IEC 27033-2 Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security
 - ISO/IEC 27033-3 Information technology - Security techniques - Network security - Part 3: Reference networking scenarios – Threats, design techniques and control issues
 - ISO/IEC 27033-4 Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways
 - ISO/IEC 27033-5 Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
 - ISO/IEC 27033-6 Information technology - Security techniques - Network security - Part 6: Securing wireless IP network access
- ISO/IEC 27034 Information technology - Security techniques - Application security - soustava norem zaměřená tvorbu, implementaci a užívání software (aplikací)
 - ISO/IEC 27034-1 Information technology - Security techniques - Application security - Part 1: Overview and concepts
 - ISO/IEC 27034-2 Information technology - Security techniques - Application security - Part 2: Organization normative framework
 - ISO/IEC 27034-6 Information technology - Security techniques - Application security - Part 6: Case studies
- ISO/IEC 27035 Information technology – Security techniques – Information security incident

management

- ISO/IEC 27036 - IT Security - Security techniques - Information security for supplier relationships - sada norem určená organizacím k hodnocení a snižování rizik pořizování zboží a služeb v rámci **Business to Business (B2B)**
 - ISO/IEC 27036-1 Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts
 - ISO/IEC 27036-2 Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements
 - ISO/IEC 27036-3 Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
 - ISO/IEC 27036-4 Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services
- ISO/IEC 27037 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence
- ISO/IEC 27038 Information technology - Security techniques - Specification for digital redaction
- ISO/IEC 27039 Information technology - Security techniques - Selection, deployment and operation of intrusion detection [and prevention] systems (IDPS)
- ISO/IEC 27040 Information technology - Security techniques - Storage security
- ISO/IEC 27041 Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative methods
- ISO/IEC 27042 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043 Information technology - Security techniques - Incident investigation principles and processes
- ISO/IEC 27050 Information technology - Security techniques - Electronic discovery
 - ISO/IEC 27050-1 Information technology — Electronic discoveryPart 1: Overview and concepts
 - ISO/IEC 27050-2 Information technology — Electronic discoveryPart 2: Guidance for governance and management of electronic discovery
 - ISO/IEC 27050-3 Information technology — Electronic discoveryPart 3: Code of practice for electronic discovery
 - ISO/IEC 27050-4 Information technology — Electronic discoveryPart 4: Technical readiness
- ISO/IEC 27799 Health informatics - Information security management in health using ISO/IEC 27002

Možná jste ve výše uvedeném seznamu postřehli několik mezer, např. ISO 27015, nebo ISO 27020. Důvody jsou různé. Kodex norem je živý, což znamená, že jednotlivé normy procházejí revizemi. Nové přibývají a mezery se tak postupně zacelují. Některé normy ale pozbývají platnosti, což byl případ právě ISO 27015. ISO 27020 je jiný případ. Tato norma existuje, je platná, ale je z oboru stomatologie, tedy bez vazby na systémy řízení bezpečnosti informací. ISO 27024 je zase ve fázi návrhu a přijetí normy se tak očekává v roce 2026 nebo 2027.

Jak vidno, je norem v kodexu celá řada. Ve výše uvedeném přehledu jsem proto zvýraznil ty, které jsou pro pochopení základů nutné. Ostatní normy lze považovat za podpůrné, např. ISO/IEC 27003 obsahuje implementační návody pro bezpečnostní politiky, což je sice užitečné, ale lze se bez této normy obejít a bezpečnostní politiky implementovat přímo pomocí ISO/IEC 27002.

ISO/IEC 27011 obsahuje specifika týkající se telekomunikačních firem a ISO 27799 je určeno pro organizace působící ve zdravotnictví.

Je potřeba si uvědomit, že kodex norem řady 27 000 je relativně mladý – první normy kodexu byly schváleny (lépe řečeno zařazeny do kodexu) teprve v roce 2005. ISO/IEC 27002 totiž bylo v té době již používanou normou, ale pod jinými čísly a to konkrétně ISO/IEC 17799. K přečíslování došlo v roce 2005 v souvislosti s konsolidací norem zabývajících se informační bezpečností do řady 27000.

V roce 2017 lze říci, že většina norem kodexu ISO 27000 se obsahově ustálila. Stále se sice ještě připravují některé nové normy např. v sadě ISO 27034, ale je jich minimum.

Podobně jako ostatní ISO normy i normy v tomto kodexu procházejí revizemi v intervalu 2 - 5 let. Většina revizí se ale omezuje na drobnější opravy a změny - tedy základní filozofie norem zůstává nezměněna.

Ačkoliv je celý kodex norem nesmírně obsáhlý, jeho základy lze pochopit na základě tří základních norem zvýrazněných v přehledu a to ISO 27001, 27002 a 27005. Tyto normy pokrývají problematiku systému ISMS jako takového (ISO 27001), politik v těchto systémech (ISO 27002) a řízení informačního rizika (ISO 27005).

2.1 ISO 27001 – systémy ISMS

ISMS znamená systém řízení informační bezpečnosti. Jedná se o poměrně sofistikovaný systém, který umožňuje, aby organizace, která implementuje tento systém získala kontrolu nad bezpečností informací, bez ohledu na to v jaké podobě se nachází (ve formě čistě elektronických dat nebo v tištěné podobě na papíře, nebo dokonce v podobě znalostí „uložených“ v hlavách svých zaměstnanců).

Filozoficky je koncept ISO 27000 založen na byrokratickém způsobu řízení, tedy svým způsobem se jedná o „papírovou válku“ podobně jako v případě systémů řízení jakosti dle ISO 9000 (viz předmět Řízení jakosti I nebo literatura [59, 60]) a jako takový je v některých případech problém zajistit promítnutí se nastavení procesů do praktického způsobu, jakým jsou procesy vykonávány - tedy zajištění, aby řízení bezpečnosti informací (nebo jakosti) nebylo pouze formální, na papíře, ale mělo pozitivní praktické dopady.

Rozdíly v selhání řízení dle ISO 9000 a ISO 27000 jsou zásadní. V případě, že selžeme při řízení jakosti, výsledkem našeho selhání bude ztráta předvídatelnosti výsledků procesů organizace. U výrobních podniku se to může projevit formou zvýšeného podílu zmetků (neshodných výrobků). U nevýrobních organizací se to může projevovat v kvalitě poskytovaných služeb, lhůtách na vyřízení apod. Tyto následky jsou poměrně závažné a mohou vést dlouhodobému poškození dobrého jména organizace a mohou vyústit až k odchodu zákazníků ke konkurenci. Následky tohoto typu se ale projevují obvykle postupně v průběhu relativně dlouhého času.

Pokud ale nejsou problémy s jakostí skutečně extrémní, pak selhání v této oblasti obvykle neohrožuje organizaci existenčně.

Selhání při řízení informační bezpečnosti ale může vést k uniku citlivých informací, nebo dokonce přímého narušení poskytované služby. Uvažovat lze také scénáře, kdy IT infrastruktura jako taková je napadena např. ransomware, což velmi často vede k celkové paralýze dané organizace do doby než je obnoven provoz na klíčových částech infrastruktury. To ale může trvat klidně i dny, úplné zotavení pak klidně i týdny.

Scénáře narušení bezpečnosti informací jsou často velmi rychlé, doprovázené masivními škodami. Přímými v důsledku nemožnosti poskytovat zboží nebo služby podle poslání organizace, ale také nepřímými jako jsou reputační škody v důsledku ztráty důvěry ze strany zákazníků po bezpečnostním incidentu. Celkově mohou být škody natolik závažné, že mohou vést až úpadku organizace.

Abychom to shrnuli - tlak na vytvoření a udržení funkčního systému ISMS je výrazně vyšší než je tomu v řadě jiných řídicích systémů.

Certifikační proces pro systém **ISMS** bychom si graficky mohli znázornit podobně jako na obr. 2.1. Na obr. 2.1 znamená:

- **Plan Do Check Act (PDCA)** - Naplánuj, proved', zkontroluj, oprav
- **SOA** - studie aplikovatelnosti
- **RTP** - plán na zvládání rizik

Všimněte si, že celý proces přípravy organizace na zavedení systému **ISMS** a jeho následná certifikace podléhá několika základním normám, jedná se především o:

- ISO/IEC 27001 – samotný systém ISMS
- ISO/IEC 27002 – praktická opatření a postupy využívané především při navrhování bezpečnostních politik IT aktiv
- ISO/IEC 27005 – řízení rizika IT aktiv

Tyto normy organizace při zavádění ISMS používají vždy. Podle toho ale co přesně dělají a jaké cíle si pro implementaci tohoto systému kladou, volí další doplňkové normy pro posílení schopnosti ISMS v dané oblasti.

Proces certifikace, jak je naznačen na obr. 2.1, odpovídá také struktuře normy ISO/IEC 27001. Obsahuje v sobě základní rámec procedur a činností, které je nutné pro zavedení **ISMS** v organizaci zvládnout. Podrobnosti pak řeší pro danou oblast upřesňující normy (např. ISO/IEC 27002 a 27005).

přiját, nemají charakter vnitropodnikového předpisu, ale pouze podpůrné dokumenty. Jedná se o operativní dokumenty, které jsou dále používány při přijetí rozhodnutí o ten, co přesně má systém ISMS řešit. Toto rozhodnutí je formálně uděláno v předpisu *ISMS rozsah*.

Na základě rozsahu je pak formován první skutečný předpis, který má přímý dopad na bezpečnost informací a to *Politika systému ISMS*. Tato politika nastoluje základní obrysy fungování systému ISMS, především role a organizační struktury, které se mají podílet na plnění úkolů v rámci tohoto systému. Politika také stanovuje základní obrysy procesů, které zajistí funkce tohoto systému.

Politika systému ISMS je strategickým dokumentem. Neočekává se proto, že bude řešit detaily fungování tohoto systému. Podrobnosti budou řešeny samostatnými politikami, které budou již úžeji zaměřené a budou pak určitý problém řešit podrobněji.

Pro návrh takových politik ale v rámci systému ISMS potřebujeme další informace (další přínosy v rámci systému ISMS).

Všimněte si na obr. 2.1, že tento krok je spojen s ISO/IEC 27002. Je tomu tak proto, že ISO/IEC 27001 definuje pouze filozofii **ISMS**, zatímco další normy se zaměřují více na podrobnosti a náplň jednotlivých dokumentů.

Dalším krokem certifikačního procesu je *inventarizace informačních aktiv*. Tuto oblast normy řady 27000 v podstatě neřeší – tedy nemají formální požadavky na to, jak by inventarizace aktiv měla vypadat. Existují zde ale některé momenty, které můžeme použít k odvození základních vlastností, které by inventarizace aktiv měla obsahovat. Podrobnosti o rozsahu vedených informací a procesech si ale musí organizace rozhodnout a nastavit sama.

Inventarizace aktiv by měla být kontinuálním procesem. Důvodem je to, že neustále dochází k obměně výpočetní techniky (hardware), software. Mění se ale také lidé, kteří s nimi pracují, stejně jako data a požadavky na ně kladené a to funkční i bezpečnostní. Bezpečnost informací pak vyplývá (je determinována) interakcí všech těchto komponent. Může se také měnit úloha, jakou aktivum vykonává. Např. starší počítače je možné použít pro některé méně výpočetně náročné úkoly, kde mohou spokojeně se používají „dožít“ - tedy plní jinou úlohu, než pro kterou byly původně pořízeny. Systém inventarizace toto musí zohlednit.

V takto dynamickém prostředí proto nemůže žádný statický dokument obstát. Inventarizací aktiv a podpůrným software pro tyto účely se budeme zabývat v kapitole *Systém řízení konfigurací*.

Účelem inventarizace je tedy identifikovat všechna relevantní aktiva s dopadem na bezpečnost chráněných informací (dle Rozsahu ISMS) a způsobu jakým jsou využívána. Výsledkem je repozitář informací o aktivech, jejich současném stavu, případně pak historických údajů, které jsou využitelné velmi různorodým způsobem nejen v systému ISMS.

Tyto informace lze použít např. pro hodnocení efektivity investic do IT, hodnocení technické spolehlivosti systémů, dodavatelů apod. Takové přístupy dávají hluboký smysl z hlediska celkového řízení organizace, ale samy o sobě se netýkají přímo bezpečnosti informací.

Pro účely ISMS planí informace o aktivech zcela zásadní roli - poskytují základní podklady pro zpracování rizikových analýz. Pro tyto analýzy nám inventarizace identifikuje aktiva. Ta nám specifikují objekt zájmu, na který se budoucí analýza zaměří. Inventarizace nám také poskytne další informace použitelné pro návrh scénářů realizace hrozeb, případně historické údaje pro kvantifikaci pravděpodobnosti výskytu těchto hrozeb a případných dopadů realizace hrozby. Tedy poskytuje podklady pro specifikaci všech běžně používaných komponent modelu rizik.

Rizikové analýzy v systému ISMS řeší ISO/IEC 27005. Základní metodologie identifikace aktiva managementu rizik mají charakter vnitropodnikových předpisů. Oproti tomu samotný seznam aktiv a informací o nich je pouze podpůrný dokument, stejně tak analýzy rizik, které na základě nich budeme tvořit.

Na základě realizovaných analýz rizik a apetitu organizace k riziku musí organizace rozhodnout o tom, co a také kdy s jednotlivými riziky bude dělat. Toto rozhodnutí musí být formální a má charakter plánu. Tento plán označujeme jako **RTP**, česky *Plán zvládnutí rizik*.

Dalším důležitým dokumentem, který do této oblasti také spadá je **SOA**, česky *Prohlášení o aplikovatelnosti*. Tento dokument shrnuje požadavky norem, popř. další požadavky, které vyplývají např. ze smluvních závazků a specifikují, které části systému ISMS tyto požadavky řeší.

RTP i SOA jsou podrobněji rozebrány v kapitole ISO 27005.

Znalost rozsahu **ISMS**, rizik, která hodláme řešit a vhodnou volbou kontrolních kritérií jsou základními stavebními kameny k tomu, abychom mohli začít se samotnou implementací **ISMS**. Zavádění **ISMS** se neděje obvykle najednou pro všechny procesy a aktiva využívané danou organizací. Postupuje se spíše po částech. Pro každou část vytváříme samostatný projekt a k projektu plán implementace,

který posléze prakticky realizujeme.

Výsledkem je:

1. navržení bezpečnostní politiky daného procesu, aktiva nebo skupiny aktiv dle ISO 27 002
2. proces auditu
3. dokumentace kontrolních mechanismů
4. metriky pro kontrolu efektivity

Systém ISMS nám tak postupně nabíhá tak, jak v něm přibývají předpisy řešící jednotlivá problémové oblasti.

ISMS je sice integrovaný systém a tak ke své úplné funkčnosti vyžaduje úplnou implementaci. Stačí to ale ke spuštění **PDCA** cyklu (podrobněji níže) pro postupné zlepšování systému. Systém se tak s každou iterací PDCA bude zlepšovat na základě identifikovaných problémů a jejich postupného vypořádávání.

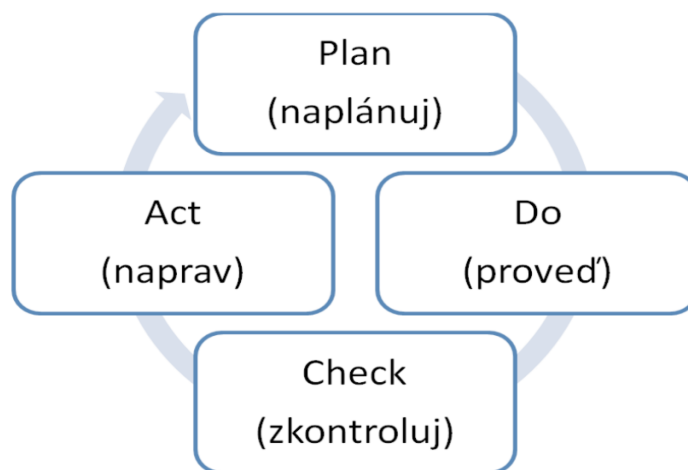
Bezpečnostním politikám se budeme podrobněji věnovat v následující podkapitole, co ale další dokumenty, které mají být výsledkem implementačního procesu? Opatření definovaná bezpečnostními politikami musíme podle něčeho kontrolovat. Za tímto účelem se navrhuje proces auditu. Tento proces nám říká, jakým způsobem proběhne kontrola toho, že implementovaná opatření řízení informační bezpečnosti, jsou implementována správně.

V ideálním případě lze použít vybrané metriky pro hodnocení naší úspěšnosti. Pro IT se nabízí metriky funkčnosti (systém běží) a dostupnosti (koncoví uživatelé jej mohou využívat). Podle kritičnosti lze také nastavit třeba požadovaný uptime chráněných systémů za rok apod.

Výsledkem realizace plánů v obecné rovině je zavedení **ISMS** systému do dané organizace. My už víme, že povaha hrozeb není statická, ale že se vyvíjí v čase. Podobně se v čase vyvíjí také samotná aktiva, která jsou v dané organizaci používána. To je důvod, proč ani systém **ISMS** nemůže být statický.

Pro vývoj/údržbu systému **ISMS** se používá postup známý pod zkratkou **PDCA**, tedy v českém překladu naplánuj - dělej - zkontroluj - naprav. **PDCA** také bývá někdy označován jako Demingův cyklus, podle W. E. Deminga, kterému se, nesprávně, připisuje autorství tohoto přístupu. Skutečným autorem je W. A. Shewhart, Deming byl Shewhartův žák a také velký popularizátor **PDCA** přístupu.

Je potřeba ale poznamenat, že **PDCA** je postup odvozený z mnohem starších manažerských postupů. Sheward a Deming je pouze exaktně popsali a aplikovali pro řešení řady problémů.



Obrázek 2.2: PDCA princip

Původní **PDCA** byl určen pro management, jako sled jednoduchých činností, které umožňují postupně zlepšovat kontrolu nad řízeným procesem. Kromě tohoto účelu však **PDCA** našel uplatnění v řadě dalších oblastí, jako je řízení kvality nebo také řízení bezpečnosti informací.

PDCA v sobě obsahuje motivaci pro revizi způsobu, kterým se provádí řízení informační bezpečnosti. Pokud si totiž nastavíme správně kontrolní mechanismy budeme schopni včas odhalit problémové oblasti a ty následně v Act části napravit modifikací našeho přístupu. V dalším kole PDCA pak hodnotíme, zda změny, které jsme provedli skutečně vedly ke zlepšení a zároveň zda-li tyto změny byly dostatečné.



Kontrolní otázky: 2.1 Systém ISMS

1. Co je to ISMS?
2. Co je účelem stanovení rozsahu a politiky ISMS?
3. Vysvětlete princip PDCA.
4. K čemu slouží RTP?
5. K čemu slouží SOA?

2.2 ISO 27002 – bezpečnostní politiky

V předchozí kapitole, jsme definovali několik dokumentů, které mají být v rámci **ISMS** zpracovány, zkusme si je tedy podrobněji rozebírá.

Dokument *Rozsah ISMS* je krátkým dokumentem, který definuje co chápeme pod pojmem ISMS. Je to pouze ochrana informačních aktiv v elektronické podobě používaných organizací, nebo chápeme ISMS širěji a budeme se snažit o zavedení integrované ochrany včetně informací třeba v papírové podobě, archivu apod.? Takové rozhodnutí je velmi závažné protože informace v různých podobách jsou vystaveny různým rizikům a proto také náročnost implementace a údržby takového systému bude odlišná.

Rozsah ISMS je z hlediska délky obvykle krátký (orientačně do 1 strany textu), zároveň se nepředpokládá, že by někdy v budoucnu docházelo k výraznějším změnám tohoto dokumentu, každá změna by totiž výrazně změnila celou filozofii ISMS v dané organizaci, z tohoto důvodu mohou být lhůty na revizi tohoto dokumentu delší.

Představme si situaci, kdy by k zásadní změně rozsahu ISMS skutečně došlo. Změna v takovém případě může jít směrem k začlenění dalších zájmových oblastí do rozsahu ISMS nebo naopak zmenšení tohoto rozsahu. Proces zavádění již známe (viz obr. 2.1) - co přesně se stane v případě výše uvedených změn?

Pokud rozsah ISMS bude rozšířen znamená to, že postupně musíme vyvinout novou dokumentaci pro do ISMS nově zařazená aktiva a procesy a to včetně:

- revize inventarizace aktiv
- identifikace hrozeb
- rizikové analýzy těchto aktiv
- revize přijatelnosti rizik ve světle nově provedených analýz
- revize Politiky ISMS
- implementace bezpečnostních politik do ISMS nově zařazených aktiv
- a další

Na změnu je pak potřeba vyčlenit zaměstnance a to stojí čas a peníze.

Je potřeba říci, že doplnění probíhá obvykle s výrazným časovým odstupem od doby prvotního zavedení systému ISMS. To znamená, že již nemusí být k dispozici podpůrná infrastruktura a lidský kapitál, které si pro zavedení systému organizace vyčlenila. Bude proto potřeba ji obnovit, což představuje další náklady navíc.

Provázanost s dalšími částmi systému ISMS také znamená, že revidovány budou muset být podstatně části již existujícího systému a to nad rámec běžných periodických revizí.

V případě, že se naopak rozsah ISMS zmenší, pak činnosti, které jsme realizovali pro získání kontroly nad těmito procesy z pohledu informační bezpečnosti byly prostým mrháním zdrojů, které jsme vyřazením z rozsahu ISMS odepsali.

Politika ISMS oproti tomu definuje základní proces ISMS, tedy jakým způsobem bude ISMS organizován. Oproti stanovení rozsahu ISMS se jedná o delší dokument, který definuje zejména:

- organizační struktury hrající úlohu v ISMS,
- přiřazuje jednotlivým významným strukturám role v rámci ISMS,
- definuje základní pojmy, které organizace používá.
- základní bezpečnostní principy, které souvisí s informační bezpečností

Výše uvedené principy bychom mohli také zobrazit formou stručné osnovy politiky ISMS:

1. Úvod

- Motivace pro zavedení ISMS
- cíl

- Komu je dokument určen (obvykle všem zaměstnancům)
 - Podle čeho je navržen (ISO 27002)
2. Slovník pojmů – pouze zásadní pojmy využívané politikou
 3. Organizace bezpečnosti
 - Z pohledu ISMS důležité organizační struktury (oddělení IT, management, fyzická bezpečnost, IT bezpečnost <- každá organizace má jinak)
 - Role a základní pravidla (jen to co je relevantní pro ISMS) – může se jednat o CEO, CIO, CISO, administrátory, auditory, architekta KB, běžné uživatele.
 4. Návaznosti na další procesy systému ISMS
 - Řízení IT aktiv
 - Řízení rizik
 - audit
 - Tvorba politik aktiv
 - Jen velmi stručně cíl + odkaz, kde je to řešeno. V politice ISMS rozhodně neřešit podrobně
 5. Proces schvalování/modifikace politik - kdo se ho účastní, jak to probíhá
 6. Bezpečnostní incident
 - Obecný postup řešení
 - Možnost objednání externích konzultací (např. pro CISO)
 - Kázeňské postihy (pouze v obecné rovině)
 7. Závěrečná ustanovení
 - Kdy vchází v platnost
 - Revize politiky

Co tedy přesně má politika **ISMS** obsahovat? V úvodní části se společnost obvykle hlásí k řízení informační bezpečnosti a zároveň definuje podle čeho se bude řídit. V našem případě se jedná o ISO/IEC 27002.

Pokud je organizace povinnou osobou dle zákona O kybernetické bezpečnosti, pak by se k této povinnosti měla přihlásit už v úvodu. V tomto případě se ale obvykle uvádí také vyhláška, podle které se postupuje tedy 408/2025 Sb. nebo 409/2025 Sb. podle toho jestli se na organizaci vztahuje nižší nebo vyšší úroveň regulace.

Pokud organizace v rámci ISMS řeší taské požadavky jiné legislativy, měla by se k ní přihlásit v úvodu také. Jedním z účelů formálně nastaveného systému ISMS je prokázat soulad (compliance) s požadavky legislativy. Z tohoto pohledu je dobré mít jedno místo, kde se všechny tyto odkazy shromáždí a na které v případě kontroly budeme moci ukázat a říct - splňujeme.

Požadavky jiné legislativy ale nutně nemusí být řešeny systémem ISMS. Organizace často volí samostatné předpisy. Problematiku odlišných požadavků různých zákonů a vyhlášek pak mohou řešit nezávisle, což by v případě realizace jedním předpisem nešlo.

Dále následuje organizace **ISMS**. Do této kapitoly můžeme zařadit definici role **CISO** nebo někoho, kdo bude zodpovědný za informační bezpečnost. **CISO**, ale při řízení informační bezpečnosti, jak již víme, není osamocen - svou úlohu mají také oddělení (útvary, úseky, ...) informačních technologií, fyzické bezpečnosti, popřípadě další v závislosti na zvoleném způsobu řešení. Do této kapitoly patří také definice role Výboru KB.

Musí být definovány také klíčové bezpečnostní role, především *architekt kybernetické bezpečnosti*. Architekt navrhuje plánuje a koordinuje bezpečnostní infrastrukturu organizace.

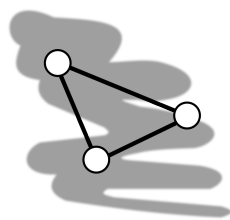
Další klíčovou rolí je *auditor*. Zde je kladen obzvláště velký důraz na odbornost osoby auditora, tedy schopnost identifikovat a popsat problém a také nezávislost osob vykonávajících tuto roli.

V případě Výboru, bychom ale také mohli definovat jeho jmenování, pravomoci a způsob práce, pokud nemá Výbor vlastní statut, tedy samostatný dokument, který tyto věci definuje. Pokud existuje statut rady můžeme se v Politice ISMS omezit na prosté začlenění tohoto Výboru do širší organizace bezpečnost informací a pro podrobnosti se na tento statut odkázat.

Kromě výše uvedených funkcí a organizačních struktur politika obvykle obsahuje také definici roli administrátora a také běžného uživatele. Politika ISMS s těmito rolmi zachází velmi obecně - běžným uživatelem tak rozumíme jakéhokoliv uživatele řízených systémů organizace, které ke své činnosti nevyžadují zvýšená (administrátorská práva).

Podobně administrátor se v obecné rovině obvykle stará o svěřená informační aktiva a řeší bezpečnostní incidenty.

Z pohledu práv a povinností těchto generických rolí můžeme např. specifikovat, že uživatel má



Návaznosti

Pro nové vydání skript jsme připravili také samostatné komentované šablony základních předpisů v systému ISMS. Šablony naleznete na LMS v kurzu *Bezpečnost informačních systémů*, ale jsou dostupné také na portálu e-výuka a na mých domácích stránkách [83].

právo na to, aby informační aktivum pracovalo tak jak má a uživatel tak mohl vykonávat své pracovní povinnosti. Mohou zde být také obecná omezení že aktiva je možné využívat pouze k plnění pracovních povinností, že při využívání je nutné dodržovat platnou legislativu, apod.

Pro administrátory lze specifikovat, že jednotlivý uživatelé, využívající administrátorem spravované aktivum musí dbát pokynů administrátora apod.

Politika ISMS by také měla obsahovat základní definice procesu řízení rizik, popřípadě další funkce, které souvisí s řízením informační bezpečnosti jako je inventarizace, reakce na bezpečnostní incidenty apod. Politika ISMS, ale tyto oblasti neřeší do podrobností, pouze je zasazuje do širšího kontextu řízení informační bezpečnosti jako takové. Podrobnosti samotné politika ISMS ponechává na specializovaných vnitropodnikových předpisech, na které se může přímo odkazovat a to i v případě, že v době přijetí politiky tyto navazující předpisy ještě neexistují.

Tomuto přístupu říkáme *policy first*. Znamená to, že návaznost zde sice v první fázi není, ale odkaz na tento neexistující předpis sám o sobě zaručuje vznik rozporu mezi očekáváním a realitou, se kterým lze efektivně pracovat v PDCA cyklu. Iteracemi PDCA pak postupně doplníme chybějící věci.

Použití tohoto přístupu také zajistí, že jediná změna, kterou budeme potřebovat udělat bude doplnění chybějících dokumentů. Kdyby jsme měli napsán předpis tak, že nepočítá s existencí chybějících předpisů, museli bychom přidat nový předpis a pak hledat všechna místa existujících předpisů, které by na něj měly odkazovat a tyto odkazy tam doplňovat. Jinými slovy rozsah potřebné revize by byl výrazně větší.

Pokud organizace provádí klasifikaci dokumentů podle důvěrnosti pro interní použití (nemyslí se klasifikace údajů podle zákona 412/2005 Sb. O ochraně utajovaných informací [1] – viz upozornění níže), pak základní principy této klasifikace jako jsou např. stupně ochrany, by měly být v politice ISMS taktéž obsaženy.

Příklad jednoduchého členění informací podle důvěrnosti:

- veřejné
- neveřejné
 - neveřejné
 - obchodní tajemství
 - strategické dokumenty
 - ...

Politika ISMS obsahuje dále obecné ustanovení vyžadující pravidelné revize jednotlivých dokumentů zařazených do bezpečnostní dokumentace.

V případě, že daná organizace pracuje s informacemi v nějakém stupni utajení, musí být tato skutečnost zohledněna také v politice ISMS.



Informace v některém ze stupňů utajení

Z hlediska organizace bezpečnosti se jedná o jeden z nejsložitějších problémů. Systémy, které budou takové informace zpracovávat totiž musí být certifikovány. Pro získání certifikátu je nutná realizace opatření, která definuje zákon 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní způsobilosti [1].

Certifikaci samotná provádí **Národní bezpečnostní úřad (NBU)** podle Společných kritérií [3]. Také ty v sobě obsahují určité nároky, které je nutno při řízení informační bezpečnosti brát v úvahu.

Prohlášení o aplikovatelnosti (SOA) vychází primárně z přílohy A ISO 27001, která obsahuje tzv. *kontroly*. Kontrolou v tomto kontextu rozumíme bezpečnostní opatření, která slouží ke snižování rizik v oblasti bezpečnosti informací.

Příloha A obsahuje celkově 93 opatření ve 4 oblastech:



Politika ISMS – semestrální projekt

Z tohoto důvodu, až budete psát politiku ISMS jako semestrální projekt, se ochraně utajovaných informací nevěnujte (předpokládejte že organizace utajované informace nemá).

Pokud návaznost na utajované informace v dokumentu bude existovat - bude při hodnocení semestrálního projektu vyžadováno splnění této návaznosti (do čehož se nechcete pouštět)!

- organizační
- lidské zdroje
- fyzická opatření
- technologická opatření

Některé další normy kodexu ISO 27000 obsahují dodatečné kontroly, které pak v případě potřeby do prohlášení doplňujeme také. Dodatečné normy volíme podle záměrů (cílů) organizace se systémem ISMS, podle zvoleného rozsahu. Dodatečná opatření, která organizace musí implementovat mohou také vyplývat z potřeby vyhovět požadavkům externích subjektů. Např. ze strany státu takové požadavky budou vycházet z legislativy. Požadavky mohou také pocházet od smluvních partnerů. V takovém případě budou vycházet ze smluvních pojednání.

Všechny tyto požadavky se konsolidují na jednom místě do prohlášení SOA. Různé zdroje požadavků v SOA pak obvykle mají samostatné sekce umožňující rychle a jednoznačně identifikovat zdroj daného požadavku. U každého požadavku (kontroly) organizace rozhoduje:

- zda se jí daný požadavek týká (je aplikovatelný, odtud název celého dokumentu)
- pokud se jí týká tak, jaký dokument v systému ISMS toto opatření řeší

SOA je tak vynikajícím východiskem pro realizaci plánování implementace celého systému ISMS do organizace a po jeho implementaci také pro realizaci auditů.

Bezpečnostními politikami rozumíme dokumenty upravující bezpečnostní aspekty použití IT aktiv v dané organizaci. Bezpečnostní politiky koncipujeme tak, aby svými ustanovení pokrývaly jedno, vybrané IT aktivum, nebo skupinu IT aktiv s podobnými vlastnostmi.

Ve srovnání s Politikou ISMS je tedy hlavní rozdíl v zaměření na konkrétní aktivum nebo skupinu aktiv. Lze také říci, že bezpečnostní politika aktiva implementuje Politiku ISMS pro potřeby řízení informační bezpečnosti tohoto aktiva (procesu, problémové oblasti).

Bezpečnostní politika obsahuje:

1. deklaratorní část
2. slovník pojmů
3. samotná opatření bezpečnostní politiky
4. závěrečná ustanovení
5. kdy vstupuje politika v platnost
6. plán revizí, pokud se interval revize liší od intervalu definovaného v politice ISMS

Základní strukturou je bezpečnostní politika aktiva podobná Politice ISMS ovšem s tím, že se nezabývá organizačními strukturami a podobnými „vysokoúrovňovými“ problémy.



Tip: pojmenování politiky aktiva

To, že píšete bezpečnostní politiku aktiva neznamená, že se musí jmenovat *Bezpečnostní politika aktiva*! Jde o to, že název samotný by měl naznačit to, čím se bude dokument zabývat. Proto buďte alespoň trochu kreativní, pokud řešíte politiku místnosti s kontrolovaným vstupem, jako je např. serverovna můžete zvolit třeba název: *Provozní řád serverovny*.

Pokud řešíte problematiku bezpečnosti notebooků, můžete politiku nazvat: *Bezpečnostní politika notebooků*.

Bez ohledu na to, jaký název ve finále zvolíte - buďte konkrétní!

V deklaratorní části organizace deklaruje svůj záměr řešit informační bezpečnost daného aktiva nebo skupiny aktiv, zároveň je zde prostor k definování návaznosti na další předpisy a dokumenty, ze kterých se při tvorbě politiky vychází. Z norem to v tomto případě bude ISO/IEC 27002, z vnitropodnikových dokumentů by to měla být Politika ISMS. Lze odkazovat také jiné dokumenty ať už jiné vnitropodnikové předpisy, legislativu, normy nebo procesy, které jsou pro danou politiku relevantní.

Odkazované dokumenty by měly být jednoznačně identifikovatelné, zejména pokud se jedná o vnitropodnikové dokumenty. Prakticky je tento problém řešen zaváděním řízené dokumentace, kde jsou jednotlivé dokumenty označovány unikátním číslem. Dokumenty je pak následně podle těchto čísel možno dohledat buďto elektronicky na portálu sloužícím ke zveřejňování nebo v papírové podobě u správce dokumentace.

Slovník pojmů se přikládá do bezpečnostních politik z důvodu zajištění jednoznačnosti výkladu ustanovení politiky. Jednotlivé pojmy totiž mohou být vykládány různě v různých kontextech → pokud naším cílem je zajistit, aby bezpečnostní politika byla dodržována a také vymahatelná, jednoznačnost výkladu je jedním z nejdůležitějších momentů, na který při tvorbě bezpečnostní politiky je nutno brát zřetel.

Zbytek náplně je přímo závislý na způsobu, jakým je nastavena informační bezpečnost. Osnova zbytku politiky by proto mohla (ale nemusela) vypadat například následovně:

1. specifikace rolí uživatelů chráněného aktiva (jejich práva a povinnosti)
2. mechanismus vytváření a rušení uživatelských účtů aktiva (pokud není řešeno centrálně návazností na **IDM**)
3. specifikací dalších procesů, které mají význam z hlediska informační bezpečnosti (měly by vyplynout z rizikové analýzy daného aktiva)
4. závěrečná ustanovení
5. kdy politika vstupuje v platnost
6. plán revizí (pokud se interval odlišuje od intervalu definovaného v politice **ISMS**)
7. změnový list

Role se primárně vztahuje k IT aktivům typu IS, kde může být velké množství různých rolí s různými přístupovými právy k objektům IS. S každou rolí proto mohou být spojeny odlišné postupy vedoucí k zajištění bezpečnosti informací zpracovávaných v IS.

Příkladem může být třeba IS EDISON. V něm existují role jako je student, studijní referent, garant studijního programu, garant oboru, vyučující a řada dalších. Jednotlivé role se výrazně liší rozsahem práv k systému, ale také způsobem jeho použití.

V některých případech, ale takto podrobné členění není potřebné. U běžných webových aplikací, řešených na bázi **CMS** může stačit rozlišení mezi administrátorem spravujícím systém a připravujícím obsah serveru a uživatel, který bude obsah „konzumovat“

Vytváření a rušení uživatelských účtů k systému je další oblastí, která může tvořit podstatnou část bezpečnostní politiky aktiva. Jednotlivé účty totiž identifikují uživatele systému, kteří mají v systému určité role, využívají systém určitým způsobem. Pokud toto nastavení nebude provedeno správně - výsledkem bude uživatelský účet, který má menší práva než jsou práva potřebná k výkonu pracovních povinností uživatele nebo naopak účet s vyššími než potřebnými právy. Takový účet pak představuje bezpečnostní riziko.

Tato část bezpečnostní politiky by měla zodpovědět otázku, jak se administrátor spravující účty dozví, že má účet vytvořit a s jakými právy a při změně role nebo zániku role pak zodpovědět otázku, jak se dozví že účet má být zablokovat nebo smazat (popř. že se mají změnit uživateli práva).

Tato problematika přitom nemusí být nutně zpracovávána pomocí bezpečnostní politiky. Proces vytváření/blokování účtu v chráněném systému může být zpracován v rámci např. ISO 9000 při dokumentaci určitého pracovního procesu, který dané IT aktivum extenzivně využívá. V takovém případě by ale na tento dokument bezpečnostní politika měla odkazovat.

Druhou možností je realizovat management účtů na jiném místě, v jiném systému. Tím může být systém **IDM**. V takovém případě aktivum funkce pro vytváření a správu uživatelských účtů buďto vůbec nemá nebo ji nevyužívá - účty a práva k nim jsou přejímány ze systému **IDM**. Z pohledu bezpečnostní politiky je přejímáním údajů z jiného systému situace zjednodušena - do bezpečnostní politiky stačí zapsat, že účty jsou přejímány z **IDM** a problém je tím pádem vyřešen.

Bezpečnostní politika může vzhledem k chráněnému aktivu obsahovat řadu dalších postupů, např. zavedení postupů kontroly toho, že daný WWW server je online a poskytuje své služby v očekávaném čase odezvy, nastavení spouštění udržovacích skriptů apod.

Tyto postupy, opatření a aktivity jsou přitom obvykle unikátní pro řízené aktivum a proto není možné taková opatření zobecnit a zařadit je do tohoto textu.

Závěrečná část politiky aktiva stanovuje obvykle platnost politiky a případně také určuje termíny revize, zejména v případě, že je předpokládán čas revize odlišný, než ten, který určila Politika ISMS.



Kontrolní otázky: 2.2 Bezpečnostní politiky a prohlášení o aplikovatelnosti

1. Co je to SOA a k čemu slouží?
2. Vysvětlíte rozdíly mezi politikou ISMS a bezpečnostní politikou IT aktiva.
3. Proč je nutné provádět pravidelné revize politik?
4. Podle čeho se řídíme, pokud IT aktivum pracuje s utajovanými skutečnostmi?

Před tím, než se pustíme do rozebírání možných jednotlivých typů bezpečnostních politik a jejich obsahu, zastavme se na chvíli u požívaných formulací. Zejména pro začátečníky v této oblasti jsou právě používané formulace poměrně zásadní problém, protože způsob jakým nějaký požadavek napíšeme často rozhodne o tom, zdali toto opatření bude účinné, nebo ne.

Opatření samotné tedy může být správné, ve správné politice, na správném místě této politiky, přiřazeno ke správné roli a přesto může být zformulováno tak, že bude nevymahatelné.

Právě vymahatelnost je totiž klíčovou vlastností vnitropodnikových předpisů. Pro zajištění této vymahatelnosti je potřeba požadavky velmi pečlivě formulovat. K tomuto účelu pak často potřebujeme používat slovní obraty a formulace, které v běžné mluvě příliš nepoužíváme.

V běžné mluvě třeba často používáme obraty jako že: „se něco nějak obvykle dělá“. O věci v tomto případě mluvíme popisným způsobem. Takové formulace mohou posloužit jako popis filozofie procesu (což je samo o sobě významné), ale tento proces nečiní **vymahatelným**. Pokud má formulací vzniknout nějaká povinnost, je to obrovský problém.

Všechny prvky politiky, které potřebujeme vymáhat - což je většina, protože jinak by nemělo smysl vytvářet vnitropodnikový předpis a stačil by nám nějaký postup nebo instrukce - musí být mapovány na nějakou roli (princip adresnosti) a musí být formulován tak, aby bylo patrné, jestli dané ustanovení je povinné (role **musí** něco dělat nebo naopak nedělat) nebo pouze doporučené (role by **měla** nějak postupovat).

Pro zajištění jednoznačnosti musí být role někde definovány. Obvykle je to v části za úvodem, kterou věnujeme organizaci dané problematice. Tento problém lze řešit ale také jinak, např. odkazem na jiný předpis, poznámkovým aparátem dle způsobu, jakým organizace obvykle připravuje své vnitropodnikové předpisy.

Nepředpokládejte tedy, že zaměstnanci budou podrobně analyzovat vnitropodnikový předpis a hledat v něm, co přesně mají dělat. To, co chceme aby zaměstnanec vykonával, musí být jednoznačné a na první pohled patrné z textu předpisu.

Vymahatelnost lze také podpořit přidáním odpovědnostní matice **Responsible Accountable Consulted Informed (RACI)** nebo některé z jejích variant, např. RASCI. Pokud se rozhodneme tento nástroj použít, vkládáme matici na konec předpisu. Pozor, tato matice nenahrazuje text předpisu, pouze jej shrnuje! (To je další častá chyba, se kterou se setkáváme také v praxi.)

V RACI může být nějaký úkol - něco má daná role dělat. Pro výkon samotný ale obvykle potřebujeme podrobnosti o tom **jak** má být tento úkol plněn. Tuto informaci ale RACI nemůže poskytnout! Z tohoto důvodu musí být každý úkol popsán přímo v textu předpisu.

2.3 Vybrané doporučené typy bezpečnostních politik a jejich obsah

V literatuře se objevuje celá škála různých typů bezpečnostních politik, které jsou implementovány v organizacích. Potřeby organizací jsou tak obvykle velmi různorodé, přesto lze vysledovat některé typy politik, které implementuje většina organizací:

1. Politika sociálních médií (popř. politika médií obecně)
2. Malware (popř. specializované politiky pro jeho jednotlivé typy)
3. Cloudové služby
4. Zpracovávání dat

5. Zařízení **Internet of Things (IoT)**
6. Politika **Bring Your Own Device (BYOD)**
7. Politika AI

Prosím berte v úvahu, že se v žádném případě nejedná o úplný výčet všech možných typů politik. Chybí zde např. politiky aktiv, které jsme poměrně často zmiňovali v předchozím textu. Existují také celé repozitáře šablon a vzorových politik. Jednou z největších je repozitář spravovaný SANS Institute [65], kde naleznete několik desítek šablon k využití.

Společnosti, které poskytují podporu a konzultace při zavádění systému ISMS obvykle vytvářejí vlastní repozitáře šablon politik, které navíc berou v úvahu specifika právního prostředí v daném státě.

Politika sociálních médií

Řeší způsob, jakým je v rámci organizace manipulováno se sociálními médii. Tato politika může být zaměřena jak na osobní použití sociálních sítí, tak na korporátní použití takových sítí.

Motivace organizace v této oblasti obvykle spočívá ve snaze udržet nebo vybudovat určitý mediální obraz společnosti. Takový obraz pak mohou narušit nejen nevhodné příspěvky na oficiálních účtech organizace na sociálních sítích, ale také příspěvky jednotlivých zaměstnanců na jejich soukromých účtech, alespoň pokud je možno je nějakým způsobem spojit s organizací.

Opatření politik by se měla týkat základních bezpečnostních otázek užití sítě tak, aby se předešlo ke ztrátě kontroly nad účtem. Při ztrátě kontroly nad účtem totiž není možné zajistit víceméně nic - organizace obsah zveřejňovaných příspěvků v takovém případě nemá možnost jakkoliv ovlivnit.

Některé sociální sítě mohou být také využívány pro autentizaci jednotlivých uživatelů k určitým službám - v takovém případě může být dopad na bezpečnost organizace dokonce přímý.

V některých případech může být vyžadováno po uživateli ze strany zaměstnavatele zveřejnění prohlášení o tom, že přestože jsou zaměstnanci, prezentovaný názor je jejich vlastní a nemusí nutně zcela korespondovat s názory organizace jako celku. Prohlášení může také obsahovat dovětek že sliby, termíny apod. učiněné zaměstnancem nejsou pro organizaci závazné.

Obsah prohlášení obvykle specifikuje právník a také rozhoduje o tom, kdy bude vyžadováno tak, aby se organizace maximálně chránila. Pro zajištění vymahatelnosti je ale nutné, aby organizace tuto povinnost zakotvila do některého vnitropodnikového předpisu, tedy např. politiky sociálních médií.

Takové postupy se často používají pro e-mailovou komunikaci, ale také příspěvky v diskuzních fórech, videa na TikTok, YouTube apod.

V korporátní verzi politiky by měly být specifikovány postupy zveřejňování příspěvků - především *kdo*, *kdy* bude *jaké* informace zveřejňovat. Podstatnou složkou musí být také následná moderace média beroucí v úvahu možnost reakce na příspěvek.

Internet je plodným místem pro vznik *dramat*. Většinou stačí nevhodná věta nebo jenom vyjádření, které je možno vykládat různým způsobem. Organizace by měla mít možnost identifikovat problém při jeho vzniku a případnými doplňujícími vyjádřeními minimalizovat následky na svém mediálním obrazu.

Pokud ale toto má fungovat, musí existovat v organizaci procesy, které si takovou přípravu vynutí.

Zrovna pro mediální politiky existuje ohromné množství příkladů pro organizace různého zaměření i velikosti, viz: <http://socialmediagovernance.com/policies/>.

Osobní politika sociálních médií by mohla obsahovat následující:

- obecné procesy – obecná pravidla a schvalovací procesy týkající se zveřejňování informací v rámci organizace
- zakázaný obsah – jaký typ obsahu se v žádném případě nesmí zveřejňovat na sociálních médiích
- doporučení k bezpečnému užití médií – např. pravidelná změna hesla, multifaktorová autentizace, ...
- osobní užití – za jakých okolností může zaměstnanec využít prostředky organizace pro osobní užití. Může být vyžadováno např. použití nějaké formální deklarace, že se jedná o osobní názor v případě, že se použije firemní mail apod.
- způsob hlášení, pokud zaměstnanec na takovém médiu najde citlivé materiály organizace
- ochrana dat a monitorování – pokud budou použity nástroje pro monitorování použití takových prostředků je potřeba to deklarovat předem (jinak se jedná o výrazné narušení soukromí)
- sankce

Politika sociálních médií pro korporátní účty by mohla obsahovat:

- Odpovědnosti – kdo odpovídá za které sociální médium

- Pravidla, jak reagovat na zpětnou vazbu k příspěvkům (např. komentáře)
- Pravidla reakce na falešné účty na soc. sítích, které se tváří jako oficiální
- Další specifické otázky podle způsobu použití sociálního média
 - např. pokud jsou pořádány soutěže – potřeba řešit zasílání/předávání cen, případné podvody
 - atd.

Malware

Různé typy útoků viry, popř. jinými druhy škodlivého kódu jsou pro organizace na denním pořádku. Z toho důvodu si také potřebují vytvořit určité procesy pro reakci na tyto události. Hlavním motivačním faktorem pro vznik takových politik je v posledních letech zejména rozšíření tzv. *ransomware*, který šifruje data na discích napadených počítačů, což v případě chybějícího nebo špatně vyřešeného zálohování a manipulace s daty může znamenat nevratné zničení signifikantní části dat v organizaci - dat která jsou kriticky důležitá pro chod organizace.

Otázky řešení politikou:

- Zálohování a proces obnovy dat
- Segregace dat – data by měla být zálohována na různých místech (zmenšení pravděpodobnosti poškození (všech) záloh v rámci bezpečnostního incidentu)
- Aktualizace antivirového řešení
- Anti SPAM řešení
- Blacklisting webových sídel (omezení možnosti připojit se k určitým typům sídel ze sítě organizace)
- Omezení v organizaci používaných programů – měly by být instalovány pouze programy, které jsou potřebné pro výkon práce, a které jsou podporovány.
- Omezení práv uživatelů - uživatel by víceméně nikdy neměl pracovat s administrátorskými právy k systému
- školení uživatelů
- apod.

Cloudové služby

pravděpodobně není potřeba představovat - používáme je pravděpodobně všichni, byť to může být v různém rozsahu. Pro organizace může být výhodné použití cloudů také jiným způsobem než je běžné pro jednotlivce - např. provoz serverů v cloudu zažívá v posledních letech výrazný boom.

Bez ohledu na to, kterého poskytovatele těchto služeb si organizace vybere zdroje rizik zůstávají stejné - jedná se o riziko výpadku služeb a bezpečnosti těchto služeb. Obojí je přitom mimo faktickou kontrolu organizace, protože infrastruktura je ve vlastnictví provozovatele cloudu. Možnosti konfigurace a kontroly nad během jsou tak nižší, než kdyby si daná organizace provozovala infrastrukturu tzv. *on premise*, tedy na místě.

Jediným momentem umožňujícím alespoň nějak poskytování služby ovlivnit je tak smlouva s poskytovatelem služby.

Politika by se tak měla zaměřit na postupy vedoucí k uzavření pro organizaci přijatelných podmínek o provozování služby.

- Specifikace očekávání od služeb (a jejich poskytovatelů)
- Revize standardních smluv poskytovatele služeb
- Proces výběru poskytovatele služeb
- Stanovení rozsahu služby
 - co má být poskytováno (ve smyslu povahy služby)
 - Úroveň služby (**Service Level Agreement (SLA)**)
- Uzavření smlouvy s poskytovatelem nebo poskytovateli

Situace s poskytovateli cloudových služeb je často komplikována tím, že kromě samotné smlouvy se zákazníkem provozovatel služby používá také další předpisy, které jsou pro odběratele služby závazné. *Politika přijatelného užití* služby (**Acceptable Use Policy (AUP)**) se lze představit bankovní terminologií nebo terminologií používané provozovateli telekomunikačních služeb a řadě dalších subjektů tzv. *obchodní podmínky*.

Tyto podmínky specifikují okolnosti a pravidla, za jakých je poskytována služba. V případě porušení podmínek ze strany odběratele může dojít až k vypovězení služby. Problém je, že organizace

mohou tyto podmínky měnit jednostranně. Své zákazníky sice musí na změnu upozornit, ale obvykle je zde pouze relativně krátká doba na reakci ze strany zákazníka. Migrace k jinému provozovateli cloudových služeb přitom není triviální ani levná a představuje nejen nutnost technologické změny v provozovaných službách organizace, ale také vyřešení řady právních problémů.

Součástí smlouvy může být také dohoda o úrovni poskytovaných služeb **SLA**.

Velmi často také poskytovatelé cloudových služeb zpracovávají zásady ochrany osobních údajů. Takové zásady jsou nutné, neboť v rámci infrastruktury poskytovatele jsou zpracovávány často údaje, které nejsou ve vlastnictví poskytovatele (vlastníkem je odběratel služby).

V zásadách je potřeba věnovat náležitou pozornou způsobu užití dat odběratele služby poskytovatelem služby. Za ideálních podmínek by měl být poskytovatel agnostický vůči datům, ale např. Google si u svých cloudových služeb ponechává možnost zpracování údajů pro reklamní účely což může, ale nemusí být přijatelné pro odběratele služby.

Zpracování dat

V moderních organizacích všech velikostí jsou zpracovávány překvapivě vysoké objemy dat. Řada ze zpracovávaných údajů přitom může být citlivých. Politikou zpracovávání dat ale nerozumíme ochranu dat v systémech organizace jako takových. Ne, že by nás tato problematika nezajímala - spíše očekáváme řešení této problematiky přímo v bezpečnostních politikách systémů uchovávajících takové informace.

Politikou zpracování dat tak řešíme otázky týkající se analytických procesů, které umožňují spojování údajů z různých systémů a odvozování dalších informací z nich.

Zvláštní zřetel je přitom potřeba dát na ochranu osobních údajů.

Obsah politiky je potřeba stanovit na základě účelu, za jakým jsou analytické práce v organizaci realizovány. Obecně rovině by měly obsahovat:

- etické otázky zpracování osobních údajů
- odkazy na předpisy řešící ochranu osobních údajů v organizaci
- způsob uložení zpracovávaných dat
- specifikaci okruhu uživatelů s přístupem k takovým datům
- nutnost **Non-Disclosure Agreement (NDA)** - smlouvy o mlčenlivosti o citlivých údajích, se kterými se pracovník může během anýz seznámit.
- apod.

Oblast řízení zpracování dat v organizacích se posledních letech významně rozšiřuje a to až do té míry, že některé organizace začínají zavádět celé systémy tzv. *data governance* [29]. Tato problematika ale svým rozsahem výrazně přesahuje možnosti těchto skriptů.

IoT

Zařízení **IoT** představují poměrně nový problém. Jedná se o různé senzory, popř. elektroniku, která nemá charakter klasického počítače, chytrého mobilního telefonu nebo tabletu, která jsou ale zároveň připojena do sítě nebo dokonce do Internetu a vyměňují si řadu informací mezi sebou a také často s cloudovou podpůrnou infrastrukturou výrobce těchto zařízení.

Problémem IoT je to, že jeho uživatelé jsou velmi různorodí a mají od těchto zařízení odlišná očekávání (podle druhu zařízení). Proto je nutné identifikovat všechny typy uživatelů a způsoby užití a pokrýt jejich bezpečnostní aspekty. V obecné rovině by politika měla řešit:

- šifrování komunikace mezi zařízeními mezi sebou a cloudovou infrastrukturou
- správa přístupu k datům a možnosti jejich zpracování
- oddělení sítě se zařízeními IoT od běžné počítačové sítě
- identifikace a mapování všech používaných IoT zařízení (předcházení neautorizovanému nasazování zařízení IoT)
- povolené užití zařízení
- nasazování firewallů, popř. antivirů
- aktualizace firmware a zejména pak provoz již nepodporovaných zařízení IoT
- apod.

BYOD

Dalším významným trendem současnosti je **BYOD** - tedy česky *přineste vlastní zařízení*. Jedná se o přístup, kdy organizace umožňuje použít pro plnění pracovních povinností osobní IT zařízení zaměstnance. Z praktických důvodů se nejčastěji jedná o mobilní telefony a notebooky, popř. tablety.

Motivace k BYOD ze strany firem je v tom, že uživatelé pořízená zařízení budou vyhovovat lépe jejich specifickým potřebám. Na pořízení pak organizace v lepším případě přispívá určitou částkou, v horším případě pak hradí celou částku uživatel sám.

Ekonomicky představuje proto BYOD poměrně významný přínos pro organizaci. Na druhou stranu však BYOD představuje pro organizaci také výzvu z pohledu bezpečnosti. U těchto zařízení totiž nelze zabránit užití pro soukromé účely, v domácnostech apod. - resp. je zde již jistota, že zařízení bude využíváno také pro soukromé účely. Zajištění bezpečnosti je proto komplikovanější.

Politika BYOD proto obvykle obsahuje:

- Podmínky užití zařízení
- Základní požadovaná konfigurace zařízení a jeho podpora ze strany zaměstnavatele
- Finanční kompenzace za užití vlastního zařízení (výše, způsob uplatnění, apod.)
- Bezpečnost
- Rizika a odpovědnost zaměstnance užívajícího zařízení

Všimněte si odpovědnosti výše. V případě BYOD ve skutečnosti zaměstnanec nese odpovědnost za všechny osoby, které užívají dané zařízení, tedy např. včetně rodinných příslušníků - pokud mohou dané zařízení nějakým způsobem užívat.

Problémem je také správa takových zařízení. Zaměstnanec nemusí být vybaven dostatečnými znalostmi na to, aby své zařízení dokázal z pohledu bezpečnosti efektivně spravovat. Organizace disponuje infrastrukturou pro správu zařízení, ale zařízení BYOD jsou ve vlastnictví zaměstnanců a tak na ně organizace za normálních okolností nedosáhne.

Často postupujeme tak, že organizace prezentuje možnost využití podpory i pro soukromá zařízení, jako zaměstnanecký benefit. Zaměstnanci pak dobrovolně využívají této možnosti. Vhodným místem pro vyřešení organizace tohoto vztahu je právě politika BYOD.

Politika AI

Posledním typem politiky, který v této podkapitole probereme je *Politika AI*. AI v posledních letech zažívá bezprecedentní boom. Vývoj v této oblasti navíc natolik rychlý, že z pohledu organizací i jednotlivců se oblast AI již několikrát zásadně změnila a každá z těchto změn pak přinesla určité bezpečnostní otázky, které je potřeba řešit systémově - tedy v podmínkách organizace nějakým předpisem nebo politikou.

Nejprve přišly chatovací aplikace, jako je ChatGPT a další. Bezpečnostním problémem, který z nasazení takových aplikací vyplývá spočívá obvykle v tom, že AI běží na cloudové infrastruktuře plně pod kontrolou provozovatele AI. Všechny zpracovávané informace předávané do aplikace, nebo alespoň jejich podstatná část, jsou dále analyzovány a využívány pro další trénink AI. To je problém, pokud zaměstnanci budou do AI vkládat citlivé údaje.

Následně byla AI úzce integrována do vývojových nástrojů. Dospěli jsme do stadia, kdy je software z větší části vyvíjen buď přímo pomocí AI nebo alespoň s asistencí AI. Pro nasazení tohoto typu AI ale musí mít AI zajištěn přístup k vývojovým nástrojům, které může využít pro účely vývoje. Někdy v této souvislosti hovoříme o tzv. *kódovacích agentech*.

Problém s tímto přístupem je v tom, že tyto nástroje jsou velmi mocné a při nesprávném použití mohou být značně destruktivní. Z tohoto důvodu potřebujeme zajistit striktní oddělení vývoje a testování na straně jedné a provoz (běžné nasazení v produkčním prostředí) na straně druhé.

Kód napsaný AI musí také být výrazně více testován, než kód vytvořený zkušeným vývojářem.

Problematika programování (vývoje software) je ale svým způsobem poměrně uzavřená, ve smyslu rozsahu problémů. Co když stejný přístup budeme aplikovat na běžné problémy, které denodenně řešíme v organizacích? Může se jednat o extrakci dat ze souborů, zpráv, příspěvků ze sociálních sítí. AI lze použít pro automatizaci celých workflow. V takovém případě je problém poměrně špatně ohraničený a jeho řešení jen velmi obtížně automaticky ověřitelné.

AI v současnosti v sobě nemá implementován tzv. *world model*. Jedná se o vnitřní model světa, který by umožnil AI predikovat následky, které navrhované řešení bude mít na tento svět. To je problém, protože tím pádem AI, alespoň v současnosti, nemá schopnost vyhnout se řadě katastrofických selhání, které by i špatně zaškolený zaměstnanec nepřipustil.

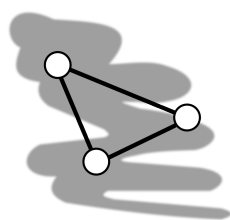
Na horizontu se pak objevuje úplně nový přístup označovaný jako *smyčka* (loop). Funguje to tak, že agent je opakovaně aplikován stejným způsobem ve stejném prostředí, aby se vypořádal s přicházející prací. Může se jednat např. o transformaci dat ze souborů, nebo cokoliv jiného. Tento přístup je natolik nový, že zde dosud ani nevidíme všechny možné dopady, natož abychom byli schopni je předvídat a bránit se jim.

Každý z výše uvedených způsobů práce AI a problémy a opatření z toho vyplývající se budou týkat různých skupin pracovníků organizace. Politika AI je místem, kde organizace na jednom místě může jasně specifikovat svůj postoj k bezpečnosti nasazení AI a konsolidovat všechny požadavky na zajištění bezpečnosti AI na jednom místě.

2.4 ISO 27005 – řízení rizika

ISO 27005 obsahuje základní vodítka pro provádění rizikových analýz a řízení rizika obecně pro účely řízení informační bezpečnosti. Svým pojetí (filozofií) vychází tato norma z kodexu norem ISO 31000 [11] [27], především pak normy ISO 31010, které se zaměřují na systémy řízení rizik obecně.

ISO 27005 ani ISO 31010 nepožadují použití určité přesně definované metody analýzy rizik. ISO 31010 ale může pomoci při výběru vhodné analytické metody tak, aby splňovala potřeby organizace. Volba metody samotné je ale přímo na dané organizace.



Pojetí rizik ISO 27005 a ISO 31010

Pozor obě normy definují riziko odlišně. ISO 27005 používá definici rizik, jak ji běžně chápeme v bezpečnostně orientovaných oborech, tedy pravděpodobnost nějakého **negativního** efektu charakterizována jeho následkem. ISO 31010 ale chápe riziko jako jakoukoliv odchylku od toho, co je považováno za normál - tedy **pozitivní i negativní**.

Obě normy proto nelze úplně zaměňovat, byť většina filozofie práce s riziky je zde stejná.

ISO 27005 je tedy obecnou normou aplikovatelnou v podstatě všechny typy organizací, metody analýzy rizika se však budou lišit oborově i typově.

Obecně si lze představit proces práce s informačními riziky podobně jako na obr. 2.3.

Obrázek 2.3 by Vám měl být povědomý – rizikové analýzy ani práce s informačními riziky se totiž neliší od práce např. s technologickými riziky. Tedy pracujeme v určitém uceleném kontextu, jehož vnímání se ale s časem vyvíjí tak, jak identifikujeme nová rizika nebo tak, jak se mění povaha těchto rizik popřípadě náš přístup k nim.

Informační aktiva je přitom potřeba vnímat v celém jejich rozsahu tedy jako hardware, software, ale také lidi, kteří s nimi pracují. Lidé jsou v tomto ohledu často tím nejslabším článkem, který se zároveň také nejhůře zabezpečuje.

Prvním krokem je *identifikace rizik*. Při identifikaci se vychází z inventarizace IT aktiv, ta by nám měla poskytnout seznam aktiv, které má daná organizace ve vlastnictví, nebo která využívá na základě třeba smlouvy o pronájmu nebo poskytování služeb a také služeb, které má dané aktivum poskytovat.

Inventarizace nám také poskytuje některé další informace také o způsobu, jakým jsou aktiva v organizaci používána, viz také podkapitola 2.1.

Následně lze použít některou z metod pro identifikaci rizik:

1. rešerše známých zranitelností obdobných aktiv v dané organizaci nebo i mimo ni,
2. průzkum/anketa na odhad hrozeb
3. analýza bezpečnostních incidentů spojených s daným aktivem
4. metody pro vizualizaci rizik a zkoumání jejich podstaty (např. brainstormin nebo Ishikawův diagram (diagram příčin a následků)).

Hrozbou v kontextu informační bezpečnosti rozumíme možnost využití zranitelného místa IS k útoku na něj s následkem způsobení škod na aktivech organizace. *Zranitelností* aktiva pak rozumíme existující místo aktiva, které je možno zneužít pro jeho napadení.

Při identifikaci rizik se snažíme nevymýšlet opakovaně již vymyšlené. V organizacích se využívá typově pouze omezené portfolio aktiv, proto zranitelnosti i rizika, kterým jsou tato aktiva vystavena, jsou obvykle známa a pouze pracujeme s adaptací jejich parametrů do podmínek dané organizace.

Také platí, že typově podobná aktiva, která využívá organizace jsou také využívány organizacemi jinými. Hrozby jsou v takovém případě často dobře zdokumentované. Společnosti zabývající se konzultacemi v oblasti řízení bezpečnosti informací pak disponují celými katalogy hrozeb, které využívají pro podporu analytických činností v rámci organizace.

Některé fragmenty takových katalogů je možné dohledat i na Internetu a podobné katalogy existují také pro zranitelnosti.

Bohužel ne všechny zranitelnosti jsou známy, popř. jsou známy všem zainteresovaným skupinám. Z tohoto pohledu zranitelnosti můžeme rozlišovat na známé a neznámé. Známé a neznámé však může znamenat spoustu věcí, podívejme se proto na životní cyklus zranitelnosti:

1. zranitelnost je objevena bezpečnostním výzkumníkem
2. podstata zranitelnosti s pokusným kódem demonstrujícím zranitelnost (*exploit*) je předána výrobci daného aktiva
3. podstata zranitelnosti je zveřejněna (je dostupná široké veřejnosti)
4. zneužívaná zranitelnost nulového dne (*zero day vulnerability*) - existuje škodlivý kód nebo v praxi zneužívaný vektor útoku na zranitelný systém
5. zveřejněn workaround výrobcem aktiva nebo bezpečnostními výzkumníky minimalizující škodlivé následky zneužití zranitelnosti
6. zveřejnění záplaty opravující zranitelnost
7. instalace záplaty na spravované IT aktivum - eliminace zranitelnosti

S výše uvedenou posloupností je jeden drobný problém – nemusí platit, resp. lze si jednoduše představit scénáře, kdy jsou některé kroky buďto zpřeházené nebo dokonce zcela chybí. Např. zranitelnost nemusí objevit bezpečnostní výzkumník (white hat), ale hacker (black hat). V takovém případě nelze předpokládat, že by výrobce aktiva byl informován o existenci takové zranitelnosti – dozví se o ní až analýzou způsobu úspěšné kompromitace jím vyvíjených systémů.

Bezpečnostní experti obvykle v případě objevení zranitelnosti ponechávají výrobci nějaký čas, aby zveřejnil záplaty před nebo zároveň se zveřejněním samotné zranitelnosti. Tato „doba hájení“ je obvykle 3 – 6 měsíců, ale nemusí být žádná, pokud expert nebude vidět dostatečnou snahu ze strany výrobce, nebo se mu výrobce prostě nebude líbit.

Většina společností vyvíjející operační systémy nebo široce nasazované programy má pro hlášení zranitelností a identifikovaných chyb v systému připraveny komunikační kanály a procesy pro práci s takto získanými informacemi. Některé společnosti dokonce za nahlášené chyby poskytují finanční odměnu.

V okamžiku zveřejnění podstaty zranitelnosti začíná závod mezi vlastníky zranitelného aktiva a případnými útočníky. Se zveřejněnou dokumentací zranitelnosti totiž útočník má podstatně lehčí práci při návrhu způsobu, jak zranitelnost zneužít. Pokud pro zranitelnost neexistuje záplata a zároveň je tato zranitelnost aktivně zneužívána útočníky - hovoříme o tzv. *zranitelnosti nulového dne*. Jediná přímá ochrana proti ní je odstavení celého aktiva nebo jeho zranitelné komponenty, což ale většinou není možné, protože by tímto způsobem byly odstaveny také služby, které aktivum poskytuje. Tyto služby jsou přitom pro provoz organizace obvykle potřebné.

Z tohoto důvodu se hledají alternativní řešení (workaround), který umožní minimalizovat dopady na dané aktivum.

Je ale potřeba říci, že nástup AI do jisté míry mění zaběhnutá pravidla hlášení incidentů. AI je totiž schopna nalézt větší množství zranitelností a umožňuje tak podstatně většímu okruhu osob nežli kdykoliv v minulosti takové zranitelnosti vyhledávat. Vedlejším efektem je to, že zranitelnosti jsou v současnosti hlášeny řádově vícekrát než kdykoliv předtím.

Problémem je, že většina identifikovaných problémů nepředstavuje závažné riziko z hlediska možnosti zneužití - to znamená, že většinu identifikovaných zranitelností je téměř nemožné zneužít v reálném provozu systému. Každý nahlášený problém ale musí být prověřen, replikován a analyzován aby se toto zjistilo. Jedná se tedy o poměrně náročný a nákladný proces. Vývojáři software se potřebují zaměřit na skutečně závažné zranitelnosti, které jsou také hlášeny, ale v záplavě nevýznamných, opakovaně hlášených zranitelností je problém je vůbec identifikovat.

Teprve poté se vytváří pro identifikovaný problém záplata a distribuuje se k uživatelům software.

Paradoxně tak lepší schopnost automatické identifikace zranitelností může vést k reálnému poklesu bezpečnosti provozovaných systémů a mohou vést také ke zvýšené frustraci samotných vývojářů. To je následek který vidíme v praxi již dnes a zatím nemáme k dispozici jeho uspokojivé řešení. Reálný dopad to má na tzv. *bug hunting programy* některých společností, které jsou vzhledem k množství problémů silně přetíženy a z tohoto důvodu jsou některé z těchto programů omezovány nebo dokonce ukončovány.

Vraťme se ale k identifikaci rizik - v případě, že daná organizace využívá nestandardní řešení, na které známá rizika nelze aplikovat, identifikujeme rizika zkoumáním různých vlastností aktiva.

Průzkum by měli provádět odborníci na všechny aspekty provozu daného aktiva tak, aby byly pokryty všechny oblasti, ze kterých by mohly plynout hrozby pro bezproblémový provoz aktiva.

Údaje o hrozbách spojených s provozem aktiva mohou být dostupné také v různých datových zdrojích archivovaných v dané organizaci. Zdrojem údajů mohou být např. různé logy. Předpokladem úspěchu je dostatečná historie dostupných údajů - jsou shromažďovány dostatečně dlouho a také ve formě, která umožní identifikovat typ události a odvodit z ní i její podstatu. Výhodou tohoto přístupu je také to, že je schopen zajistit dodatečné údaje o frekvenci výskytu dané události, což můžeme využítkovat při odhadu rizika.

Problémem v tomto ohledu je však zajištění statistické reprezentativnosti takových údajů. Pokud vzorek zachycených průvodních znaků realizace rizik v ložích není reprezentativní, pak zjištěné frekvence a z ní odvozená pravděpodobnost realizace rizika nebude správná. Výsledkem tak může být podcenění nebo naopak přecenění některých rizik, což bude mít přímý dopad na efektivitu řízení rizik.

Zpracování dostupných historických údajů by proto nemělo být jediným zdrojem informací o rizicích. Povaha rizik v IT je totiž vysoce dynamická, mohou se tedy také objevit rizika nová, zároveň mohou být některá rizika s malou frekvencí výskytu chybně zanedbána, protože je nebude možné v dostupných údajích identifikovat, protože se např. ještě v organizaci neobjevily.

Co se týče metod pro vizualizaci, tak metody brainstorming nebo Ishikawův diagram jsou nebo by měly být dostatečně známé. Existují dokonce softwarové nástroje, které tvorbu digramů podporují. Zmínit lze např. SmartDraw [19], který mimo jiné podporuje tvorbu Ishikawova diagramu nebo program FreePlane [28] pro jednoduchý záznam myšlenkových map.

Oba přístupy jsou si v zásadě poměrně blízké. Asi nejzásadnějším rozdílem je minimální počet diagramů, které můžeme použít pro plnohodnotného rozebrání rizik aktiva. V případě Ishikawova diagramu si prakticky nelze představit situaci, kdyby postačoval pouze jediný diagram pro plnohodnotné pokrytí rizik aktiva. Myšlenkové mapy je oproti tomu možné libovolně rozvíjet, kterýmkoliv směrem a to aniž by byla zásadně kompromitována pochopitelnost nebo použitelnost výsledného diagramu.

Samotná podstata zranitelnosti ovlivní způsob, s jakým s ní můžeme naložit. Některé příčiny totiž lze odstranit nebo minimalizovat jejich vliv, některé jsou našimi silami neovlivnitelné. Poznání podstaty zranitelnosti nám tedy umožňuje lépe nastavit RTP. Pozor, RTP nastavujeme až na základě plnohodnotné analýzy rizik na všech identifikovaných informačních aktivech.

Podstata zranitelnosti může být *fyzická* - v takovém případě je zranitelnost způsobena např. nevhodným fyzickým umístěním aktiva v prostoru, např. Klíčový server je umístěn na chodbě a je fyzicky dostupný prakticky komukoliv. Podstata zranitelnosti může být také *přírodní* (naturogenní). V takovém případě je aktivum zranitelné působením přírodních sil jako je povodeň, úder blesku apod. Tento typ zranitelnosti může, ale také nemusí souviset s fyzickým umístěním aktiva - to platí u povodní, kde na základě předchozích zkušeností však můžeme odhadnout pravděpodobnost této mimořádné události a přizpůsobit naše rozhodování o umístění aktiva.

Události jako je úder blesku apod. však ovlivnitelné nejsou¹.

Zranitelnost může mít však svůj původ také v nedokonalosti *hardware* (HW). Výrobci sice své komponenty fyzicky před vyskladněním testují, ale hardwarové selhání se přesto nedá vyloučit. Každá komponenta má navíc svou životnost, odhad její délky je však poměrně problematický. Pro komponenty výrobce (ale také servis) sleduje veličinu **Mean Time Between Failures (MTBF)** - průměrný čas mezi selháními komponenty. Tato veličina je však záludná, stejně jako ostatní veličiny, které pracují se zprůměrovanými hodnotami. Budou proto existovat kusy, které selžou velmi rychle a budou také existovat kusy, které naopak vydrží podstatně déle.

Jako alternativní veličinu pro odhad délky života komponenty lze použít nabízenou záruku - čím delší je záruka, tím vyšší předpokládá výrobce životnost komponenty. I tato veličina může být zavádějící. Výrobce totiž pracuje s určitým předpokládaným nasazením komponenty. Pokud např. výrobce předpokládá nasazení komponenty do běžného kancelářského PC a my jej použijeme ve velmi vytíženém serveru pracujícím 24/7 pak nelze předpokládat, že výrobcem odhadovaná doba životnosti bude skutečně dosažena.

Zranitelnost může být také obsažena v *software* (SW). Bude se jednat jednak o běžné chyby, kterým se během programování bohužel nedá úplně vyhnout². Většina chyb sice nebude zneužitelná → nevede tedy ke vzniku zranitelností, některé však zneužitelné jsou. Pokud je SW vyvíjen ve vlastní režii, pak

¹Žádné ze známých opatření proti úderu blesku „hromosvody“ není 100 % účinné, proto pokud bude budova zasažena bleskem nelze zaručit, že nevzniknou škody. IT je přitom na přepětí obzvláště citlivé. Podrobnosti o ochraně před bleskem lze najít např. v ČSN EN 62305 části 1 - 4 [73-76].

²Uvádí se, že dobrý programátor udělá chybu minimálně 1x za 100 řádků. IS mají běžně miliony řádků kódu.

lze pro minimalizaci doporučit TDD nebo metody tzv. agilního programování, které minimalizují počet závažných chyb již v průběhu programování.

Kromě toho je však nutné SW udržovat i během provozu. Nasazení v ostrém provozu může totiž odhalit problémy a chyby, které je potřeba odstranit. Tato údržba SW je velmi důležitá a měla by být realizována bez ohledu na to, zda SW vznikl z vlastních zdrojů nebo byl zakoupen od nějakého dodavatele.

Podstata zranitelnosti může být také fyzikální, v takovém případě často hovoříme o tzv. *postranních kanálech*. Jedná se o fyzikální efekty které má vykonávání určitých činností IT aktivem. Může se jednat třeba o elektromagnetické vyzařování (CRT monitory), může se jednat o zvukovou nebo optickou signalizaci datového přenosu u klasických modemů, zvuk (rytmus) úderu kláves, optický odraz, přenos vzduchem (WI-FI, Bluetooth, ...), drobné výkyvy v odběru elektrické energie v souvislosti s činností aktiva apod.

Proti některým z těchto postranních kanálů je možné se bránit nasazením vhodných technických opatření v místnostech, kde se aktiva používají. Musíme však brát také v úvahu aktiva jako jsou notebooky, tablety nebo chytré mobilní telefony, které jsou ze své podstaty přenosné a proto taková technická opatření nejsou nikdy 100 % účinná.

Podstata zranitelnosti může být a také často je v samotné *člověku samotném*. Zneužití aktiva může motivováno různě - nedbalostí, třeskutou hloupostí, ale třeba také zlým úmyslem a to buď samotné obsluhy, nebo z vnějšku manipulací ze strany zdatného sociálního inženýra. Podstatu zranitelnosti lidského činitele velmi dobře popisuje ve svých knihách jeden z nejznámějších hackerů Kevin Mitnick: Umění klamu [55] (vyšlo v češtině) a The Art of Intrusion [56], která bohužel vyšla pouze v angličtině.

Riziko samotné určujeme objektivně, opakovatelně a na základě pevně stanovené metodologie. Metodologii si každá organizace určuje sama, na základě svých zkušeností a požadavků na řízení rizika. S přípravou metodologie (tedy ne samotnými metodami analýzy rizik) nám mohou pomoci normy jako ISO 27005 nebo ISO 31010.

Fáze identifikace rizik je popsána výše v souvislosti s dalšími činnostmi, které organizace vykonává (inventarizace aktiv, apod.), podívejme se proto na alespoň krátký přehled metod, které lze pro účely hodnocení rizika použít.

Mezi nejpopulárnější metody lze zařadit **Event Tree Analysis (ETA)** nebo **Fault Tree Analysis (FTA)**. Obě metody by Vám měly být velmi dobře známy a obě jsou použitelné pro analýzu rizik IT aktiv. V oblasti informační, popř. kybernetické bezpečnosti se pak poměrně často používá metoda *Attack Tree* filozoficky odvozená z FTA, která je určena přímo pro tuto oblast.

Existuje celá řada dalších metod, které lze použít. Vliv lidského faktoru lze třeba zachytit pomocí **Human Reliability Analysis (HRA)** metody. Metody volíme podle charakteru hrozeb, kterým dané aktivum čelí, tedy tak, abychom byly schopni pokrýt podstatu zranitelnosti.

Metody volíme také především takové, které jsou nám, jako zpracovatelům, dobře známy. Teprve pokud portfolio metod neodpovídá portfolio hrozeb, které máme pokrýt, volíme další.

Volba metod je tedy kritickým problémem! Platí, že ne všechny metody jsou použitelné pro všechny typy hrozeb. Např. metoda CARVER poměrně dobře umožňuje zachytit motivaci případného útočníka na chráněná aktiva, svým zaměřením je ale metoda pevně spojena s antropogenními hrozbami a to konkrétně úmyslnými útoky. CARVER tedy není schopen pokrýt naturogenní hrozby a také neúmyslné antropogenní hrozby (např. efekty neznalosti nebo nedbalosti).

Metody, které si organizace vybere pro analýzu rizika IT aktiv, firma vyjmenuje a popíše v dokumentu *Metodologie analýzy rizika IT aktiv*. Pojmenování se samozřejmě může lišit podle vnitřních pravidel pojmenování, což souvisí s vnitropodnikovou kulturou. Pokud je potřeba použít metody popsat podrobněji, mohou tyto být řešeny pomocí samostatných vnitropodnikových předpisů. Metodologie se následně aplikuje na jednotlivá IT aktiva nebo jejich skupiny – vytváří se *analýzy rizika aktiv*.

Posledním dokumentem, kterým se budeme zabývat je **RTP**. Tento dokument nám umožňuje nastavit základní pravidla pro zvládání rizik. Zajímá nás především jaká úroveň rizika je pro nás ještě přijatelná a tudíž nemusíme investovat do jejího řešení.

Pro základní rozlišení z hlediska přijatelnosti nám může posloužit matice rizik, viz obr. 2.4.

Je potřeba však dodat, že jak odstupňování pravděpodobností, tak kategorií závažnosti je do určité míry subjektivní záležitostí a bude se pro jednotlivé organizace tedy lišit. Obě škály proto musíme v organizaci standardizovat pomocí vnitropodnikového předpisu a to buďto metodologie analýzy rizika nebo **RTP**, podle toho jaké úkoly těmto dokumentům připsáme.

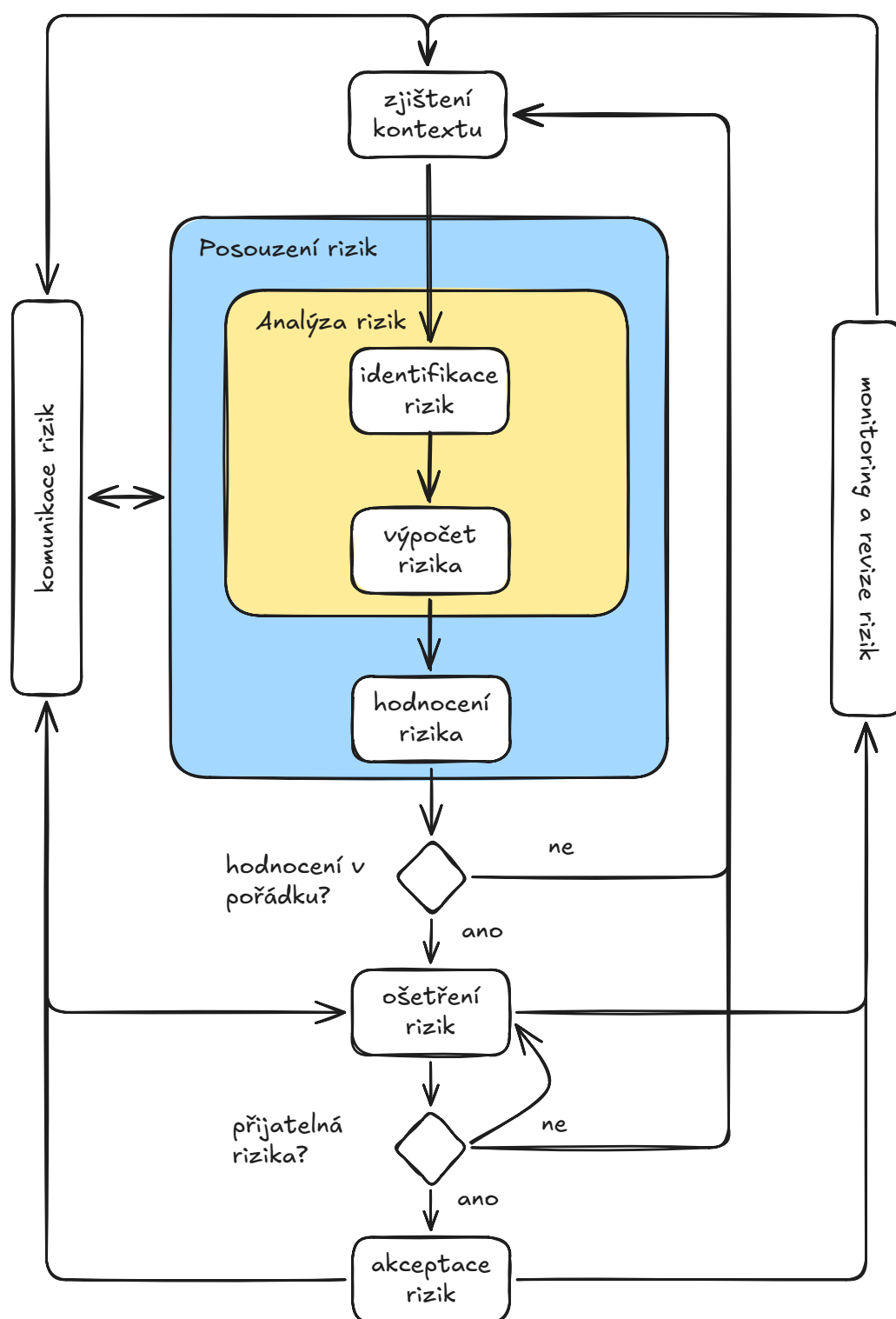
Standardizace je obzvláště potřebná u závažnosti, jelikož se jedná o tzv. kategoriální proměnnou s

neostrou definicí. O závažnosti můžeme říci, že je například malá, střední nebo velká, můžeme ale vymyslet naprosto odlišnou stupnici (bez následků, ohrožení chodu systému, ohrožení chodu organizace, ohrožení existence organizace).

Podobný problém můžeme mít u pravděpodobností, pokud ji nevyčíslujeme pomocí „tvrdých“ metod, tedy např. na základě studia frekvence výskytu incidentu, ale prostým „měkkým“ odhadem.

Přijatelná míra rizika kromě veličin pravděpodobnosti a závažnosti dopadů má také svůj ekonomický rozměr. S otázkou přijatelnosti proto bude souviset to, kolik finančních prostředků je organizace schopna a také ochotna vyčlenit na řešení identifikovaných rizik. Ekonomická situace nás tedy může donutit akceptovat rizika, která bychom za normálních okolností neakceptovali. Do této oblasti často spadají rizika související s ochranou duševního vlastnictví, která vyžadují nasazování specializovaných a přitom také velmi drahých softwarových produktů – organizace prostě nemusí mít dostatek finančních prostředků k jejich zakoupení a proto se musí smířit s tím, že rizika spojená s **Intellectual Property (IP)** vlastnictvím nemá pokryta tak, jak by si představovala.

Pokud se rozhodnete použít matici rizik, pak vězte, že i tato metoda má řadu omezení, která snižují její použitelnost. Existují sice určitá pravidla, která lze použít pro zvýšení šance na dosažení správného výsledku viz Cox [37] a Thomas [68], ale ani tato pravidla bohužel nezaručují plnou konzistenci matice rizik.



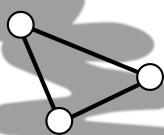
Obrázek 2.3: Proces posuzování informačního rizika (převzato z ISO 27005 [10])



Průvodce studiem

Minimálně *Umění klamu* Vám doporučuji prostudovat, obsahuje totiž poutavě popsané průniky do různých systémů, které se staly nebo se stát mohly a jsou zde rozebrané také postupy, které použil útočník a naznačeny způsoby ochrany proti nim.

Při úvahách o bezpečnosti IT totiž máme někdy tendenci sklouznout k prohlášení – jedná se o IT, řešení je proto nutno hledat opět v oblasti IT, proto by se o řešení měli postarat „ajtáci“. Ve skutečnosti je problém poněkud širší a tato kniha Vám pomůže získat lepší představu o jeho podstatě - a ani ji přitom nemusíte přečíst celou :-).



Analýza rizika - metody

Při volbě metod bereme v úvahu také fakt, že často existuje celá řada variant metod. Abychom zajistili opakovatelnost musíme metodu nějak zakotvit. V případě metod **FTA** a **ETA** je to jednoduché, obě metody jsou normalizované. V případě **FTA** je to ČSN 61025 [71], v případě **ETA** je to ČSN 62502 [72].

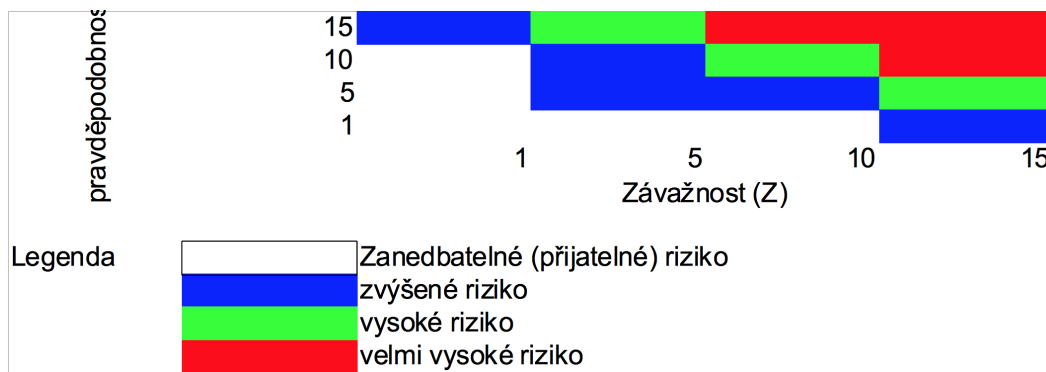
Pokud ale analýza rizika není normalizovaná je postup potřeba zakotvit pomocí vnitropodnikového předpisu.



Analýza rizika – semestrální projekt

Jeden ze semestrálních projektů je na zpracování analýzy rizik aktiva. Tuto analýzu můžete pojmout buďto aplikovanou na konkrétní aktivum nebo můžete zpracovat právě metodologii analýzy rizik.

Každý z přístupů má své výhody, ale bohužel také nevýhody. Metodologie může být přijatelnější z toho pohledu, že se jedná o dokument obecnější. Analýza rizik aktiva je má výhodu v tom, že na zvolené aktivum pouze aplikujeme vhodnou metodu analýzy rizik a interpretujeme její výsledky.



Obrázek 2.4: Matice rizik



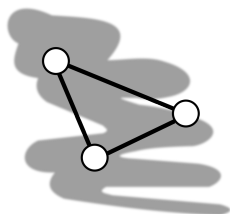
Limity metod

Všechny metody mají určitá omezení. Pochopení metody, je jedno jaké, proto vyžaduje plné pochopení nikoliv pouze způsobu jejího nasazení, ale také přijímaných předpokladů a omezení metody.



Příklad matice rizik

Na obr. 2.4 naleznete matici rizik. Na základě svých znalostí, popř. studia [37,68] rozhodněte, zda-li je matice alespoň slabě konzistentní. Pokud zjistíte problém, popište, kde se nachází a navrhnete odlišnou matici, která identifikovanými problémy netrpí.

**RA2 – The Art of Risk [33]**

RA2 – The Art of Risk je softwarový produkt, který slouží k zpracování analýz rizik podle ISO 27 005. Demo verze tohoto produktu je dostupná na Internetu se zpracovaným příkladem. Tento příklad Vám může posloužit jako inspirace pro zpracování semestrálního projektu.

**Shrnutí kapitoly**

ISO 27000 je kodex norem pro systémové řízení bezpečnosti informací. V kodexu jsou 3 základní normy ISO 27001 (systém ISMS), ISO 27002 (bezpečnostní politiky), ISO 27005 (řízení rizik). Účelem implementace je získání kontroly nad bezpečností informací a zajištění, že společnosti nevzniknou neúměrné škody v důsledku bezpečnostních incidentů.

Implementace začíná Závazkem vedení implementovat systém. Následuje rozhodnutí o rozsahu ISMS a nastínění základních obrysů ISMS v politice ISMS. Pro nastavení ISMS je nutno inventarizovat všechna informační aktiva a realizovat jejich analýzy rizik. Na jejich základě jsou vytipována opatření, která má smysl v ISMS implementovat. Implementace je obvykle postupná. Do systému jsou postupně přidávány předpisy, což vede k spuštění cyklického PDCA cyklu postupného zlepšování a nápravy zjištěných nedostatků.

**Kontrolní otázky: 2.3 Řízení rizik**

1. Co je to RTP a jaký je u tohoto dokumentu rozdíl od běžné analýzy rizik?
2. Co rozumíme opakovatelností výsledků analýzy rizik?
3. K čemu slouží metodologie analýzy rizik IT aktiv?
4. Vyjmenujte alespoň tři zdroje zranitelností.
5. Jaká je podstata fyzikálních zranitelností IT aktiv?
6. Co je zero day vulnerability?
7. Jaký je životní cyklus zranitelnosti?

Kapitola 3

Správa informačních aktiv



Průvodce studiem

V minulé kapitole jsme se dozvěděli, že základem úspěchu při implementaci nejen norem řady ISO 27000 je potřeba inventarizace informačních aktiv. Právě této problematice se budeme věnovat podrobněji v této kapitole.

Po přečtení této kapitoly budete

Znáť

- základní pojmy inventarizace IT aktiv
- způsob řízení zranitelností
- možnosti softwarové podpory procesu inventarizace
- návaznosti na další podnikové agendy a povinnosti

klíčová slova: management aktiv, vlastník, správce, garant, CMDB

požadavky na vstupní znalosti: pro pochopení této kapitoly potřebujete zvládnout minimálněš kapitolu 2.1, nejlépe ale celou kapitolu 2.



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 3 hod.

Inventarizace IT aktiv, jak jsme si řekli v předchozí kapitole, je podmínkou nutnou nikoliv však postačující k získání kontroly nad informační bezpečností. Slovo inventarizace naznačuje, že se bude inventarizovat – tedy pořizovat soupis aktiv, jak jsme zvyklí z inventarizace běžného majetku, a skutečně tomu tak bude. Tento typ inventarizace je však pouze jednou z funkcí, které při správě aktiv vykonáváme:

1. inventarizace IT aktiv
2. management konfigurací
 - správa požadavků (helpdesk)
 - evidence poruch
 - nákup a vyřazování aktiv
3. správa licencí
4. správa zranitelností

Jak vidno správa aktiv je poněkud složitější, než by se na první pohled mohlo zdát. Asociace, které se nám vybaví při vyslovení slova inventarizace jsou pak ne úplně reprezentativní. Na to si dejte pozor při studiu následujícího textu.

3.1 Inventarizace aktiv

Inventarizací aktiv rozumíme proces, kterým pořizujeme soupis informačních aktiv. Inventarizace může probíhat do určité míry obdobným způsobem jako běžná inventarizace majetku (stoly, židle, ...). Možná Vás napadne otázka – co je na tom tak komplikovaného, aby si inventarizace zasloužila samostatnou podkapitolu? Záludnost spočívá už v samotné definici pojmu informační aktivum a také účelu, za jakým je inventarizace prováděna.

Běžná inventarizace se týká především položek tzv. hmotného (**hmotný investiční majetek (HIM)**) a nehmotného (**nehmotný investiční majetek (NIM)**) investičního majetku. Tímto majetkem se rozumí majetek s pořizovací cenou vyšší než 80 000,- Kč. Inventarizace se provádí podle zákona o účetnictví a jeho hlavním účelem je kontrola cenného majetku společností, jehož hodnota je postupně „odepisována“.

Příkladem **HIM** může být server v pořizovací ceně 250 000,- Kč. Příkladem **NIM** pak může být zakoupený systém **Enterprise Resource Planning (ERP)** v ceně 1 500 000,- sloužící pro plánování zdrojů podniku.

Z hlediska účetnictví drobný majetek s pořizovací cenou pod 80 000,- není předmětem zájmu, protože je možné jej v podstatě okamžitě odepsat. Z pohledu systému ISMS je tento pohled ale chybný. Pořizovací cena může být jedním z použitých ukazatelů, ale nikoliv jediným. Co např. dělat s databází MySQL, která funguje jako databázový backend pro interně vyvíjený systém spravující pro organizaci kritické informace. MySQL je open source databáze s pořizovací cenou 0,- Kč (Community verze). Z tohoto důvodu se neobjeví v evidenci majetku realizované podle zákona o účetnictví. Protože ale uchovávání kritické informace organizace, bylo by neuvážené toto aktivum ignorovat.

Další otázkou je, co je přesně aktivum? Tímto pojmem jsme se extenzivně zabývali v předchozích dvou kapitolách. Možná jste si všimli, že z kontextu vyplývalo, že aktivum mělo v některých případech charakter spíše hardware zatímco v jiných případech mělo charakter software, lidí, archivů dokumentů. Co je tedy aktivum? Záleží na kontextu ve kterém si tuto otázku položíme. V obecné rovině je informační aktivum jakékoliv aktivum, které uchovává nebo jakýmkoliv způsobem zpracovává informace, které chceme pomocí ISMS chránit. Taková aktiva označujeme jako **primární**.

Tato aktiva ale často nejsou samostatně funkční. K jejich činnosti je potřeba hardware, software, obsluha, budovy a případně řada dalších věcí. Toto jsou také aktiva, která z pohledu bezpečnosti informací musíme také řešit. Tato aktiva označujeme jako **podpůrná**.

Platí, že potřebujeme zajistit bezpečnost primárních aktiv, protože ty potřebuje organizace udržet v chodu pro zajištění běhu klíčových funkcí organizace. Aby takový běh ale mohl být možný, je nutné udržet v běhu také podpůrná aktiva, která primární aktiva potřebují ke své funkci. Právě na podpůrná aktiva se bude soustřeďovat většina analýz a také opatření, která budeme realizovat k jejich ochraně.

Provázanost mezi aktivy může být poměrně složitá. Můžeme si např. představit rozsáhlý databázový systém, který pracuje jako klastr – to znamená že jej tvoří několik databázových serverů, které vzájemně replikují svá data a jsou schopny se plnohodnotně vzájemně zastoupit, vůči koncovému uživateli se ale celý klastr tváří jako jediný systém. Z tohoto pohledu můžeme jako IT aktivum brát v úvahu klastr jako celek nebo jednotlivé servery.

K podobným problémům se dostaneme, pokud začneme uvažovat o virtualizaci serverů – je aktivum virtuální server nebo hardware, na kterém běží (kde mohou běžet desítky virtuálních strojů). A co v případě, že i pro virtualizaci máme zřízeny klastery? Virtualizace je moderní technologií, která se ve stále větší míře používá i v malých a středních podnicích.

Inventarizace tedy vyžaduje provedení určitých rozhodnutí. K tomuto účelu je vhodné mít k dispozici určité podkladové materiály, ideálně ve standardizované podobě. Strukturu aktiv a jejich vzájemnou vazbu můžeme zachytit například pomocí *deployment diagramu* z jazyka UML.

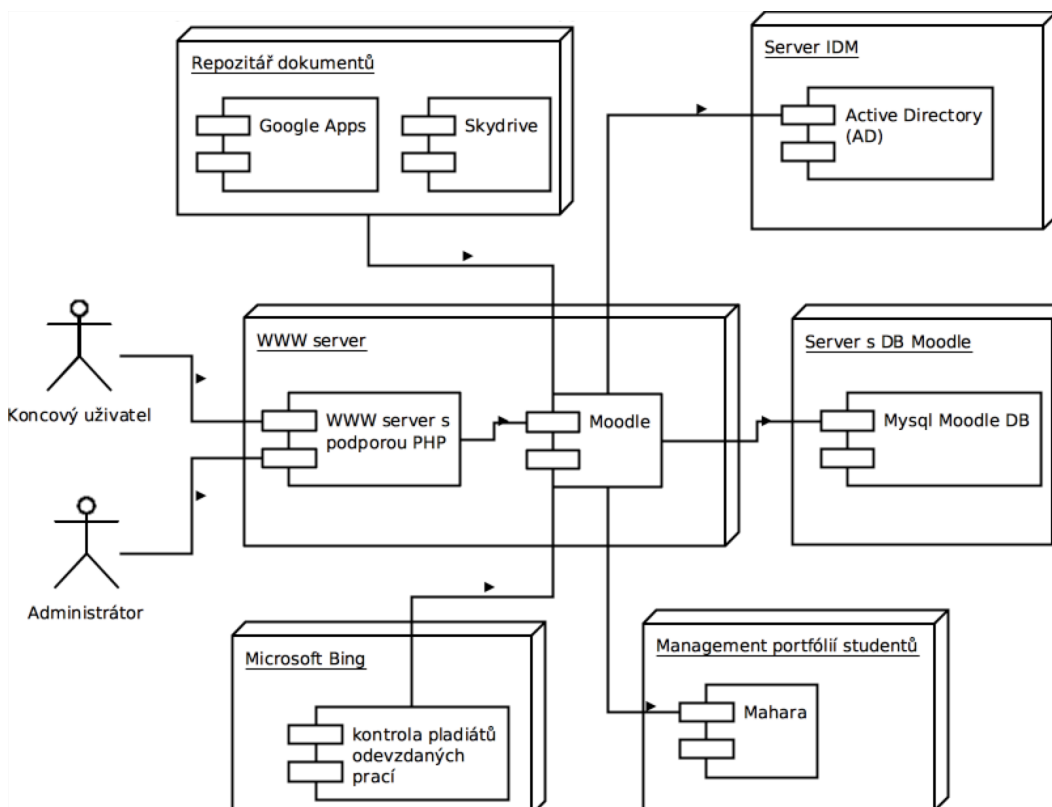
Unified Modeling Language (UML) je grafický jazyk sloužící k popisu systémů a jejich interakcí. Tento jazyk standardizuje skupina **Object Management Group (OMG)**. V době psaní této kapitoly byla poslední verze jazyka UML 2.5 [62] z června 2015.

Jazyk UML byl původně určen především pro programátory, protože jim umožňoval získat trochu jiný pohled na vyvíjený systém s cílem posílení analytické části návrhu nového systému. Programátor pak následně pouze implementuje model, který je vnitřně konzistentní a práce proto probíhá rychleji s menším množstvím chyb a také je větší šance, že ve finále bude systém dělat to, co ve skutečnosti dělat má. Tomuto přístupu pro zajímavost říkáme **Model Driven Approach (MDA)**.

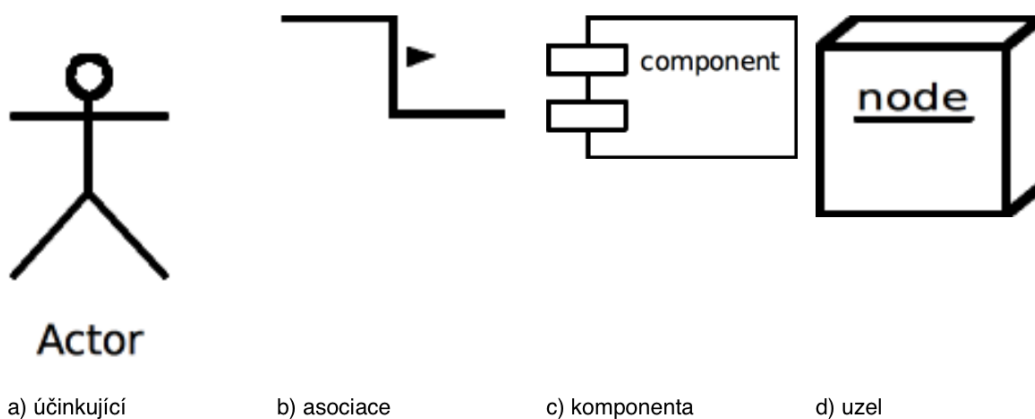
Nás pro účely konfigurací bude zajímat pouze jeden z mnoha diagramů, které jazyk UML poskytuje a to konkrétně diagram nasazení (deployment diagram). Tento diagram popisuje jakým způsobem jsou

rozmístěny jednotlivé komponenty systému na HW.

Zkusme si diagram nasazení demonstrovat na rozebrání aktiva systému podpory vzdělávání Moodle, viz obr. 3.1.



Obrázek 3.1: Deployment diagram Moodle



Obrázek 3.2: Konstruktory deployment diagramu jazyka UML

Actor (účinkující) (viz obr. 3.2 a)

Jedná se o fyzickou osobu nebo osoby, které přicházejí do styku s modelovaným systémem nebo jeho komponentou.

Association (asociace) (viz obr. 3.2 b)

Slouží pro propojování jednotlivých komponent modelu. Asociace nám tedy umožňuje naznačit, že

jednotlivé modelované komponenty jsou ve vzájemném vztahu – existuje mezi nimi nějaká forma interakce.

Component (komponenta) (viz obr. 3.2 c)

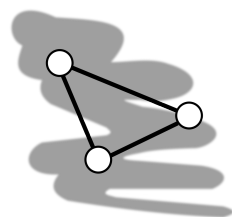
Jedná se o část systému. Může se jednat o fyzicky realizovanou (HW) komponentu nebo o SW popř. jeho část (např. nějaký modul nebo jeho část). Komponenta není samostatně funkční bez uzlu, ve kterém je umístěna.

Node (uzel) (viz obr. 3.2 d)

Uzlem rozumíme fyzický HW, na kterém běží jednotlivé komponenty modelovaného systému. Uzel proto může být počítač, server, serverový klastř, aktivní síťové prvky apod. Jeden uzel tedy nutně nemusí znamenat jedno zařízení.

S pomocí znalosti konstruktorů jsme schopni poznat lépe systém znázorněný na obr. 3.1. Jeho jádrem je samotný systém Moodle, který běží nad zvoleným WWW serverem s podporou PHP. Data-bázový backend systému je veden na samostatném databázovém serveru – v tomto případě na serveru MySQL.

Identitu uživatelů Moodle ověřuje vůči externí databázi uživatelských účtů, v tomto případě realizovanou pomocí **Active Directory (AD)**. Kromě toho kontroluje Moodle semestrální projekty na plagiáty pomocí vyhledávače Bing, umožňuje připojování externích repositářů údajů (Google Apps, MS OneDrive (původně pojmenovaný jako SkyDrive), a další) a také systém pro management portfolií prací studentů (Mahara).



Další diagramy jazyka UML

Diagram nasazení je pouze jedním z mnoha diagramů, které jazyk **UML** používá. Ačkoliv ostatní diagramy zde nepoužijeme, i ony Vám mohou být užitečné, především se jedná o diagramy:

- *případy užití* (use case diagram) - popisující různé způsoby použití modelovaného systému různými jeho uživateli.
- *činnosti* (activity diagram) - popisující posloupnost činností jednotlivých modelovaných procesů v rámci systému. Tento diagram lze použít např. jako náhradu diagramu algoritmu.
- pokud potřebujete jít v analýze až na úroveň dat pak se hodí také *třídní diagram* (class diagram).

UML diagramy obvykle nevytváříme ručně v obecném kreslícím programu, ale pomocí buďto specializovaných nástrojů pro tvorbu diagramů v jazyku **UML**, což jsou systémy **Computer Aided System Engineering (CASE)**, jako je třeba StarUML 2 [57], nebo software pro tvorbu diagramů, do kterého je podpora **UML** přidána – příkladem takových programů může být třeba open source nástroj Dia [4] nebo MS Visio Profesional¹.

Použít lze také některé webové aplikace, jako je např. Draw.io [5]. Výhodou webových aplikací bývá jejich nezávislost na operačním systému a také možnost integrace s cloudovými službami jako např. Google Drive [8], DropBox [6] a další.

Podrobnější informace o jazyku **UML** můžete získat buďto z knih jako je např. *Myslíme v jazyku UML* [66] (nebo kterékoliv jiné knize zabývající se UML), použít můžete ale také skripta z předmětu Umělá inteligence v bezpečnosti [82], které obsahují také kapitulu věnovanou jazyku UML (a nemusíte za ně platit :-).

Jazyk UML přitom není jediný nástroj, který lze za účelem podchycení struktury a vzájemných vazeb mezi aktivy použít, můžeme zde zmínit také topologie sítě CISCO a další. Tyto diagramy se obvykle kreslí v nástrojích jako je Dia nebo Visio a další. Výhodou tohoto zápisu je to, že je velmi často využíván „síťáři“, tedy pracovníky IT, kteří se zabývají správou síťové infrastruktury a může být v dané organizaci již k dispozici.

Máme tedy v rukou nástroje pro grafické zachycení vazeb mezi jednotlivými aktivy, jaké zdroje informací o aktivech máme vlastně k dispozici?

1. evidence běžného majetku (klasická inventarizace majetku)

¹Standard verze nepodporuje jazyk UML

2. evidence licencí software
3. procesní dokumentace (např. v systému ISO 9000)
4. nástroje pro „mapování“ sítě
5. personalistika
6. a další

První tři body si nejspíše dokážeme představit, co ale znamená mapování sítě a proč bychom ho vůbec měli dělat? Mapováním sítě rozumíme proces, v rámci kterého se snažíme sestavit mapu fyzické organizace provozované počítačové sítě. V zásadě existují dva základní přístupy k mapování sítě – strukturu můžeme zjistit na základě informací z routerů (routovacích tabulek) nebo ji můžeme zjišťovat aktivní sondáží sítě (network probing) v rozsahu síti přidělených IP adres.

Aktivní sondáž je z hlediska řízení informační bezpečnosti zajímavější, protože umožňuje zjistit i řadu dalších podrobností o zařízeních, jako je operační systém a jeho verze, stejně jako přítomnost určitých služeb. „Zmapovatelné“ jsou pouze takové služby, které využívají některý z otevřených síťových portů. Tedy pokud služba funguje čistě lokálně na daném počítači, není ji možné tímto postupem zjistit.

Úloha mapování sítě je v některých ohledech nezastupitelná, protože zobrazuje skutečný stav sítě v okamžiku napadení, nikoliv to, co si o síti myslíme nebo dokonce, co si přejeme, aby byla pravda.

Asi nejznámějším představitelem nástrojů pro mapování sítě je open source nástroj Nmap [17]. Tento nástroj je dostupný pro všechny významnější operační systémy a podporuje celé portfolio služeb mapování sítě, mimo jiné:

- identifikace zařízení na síti (host identification)
- kontrola otevřených portů na skenovaném zařízení (port scanning)
- identifikace operačního systému zařízení
- identifikace verzí provozovaného operačního systému a některých aplikací
- identifikace síťového jména (reverse DNS lookup)

Výše uvedeným způsobem je možno zjistit pouze část údajů, které jsou potřeba pro plnohodnotné řízení bezpečnosti informací. Automatizovaně pomocí mapování totiž není možné identifikovat všechny služby, které jsou na daném aktivu přítomny. Zároveň mapování nám nic neříká o osobě nebo osobách, které aktivum využívají ať už přímo (práce na desktopu) nebo dálkově (přístup ke službám).

Tyto dodatečné informace se shromažďují z celé řady různých zdrojů, které má daná organizace k dispozici. V rámci inventarizace majetku jednotlivým zařízením je přidělováno unikátní inventární číslo a přiřazuje se mu také místo, kde bude provozováno a zodpovědná osoba.

Informace o nasazovaných SW na jednotlivá aktiva je možné získat provedením auditu SW (viz kapitola Správa licencí) nebo také, alespoň částečně, z běžné ekonomické agendy – SW prostředky je potřeba také nakoupit apod.

Záznamy o jednotlivých uživateliích je taktéž možné získávat z jiných systému a to konkrétně **IDM**. Nejčastěji se pro tento účel využívá **AD** nebo **Lightweight Directory Access Protocol (LDAP)**, ačkoliv existují i jiná řešení. V těchto nástrojích jsou jednotlivým uživatelům přiřazovány unikátní identifikátory, podle kterých je jsme schopni dohledat v dalších systémech, do kterých se autentizují.

Zároveň jsme zde schopni vést další informace o uživateliích, jako jsou kontaktní informace (telefonní čísla, e-maily, ...), adresy, číslo kanceláře, v kterém oddělení daná osoba pracuje apod.

Celkově vzato zdroje informací o používaných IT aktivech mohou být velmi široké. Z tohoto důvodu, abychom získali kontrolu nad nimi, zavádíme tzv. *management aktiv*, v rámci kterého vytváříme komplexní databázi informací o jednotlivých aktivech - **Configuration Management Database (CMDB)**.

Inventarizace aktiv je tedy pouze prvním krokem v celém procesu.



Kontrolní otázky: 3.1 Inventarizace aktiv

1. K čemu slouží deployment diagram?
2. Jaké jsou konstruktory deployment diagramu (načrtněte jejich vizuální vzhled a popište co znamenají)?
3. Co rozumíme procesem inventarizace aktiv?
4. K čemu slouží mapování sítě?
5. Jaké informace můžeme mapováním sítě získat?
6. Jaké jsou další zdroje informací o IT aktivech?

3.2 Management aktiv

Pokud tedy *inventarizace aktiv* je pouze prvním krokem v procesu řízení konfigurací, co je naším konečným cílem? Cílem je získání kontroly nad způsobem, kterým jsou nasazovány a spravovány jednotlivá IT aktiva, bez ohledu to o jaká aktiva se jedná (tedy SW, HW, ale také lidé kteří s nimi pracují). Právě získání této kontroly je cílem managementu aktiv.

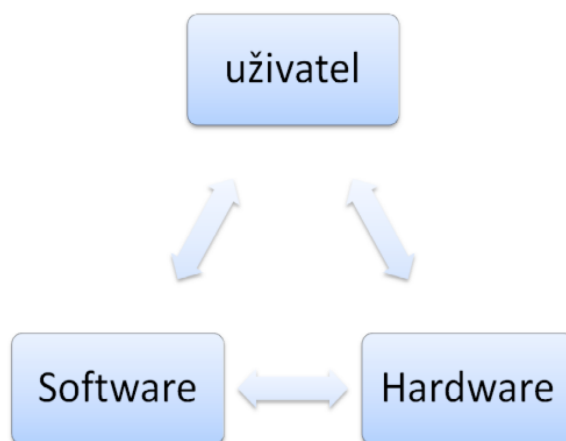
Pro účely **ISMS** lze výše uvedený cíl aplikovat také a to konkrétně jako nástroj pro získání informací nezbytných pro management rizik těchto aktiv.

Management konfigurací proto obsahuje (nebo může obsahovat) následující komponenty:

1. inventarizace aktiv,
2. pořizování a správa databáze CMDB,
3. správa požadavků,
4. správa licencí,
5. evidence poruch aktiv a jejich řešení

Těch informací, které mohou být z různých důvodů pro organizaci přínosné je tedy velké množství. Realizace řešení, které všechny tyto údaje bude schopno dát dohromady z různých zdrojů, udržovat je v aktuální podobě a ještě tak, aby byly dále využitelné není v plném rozsahu úplně snadné. Organizace proto obvykle podle svých potřeb volí podmnožinu vedených údajů určených pro integraci a zbytek zůstává ve svých původních zdrojích.

Základní strukturu objektů máme zobrazenou na obr. 3.3. Způsob, jakým bude ale realizována (zaznamenána) je přímo závislý na účelu (cíli) pořizování **CMDB** databáze. Bude nám stačit seznam např. v Excelu, nebo pro naše účely je nezbytné pořídit plnohodnotný systém **CMDB** od externího dodavatele?



Obrázek 3.3: Vztah software – hardware a lidé

Pro každé aktivum určíme několik osob. **Vlastník** - označuje osobu, která „vlastní“ (majetkově) dané aktivum. Můžeme to chápat ve smyslu útvaru, kde je aktivum evidované. Tato pozice je ale z pohledu bezpečnosti informací téměř bezvýznamná, byť organizace z logiky věci řeší také majetkové vztahy. Jenom to nedělá v systému ISMS.

Naopak klíčovou rolí z pohledu bezpečnosti informací je **garant aktiva**. Jedná se o osobu, která zodpovídá za aktivum a v případě, že aktivum postihne bezpečnostní incident tento incident bude také řešit, obvykle ale ve spolupráci s dalšími bezpečnostními rolemi.

Garant aktiva je univerzální označení. V případě IT prostředků se obvykle jedná o administrátora daného prostředku. Technická aktiva jako např. budovy ale administrátory nemají, mají ale správce. Pro různé typy aktiv se používá tedy různé označení pozice. Z pohledu logiky systému ISMS je ale výhodné mít univerzální poje, který dokáže abstrahovat tyto rozdíly v označování.

Platí, že každé aktivum musí mít stanoveného svého garanta. Celý proces má tak dva základní cíle:

- identifikovat informační aktiva (primární a podpůrná)
- k aktivům určit jejich garanty.

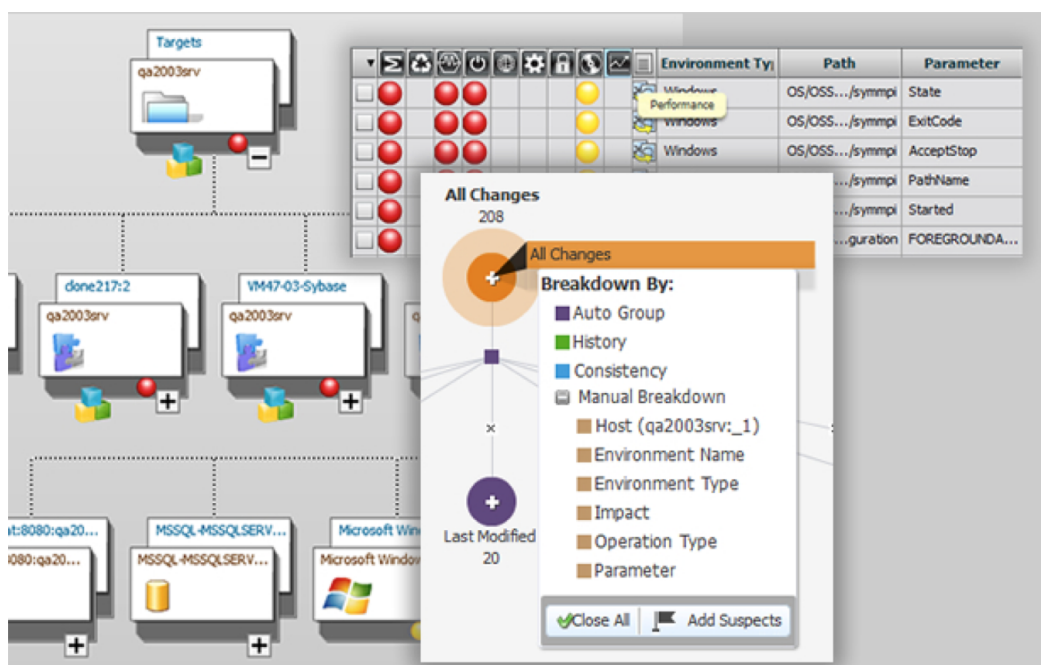
Tyto cíle musí být splněny ve všech organizacích, které systém ISMS v nějaké formě zavádějí. Rozsah shromažďovaných údajů, stejně jako další prvky a procesy managementu aktiv organizace implementují dle svých specifických potřeb a cílů.

3.2.1 Pořizování a správa databáze CMDB

Rozhodnutí o pořízení specializovaného software pro databázi **CMDB** je očividně velmi závažné. Vzhledem k velmi různorodým informacím, které do **CMDB** budou vkládány se obvykle očekává investice do datových pump, které údaje převedou z jejich původního umístění do databáze **CMDB**.

Vytvoření a údržba těchto pump není ani levná a ani rychlá, proto migrace na konkurenční produkt **CMDB** je obvykle velmi obtížná a firmy se do ní pouštějí velmi neochotně a až tehdy pokud opravdu není zbylí.

Podívejme se na některé dostupné SW produkty, které jsou za tímto účelem k dispozici. První z dostupných produktů je EVOLVEN, viz obr. 3.4.



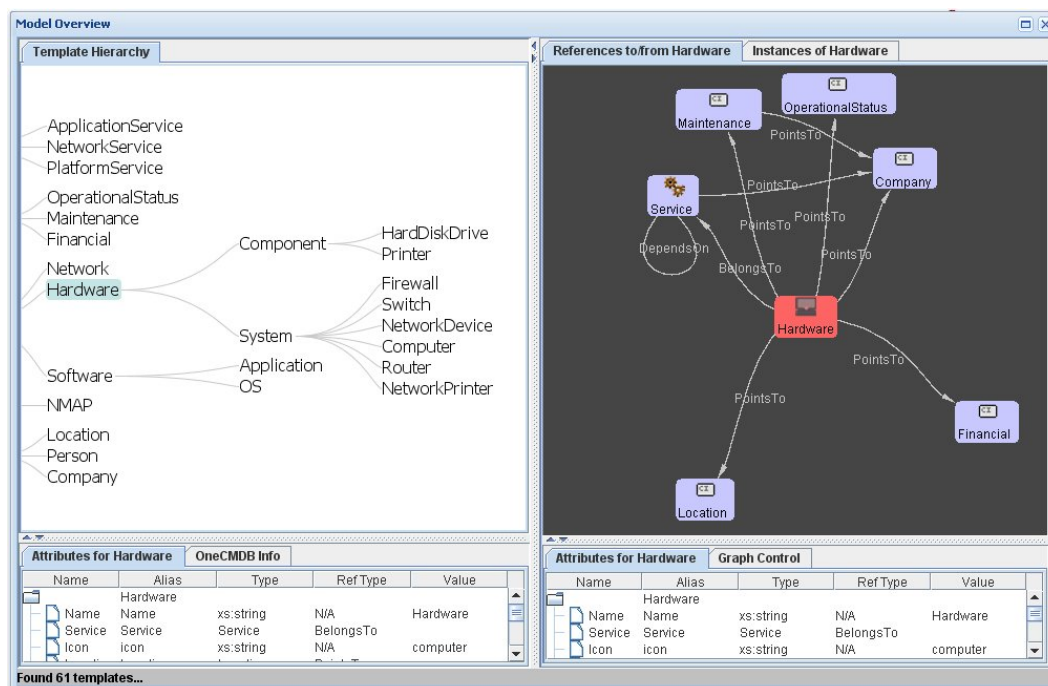
Obrázek 3.4: GUI Evolgen – pohled na aktiva (převzato z [14])

Evolgen je zaměřený především na pokrytí vazeb SW – HW. Na aktivu se spustí agent pro shromáždění potřebných informací a ty se potom uploadují na servery společnosti Evolgen, kde pro danou organizaci dochází k integraci dat. Pro jednotlivá aktiva lze pak ve stromové struktuře procházet jednotlivé služby, které jsou na něm provozovány. Je možné provádět také některé další činnosti jako je srovnávání konfigurací se zjednodušenou identifikací rozdílů. Je možné také srovnávat časové snímky aktiva z hlediska konfigurace, tedy co se v průběhu času v daném aktivu měnilo.

Z open source řešení je možné zmínit třeba iTOP [36]. Jedná se o systém s čistě WWW rozhraním, který je postaven kolem plně konfigurovatelné **CMDB** databáze. iTOP je plně integrované řešení, které kromě **CMDB** jako takového obsahuje také moduly pro sledování požadavků, incidentů, výpadků a další. Oproti řešení Evolgen ale v sobě nemá automatický detekční modul, který by části **CMDB** automatizovaně naplnil.

OneCMD [16] je přesně opačný případ než výše zmíněný iTop. Obsahuje v sobě moduly pro nastavení samotné databáze **CMDB** a autodiscovery moduly na bázi mapování sítě.

Existuje celá řada dalších nástrojů ať už proprietárních nebo open source, které tuto problematiku řeší. Jejich jediným společným rysem je, že každý z nich řeší tuto problematiku jinak, a proto je potřeba velmi pečlivě zvažovat, který nástroj bude pořízen a také jakým způsobem bude používán.



Obrázek 3.5: OneCMD – screenshot (převzato z [16])

3.2.2 Správa požadavků

Správou požadavků rozumíme v souvislosti s managementem konfigurací evidenci všech požadavků souvisejících s aktivem. Požadavky se mohou týkat žádosti o instalaci SW, hlášení poruch, žádostí o doplnění informací do informačních systémů organizace, změny konfigurace a další.

Správa požadavků se obvykle řeší odděleně od samotné databáze CMDB, může však obsahovat cenné informace, které mohou být upotřebitelné například pro účely analýzy rizik, za předpokladu, že dokážeme tyto informace ze systému správy požadavků vhodně vyfiltrovat, jelikož značná část evidovaných požadavků nebude upotřebitelná pro účely řízení bezpečnosti informací.

Správa požadavků se děje obvykle pomocí specializovaného software. Tento software se může lišit podle toho, jaké požadavky jsou jím sledovány. Např. požadavky směřované na vývoj software mohou být evidovány pomocí jiného software než požadavky na řešení problému s provozem aktiv.

Můžeme si to demonstrovat na specializovaných SW nástrojích pro evidenci požadavků na vývoj jako je Trac [20], Jira [31] nebo Bugzilla [9]. Společným aspektem těchto produktů je zaměření na podporu vývoje software. To se projevuje možností spojení hlášeného požadavku se změnami ve zdrojových kódech vedoucích k vyřešení tohoto požadavku. Zdrojové kódy jsou přitom obvykle vedeny v centralizovaných repozitářích umožňujících pohodlné verzování kódu, přidělování úkolů k řešení apod.

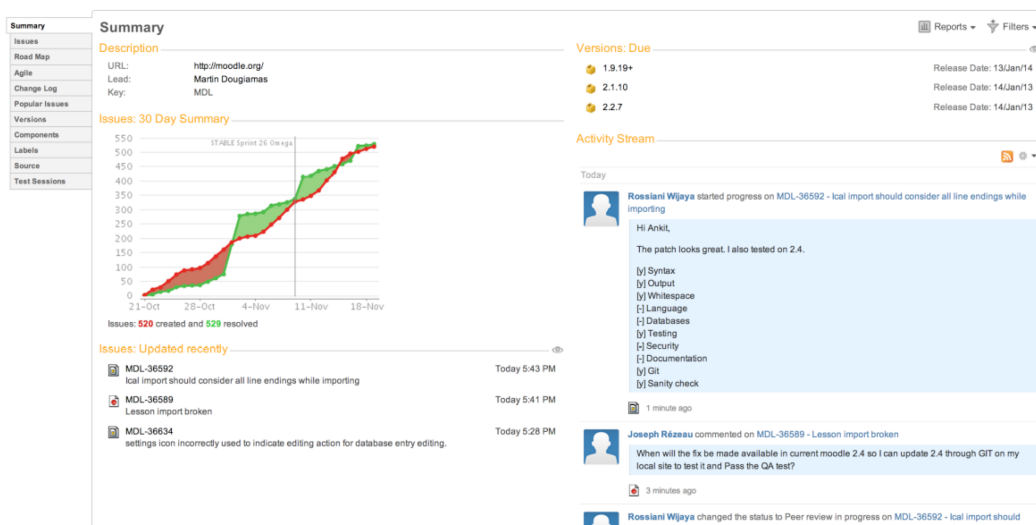
Řešení, která mají ambici řešit požadavky obecnějšího charakteru mohou být do určité míry jednodušší, není zde nutné realizovat další návaznosti na specializované softwarové produkty – řeší se pouze životní cyklus požadavků od pořízení až do okamžiku kdy se požadavek uzavře jako vyřešený.

Taková řešení jsou obvykle založena na podpoře helpdesku. Helpdesk je pracoviště (funkční místo nebo služba) určená pro podporu v různých oblastech. Může se jednat o podporu softwarového produktu, ale také o obecnou podporu.

Nás budou zajímat především řešení spíše obecná, která fungují uvnitř společností. Nejedná se tedy o helpdesk realizovaný formou hotline, který by problém vyřešil okamžitě, ale předpokládáme zadání požadavku pomocí specializovaného klienta (obvykle přes WWW) a zařazení tohoto požadavku do řady pro další řešení.

S vyřizováním požadavků proto souvisí některá nastavení procesů, která bychom si měli blíže rozebrat.

1. vytvoření řad požadavků
2. nastavení pracovníků vyřizujících požadavky v jednotlivých řadách
3. detekce dlouhodobě nevyřízených (visících) požadavků



Obrázek 3.6: Jira GUI pro projekt Moodle (převzato z [58])

4. reportování

Podívejme se na jednotlivé procesy. V prvním kroku je potřeba specifikovat jaké požadavky bude helpdesk řešit. Typ požadavků nám určí jaké typy odborností budou potřeba k jejich vyřizování. Správné rozčlenění problémových oblastí umožní, aby na jedné straně zadavatel požadavku správně identifikoval řadu, ve které se mu dostane pomoci (aniž by administrátor helpdesku musel identifikovat, že požadavek byl zadán do chybné řady a převést jej do řady správné) a na straně druhé, aby se pracovníci helpdesku mohli primárně věnovat plnění požadavků místo jejich administraci.

Řady mohou být tvořeny pro samostatné oblasti, např. síť, problémy s počítači, problémy s IS, nebo mohou být zaměřeny i na konkrétní produkty. V případě VŠB by to mohla být třeba řada pro IS Edison, OBD, SAP apod. Možné je také kombinovat oba tyto přístupy.

Pojmenování řad by mělo být pokud možno intuitivní, aby bylo na první pohled možné identifikovat účel řady.

K jednotlivým řadám je následně potřeba přidělit pracovníky, kteří jsou určeni k vyřizování požadavků v těchto řadách. Na jednotlivé pracovníky jsou kladeny jednak technické nároky z hlediska jejich schopnosti splnit z požadavku vyplývající úkoly, jednak zde mohou být organizační nároky - pracovníci musí mít možnost tyto úkoly vykonat. Možností rozumíme především dostatečným časovým prostorem k vyřízení požadavku a na straně druhé nastavení přístupových práv k jednotlivým systémům, kterých se požadavky mohou týkat.

I v rámci jednotlivých řad může existovat a většinou také existuje specializace pracovníků. Jednotliví pracovníci se proto sice částečně z hlediska pracovních povinností překrývají, nepřekrývají se ale úplně. Správné nastavení portfolia pracovníků kteří budou vyřizovat požadavky je proto klíčem k úspěchu řízení požadavků.

Z hlediska odbornosti je zejména pro některé tzv. „legacy“ systémy problém vůbec sehnat pracovníka. Problematické jsou např. systémy určené pro řešení business procesů, které byly realizovány před desítkami let v programovacím jazyce COBOL, určené původně pro běh na sálových počítačích.

Každý požadavek má svůj životní cyklus od vytvoření až po vyřízení (uzavření) požadavku. Jeho jednotlivé fáze by ale měly trvat pouze omezenou (co možná nejkratší) dobu. Podívejme se na jednotlivé fáze:

1. uživatel zadává požadavek do zvolené řady
2. operátor řady přidělí v vyřízení pracovníka a předá mu požadavek
3. pracovník převezme požadavek
4. pracovník vyřídí požadavek
5. pracovník uzavře požadavek
6. uživatel zkontroluje vyřízení a v případě nespokojenosti má obvykle možnost znovuotevřít požadavek, často přitom doplňuje další informace nutné k řešení. Z pohledu fází řešení se tak vracíme do fáze 1 – 3 podle toho s čím byl uživatel nespokojený.

Realizace helpdeskových řešení by měla zaručit, že požadavek by neměl uvíznout v žádné fázi vyřizování (mezistavu). Každý požadavek by tedy měl být zakončen buďto jeho splněním nebo zamítnutím požadavku, jako nedůvodným. To je zabezpečeno pomocí automatizovaných detekčních nástrojů, které mohou automaticky detekovat překročení nastavených intervalů pro jednotlivé kroky procesu vyřizování požadavku. Toto nastavení časových intervalů musí organizace provést předem.

Pro určitou představu můžeme zmínit řady požadavků, které ve svém helpdeskovém řešení (<https://idesk.vsb.cz/>) definovala naše univerzita:

- Campus WaH (požadavky zaměstnanců VŠB-TUO pro přidělení licenčních klíčů MS Windows a MS Office na domácí PC)
- Celoškolské PC učebny a kiosky
- Datové centrum
- EDISON
- Ekonomické IS (SAP, SAP Portál, Ekonfis, Arcotel, Docházka, Odběr stravy + stravenky, Dovolanky)
- Elektronická pošta a groupware
- EPS (Elektronický platební systém)
- Evidence projektů (Evidence projektů, Katalog vědecko-technických služeb)
- Fakultní fronta FBI (Fronta pro požadavky na fakultní správce FBI)
- Fakultní fronta FS (Fronta pro požadavky na fakultní správce FS)
- Fakultní weby (Správci fakultních webových stránek)
- Kartové centrum
- Kvalifikované certifikáty (Kvalifikované certifikáty ve smyslu Zákona 227/2000 Sb. o elektronickém podpisu)
- Nákup vybraných komodit výpočetní techniky (Dynamický nákupní systém)
- Nezařazeno (Vyberte, pokud nevíte kam zařadit svůj požadavek)
- OBD
- Osobní počítače a příslušenství (Problémy s počítačem, tiskárnou, skenerem apod)
- Počítačová síť - registrace PC (Registrace PC do počítačové sítě. Neslouží pro registraci PC na kolejkách)
- Počítačová síť a připojení (Problémy a požadavky související s provozem počítačové sítě (Internet, VPN, WiFi, ...))
- Problémy s heslem (Problémy s heslem nebo s přihlášením do univerzitních informačních systémů)
- Reprografické služby (Samoobslužné kopírování, tisky a skenování (ATS, SafeQ))
- Rozvrhy (Požadavky pedagogů na změny v rozvrhu)
- Služby serverové infrastruktury
- Stravovací systém
- Superpočítačové centrum (Superpočítačové centrum VŠB-TU Ostrava (SPC) poskytuje výpočetní prostředí a výpočetní zdroje pro náročné výpočty všem uživatelům VŠB-TU Ostrava)
- SW a licence (Problémy se SW a licencemi, žádosti o instalace)
- Webový portál (Webové stránky, Telefonní seznam, Novinky, Osobní karty zaměstnanců)

VŠB je velká univerzita s velkým množstvím zaměstnanců i studentů, z toho plyne i velké množství systémů a procesů, které musí univerzita a její jednotlivé fakulty podporovat. Nadnárodní komerční firmy mohou mít však řadu požadavků ještě podstatně více.

Samotné rozhraní pro vyplňování požadavků vypadá jako na obr. 3.7.

Obecně požadavek obsahuje přiřazení do některé z front požadavků, identifikace zadavatele. V případě helpdesku VŠB-TU Ostrava je identifikace prováděna proti univerzitnímu **IDM**. Helpdesk pak pracuje s e-mail adresou zadavatele, na kterou zasílá upozornění na změny ve stavu požadavků. Pracovníci, kteří požadavek vyřizují mohou také helpdesk využít pro získání upřesňujících informací o charakteru požadavku.

Požadavek samotný by měl být stručný a měl by umožnit identifikovat zdroj problému, který má být řešen. Napomoci v tom mohou také přiložené soubory jako jsou např. snímky obrazovky nebo podrobnější popis problému.

Obrázek 3.7: Obrazovka požadavku v Helpdesk VŠB-TU Ostrava

3.2.3 Management změn

Změnou ve smyslu probírané problematiky rozumíme obvykle pořízení (začátek životního cyklu aktiva), vyřazení (konec životního cyklu aktiva) nebo jeho zásadní inovace (např. upgrade na novou verzi „majoritní“ verzi provozovaného systému).

Všechny výše uvedené změny představují poměrně výrazný zásah do schopností aktiv vykonávat své funkce. Změněné schopnosti je pak nutno zohlednit v **CMDB** databázi. Evidenci změn je přitom nutné řešit procesně, zajímá nás především, jak budou tyto změny do databáze zavedeny. Jinými slovy nás zajímá, jak se pracovník evidující změny v databázi **CMDB** dozví, že došlo ke změně a jakým způsobem získá veškeré potřebné informace.

Situace je komplikovaná tím, že aktiva IT mohou být pořizována v rámci organizace často mnoha různými odděleními (útvary) nezávisle na sobě. Bez formálního procesu, který musí být navíc funkční (nestačí pouze proces sepsat, aby byl sepsaný a organizace dostala třeba nějaký certifikát).

Takový proces by měl obsahovat komu, kým a v jaké formě by informace o změnách měly být předávány. Očividně, aby management změn mohl fungovat, musí být v dané organizaci již zavedena databáze **CMDB** a nastaven způsob identifikace jednotlivých aktiv, uživatelů, ale také třeba místností (aby bylo možné jednoznačně identifikovat umístění aktiv).

Bez těchto rozhodnutí a definic proces managementu změn sice může být nastaven, nicméně pouze v obecné rovině. Případná předávaná data o změnách v aktivech logicky budou mít nízkou úroveň formalizace. Nízká formalizace prakticky znemožňuje (minimálně znesnadňuje) automatizované zpracování předávaných údajů. Ruční zpracování je přitom dražší, pomalejší a plyne z něj více chyb.

3.3 Správa licencí

Účelem správy licencí je primárně zajistit naplnění požadavků autorského zákona (zákon 121/2000 Sb. [70]), který nařizuje pořízení licence pro provoz software. Pro velké firmy však se správou software nastává problém, protože koncoví uživatelé mohou mít (a často také mají) tendenci doinstalovávat



Management změn - služby

Pozor! V této kapitole je diskutován management změn především v souvislosti s databází **CMDB**. Z tohoto důvodu nás zajímá především proces pořizování aktiv nebo změny v nich. Pojem management změn se ale také používá v jiné souvislosti – v rámci standardu ITIL je management změn brán jako součást **IT Service Management (ITSM)**, tedy je brán jako součást řízení služeb poskytovaných IT. Chápání managementu změn je tedy v ITIL posunuto.

Managementem změn se proto budeme zabývat ještě jednou v souvislosti s problematikou ITIL.



Kontrolní otázky: 3.2 Management aktiv

1. Co rozumíme správou požadavků?
2. Co je to řada požadavků?
3. Podle čeho rozhodujeme o tom, jaké řady požadavků budou podporovány?
4. Co je to management změn? Jakou úlohu v něm hraje formalizace procesu změn?
5. Co je databáze CMDB?
6. Jakým způsobem databázi CMDB pořizujeme a spravujeme?

další software, na který daná organizace nemá nakoupeny licence.

Problémem může být taktéž počet licencí – software jako takový totiž daná organizace může mít licencován, avšak počet provozovaných instalací software může být větší než počet nakoupených.

Licenční smlouvy mohou obsahovat také určité specifické požadavky na provozování. Ve školství je např. častý zákaz komerčního použití software. Tento požadavek je často ze strany výrobce SW kompenzován výrazně nižší cenou takového software.

Další omezení mohou souviset se způsobem provozování software – omezení může spočívat třeba v možnosti nebo nemožnosti provozování SW na virtualizovaných systémech.

To co v malých firmách popř. domácnostech ještě lze uhlídat ručně, ve velkých firmách s deseti tisíci provozovanými počítači již takto zajistit nelze. Udržení si kontroly nad provozem software je pak nutno realizovat s pomocí specializovaného software, který na jedné straně umožní specifikovat software, počet licencí a podporovaný způsob jejich provozu a na straně druhé umožní fyzickou kontrolu na provozovaných systémech souladu s těmito požadavky.

Management licencí je tedy poměrně složitý a jeho zvládnutí si vyžaduje zavedení a udržování procesů. Prvním krokem při nastavování procesů okolo správy licencí je určení zodpovědné osoby – *softwarového správce*. Jedná se o osobu, která má za úkol udržovat informace o zakoupených licencích a také způsobu, jakým jsou využívány.

Správce software může být určen jeden pro celou organizaci, nebo tyto úkoly může plnit více zaměstnanců, podle složitosti organizační struktury společnosti.

Na rozdíl od funkce CISO nebo některých jiných pracovních zařazení, softwarový správce nevykonává svou činnost obvykle na plný úvazek. Jeho úkolem je:

1. shromažďovat licence a doklady o zaplacení k nim příslušející
2. informace o dostupných licencích zavádět do SW nástrojů pro podporu řízení licencí
3. přidělování licencí koncovým uživatelům
4. kontrola provozovaných licencí na koncových zařízeních
5. řešení nesrovnalostí
6. reportování výsledků auditů software
7. nákup licencí

Z předchozího přehledu je patrné, že obsah práce softwarového správce je poměrně bohatý, možná až tak bohatý, že by naplnil několik pracovních úvazků – jak je tedy možné, že softwarový správce se věnuje této problematice pouze v části svého úvazku? Důvodem je, že pro výkon své práce musí úzce spolupracovat s IT pracovníky, kteří jsou mnohem blíže koncovým uživatelům, než je on sám.

Papírování samotné mnoho času obvykle nezabírá. Jednotlivé softwarové domy totiž pro licencování v podnicích používá k tomu určený typ licencování, tzv. volume licence, popřípadě SW produkt licenci je rovnou pro celou organizaci (site licence). Tímto způsobem jsou tak pokryty operační sys-

témy, kancelářské balíky, např. grafické programy firmy Adobe apod. To co zbývá, je z hlediska řešení složitější - nicméně co do počtu licencí, už to není obvykle tak hrozné.

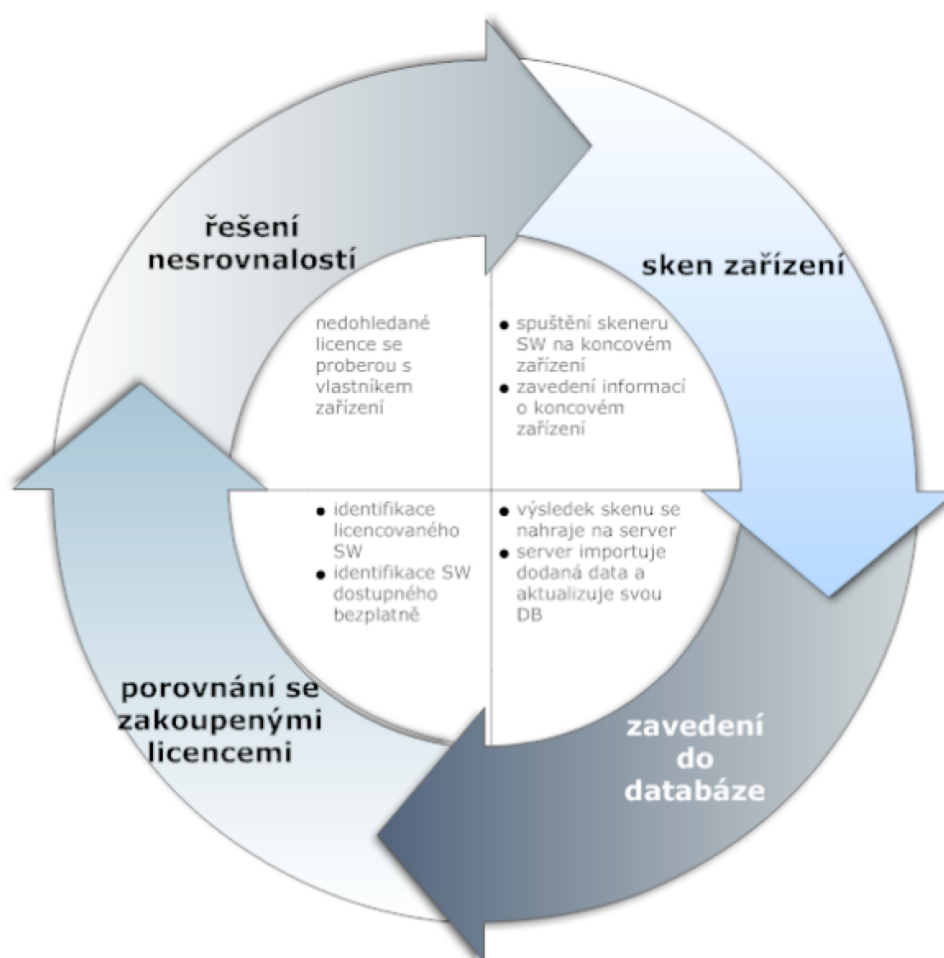
Časově nejnáročnější je kontrola provozovaných licencí na koncových zařízeních. Ta obvykle předpokládá spuštění specializovaného SW pro prohledání disku na soubory typu exe, com, dll, ocx, tbl popř. dalších. Tento software musí někdo spustit a nastavit některé údaje, např. identifikaci stroje, jméno osoby, která zařízení používá, místnost, kde se nachází atd. Tento někdo, ale obvykle není SW správce - častěji se jedná o pracovníka IT.

Software je pak ale už samostatný a nevyžaduje žádnou další obsluhu – po dokončení skenu výsledek nahraje na vzdálený počítač se serverovou částí SW pro správu licencí a ten ji dále zpracovává. Grafické znázornění procesu je naznačeno na obr. 3.8.

Vzhledem k tomu, že sken software provádí analýzu na úrovni souborů není spojení mezi licencí a soubory úplně přímočaré - jeden softwarový produkt může obsahovat klidně stovky nebo tisíce knihoven a spustitelných souborů. Software pro správu licencí pak obsahuje databázi známých souborů, které umožňují identifikaci provozovaného software. Tato identifikace ovšem obvykle není 100%-ní. Soubory, které se nepodaří přiřadit k nějakému známému softwarovému produktu musí být zařazeny manuálně.

Teprve následně se provádí hodnocení SW z hlediska licencí. U neidentifikovaného software rozhodnutí musí provést sám správce SW obvykle na základě konzultace s provozovatelem skenovaného zařízení.

Cyklus kontroly licencí SW



Obrázek 3.8: Cyklus kontroly licencí SW

Pokud je identifikován nelicencovaný software, je nutné buďto dokoupit licenci nebo daný SW odin-

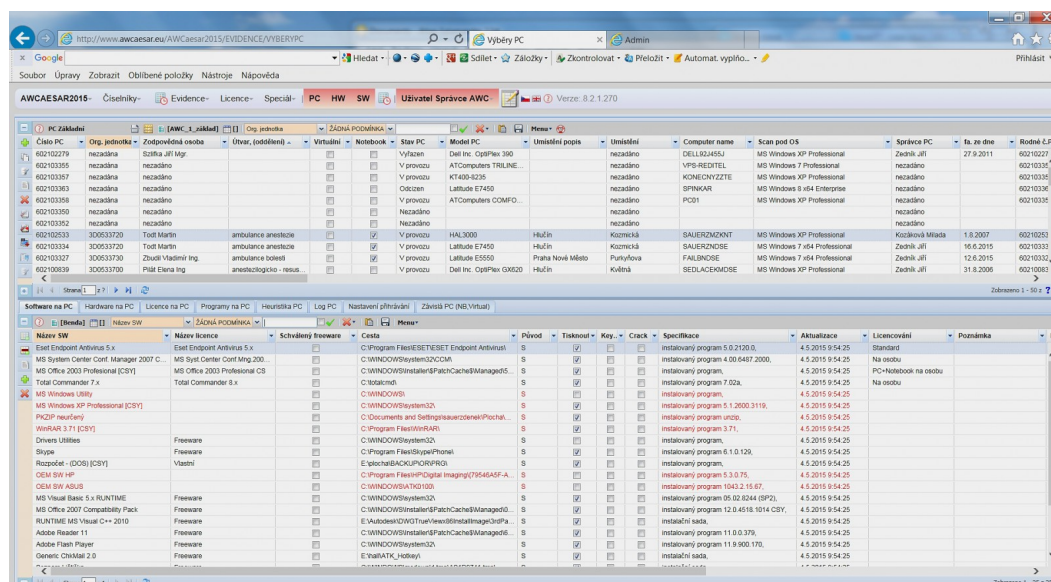
stalovat. V rámci skenu může být ale také identifikován SW, který již na daném koncovém zařízení nainstalován není (byl odinstalován někdy před provedením skenu). To může nastat pokud odinstalování neproběhlo korektně ať už v důsledku neodborného zásahu koncového uživatele nebo v důsledku chyby deinstalátoru.

V takovém případě se provádí ověření, že daný SW produkt skutečně není instalován na koncovém zařízení a výsledky se v SW pro správu licencí patřičným způsobem upraví. O celé operaci by ale v ideálním případě měl existovat záznam.

Proces správy licencí by kromě skenu samotného a jeho vyhodnocování měl obsahovat také proces pro nákup a evidenci SW a také způsob instalace a odinstalace, především kdo ji bude provádět - bude to koncový uživatel nebo pracovník IT? Tomu je potřeba přizpůsobit proces kontroly, tedy především její fáze řešení nesrovnalostí.

Dále je potřeba připomenout, že obor IT se výrazně vyvíjí a to s sebou nese inovace v oblasti SW, tedy fakt, že se neustále objevují nové verze SW, které uživatelé (nebo jejich nadřízení) požadují. Správa licencí proto není jednorázovou záležitostí. Vzhledem ale k tomu, že vyhodnocení není úplně triviální, provádí se skenování nárazovitě v kampaních 1x – 2x ročně.

Jedním z nejpoužívanějších produktů pro správu licencí je v ČR produkt AW Caesar společnosti FreeRW Soft [41]. Demonstrační snímky obrazovky tohoto produktu naleznete na obr. 3.9 a 3.10.



Obrázek 3.9: GUI AW Caesar (převzato z [40])

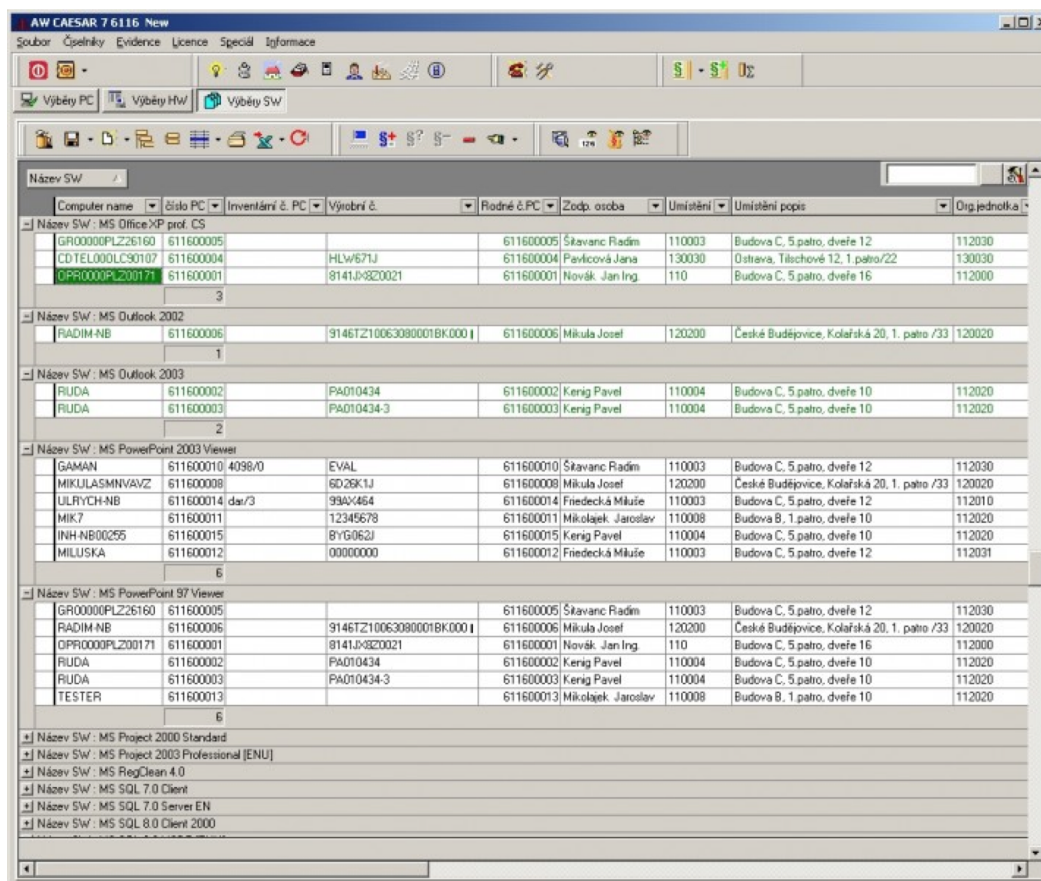
Je potřeba říci, že management licencí nemá přímou vazbu na bezpečnost informací. Pokud tedy organizace používá větší množství licencí software, než kolik si jich zakoupila, jedná se sice o stav, který je v rozporu s autorským zákonem (se všemi právními důsledky z toho vyplývajícími), zároveň tento stav neohrožuje bezpečnost informací.

Znamená to, že tuto problematiku musí organizace řešit, ale ne nutně jako součást systému ISMS. V kontextu bezpečnosti informací je pro nás správa licencí zajímavá nástroji, které se k tomuto účelu používají. Tyto prostředky totiž obvykle podporují shromažďování většího objemu informací o aktivu, než je nutné čistě pro účely managementu licencí. Tyto informace jsou pak přímo použitelné i v kontextu bezpečnosti informací.

Software je přitom také aktivum (obvykle podpůrné). Evidence software pak představuje jeden z možných zdrojů informací pro CMDB databázi.

3.4 Management zranitelností

Z předchozích kapitol již víme, co jsou zranitelnosti v IT systémech, jakým způsobem je dělíme a také co je podstatou těchto zranitelností. Při uvažování o metodách ochrany proti nim nás nepochybně napadne nasadit technologie jako jsou antivirová řešení na koncových zařízeních, firewally, IPS nebo IDS systémy a další. Tyto nástroje nás ale chrání vůči možnosti zneužití zranitelnosti, neodstraňují však



Název SW	Computer name	Číslo PC	Inventurní č. PC	Výrobní č.	Rodné č. PC	Zodp. osoba	Umístění	Umístění popis	Org. jednotka
Název SW : MS Office XP prof. CS									
GR0000PLZ26160	611600005			HLW671J	611600005	Škavanc Radim	110003	Budova C, 5.patro, dveře 12	112030
CDTEL000LC90107	611600004				611600004	Pavlovská Jana	130030	Ústava, Těškově 12, 1.patro/22	130030
OPR0000PLZ00171	611600001			8141J-820021	611600001	Novák Jan Ing.	110	Budova C, 5.patro, dveře 16	112000
Název SW : MS Outlook 2002									
RADIM-NB	611600006			9146TZ10063080001BK0001	611600006	Mikula Josef	120200	Česká Budějovice, Kolaříská 20, 1. patro /33	120020
Název SW : MS Outlook 2003									
RUDA	611600002			PA010434	611600002	Kerig Pavel	110004	Budova C, 5.patro, dveře 10	112020
RUDA	611600003			PA010434-3	611600003	Kerig Pavel	110004	Budova C, 5.patro, dveře 10	112020
Název SW : MS PowerPoint 2003 Viewer									
GAMAN	611600010	4036/0		Eval	611600010	Škavanc Radim	110003	Budova C, 5.patro, dveře 12	112030
MIKULASMNVAVZ	611600008			6D26K1J	611600008	Mikula Josef	120200	Česká Budějovice, Kolaříská 20, 1. patro /33	120020
ULRYCH-NB	611600014	dar/3		99A4464	611600014	Friedecká Mikuláš	110003	Budova C, 5.patro, dveře 12	112010
MIK7	611600011			12345678	611600011	Mikolajek Jaroslav	110008	Budova B, 1.patro, dveře 10	112020
INH-NB000295	611600015			8YG062J	611600015	Kerig Pavel	110004	Budova C, 5.patro, dveře 10	112020
MILUSKA	611600012			00000000	611600012	Friedecká Mikuláš	110003	Budova C, 5.patro, dveře 12	112031
Název SW : MS PowerPoint 97 Viewer									
GR0000PLZ26160	611600005				611600005	Škavanc Radim	110003	Budova C, 5.patro, dveře 12	112030
RADIM-NB	611600006			9146TZ10063080001BK0001	611600006	Mikula Josef	120200	Česká Budějovice, Kolaříská 20, 1. patro /33	120020
OPR0000PLZ00171	611600001			8141J-820021	611600001	Novák Jan Ing.	110	Budova C, 5.patro, dveře 16	112000
RUDA	611600002			PA010434	611600002	Kerig Pavel	110004	Budova C, 5.patro, dveře 10	112020
RUDA	611600003			PA010434-3	611600003	Kerig Pavel	110004	Budova C, 5.patro, dveře 10	112020
TESTER	611600013				611600013	Mikolajek Jaroslav	110008	Budova B, 1.patro, dveře 10	112020
Název SW : MS Project 2000 Standard									
Název SW : MS Project 2003 Professional [ENU]									
Název SW : MS RegClean 4.0									
Název SW : MS SQL 7.0 Client									
Název SW : MS SQL 7.0 Server EN									
Název SW : MS SQL 8.0 Client 2000									

Obrázek 3.10: GUI AW Caesar - Analýza SW (převzato z [40])

Kontrolní otázky: 3.3 Správa licencí



1. Co je účelem managementu licencí?
2. Definujte povinnosti správce SW.
3. Jak probíhá SW audit?
4. Jak řešíme nesrovnalosti v auditu SW?

zranitelnost samotnou. Pokud se dokážeme vypořádat přímo s podstatou zranitelnosti, dosáhneme podstatně vyšší úrovně bezpečnosti.

V současnosti existuje celá řada systémů pro management zranitelností, které pracují na různém principu. Zmínit je možné např. systém společnosti Rapid 7 Nexpose [64] nebo Qualys Guard Vulnerability Management [63] a další.

Tyto specializované nástroje provádějí audit zařízení na síti s cílem najít zranitelné systémy, identifikovat podstatu zranitelnosti a odhadnout její závažnost, tak aby pověření pracovníci mohli optimalizovat své úsilí v odstraňování popř. minimalizaci následků zneužití v případě, že odstranění zranitelnosti není možné.

Jak vypadá zranitelnost v reálu – resp. informace o ní, kterou je možné využít pro detekci přítomnosti zranitelnosti. Podívejme se na jeden příklad dokumentované zranitelnosti, viz obr. 3.11.

SA51202 je dokumentace zranitelnosti MS Internet Explorer 9.x, která je klasifikovaná jako vysoce kritická, protože umožňuje přístup do systému a to vzdáleně. SA51202 vydala společnost Secunia, která se zabývá hledáním, dokumentací a zveřejňováním zranitelností.

V tomto případě se jedná o dnes již zaplátovanou zranitelnost - identifikace zranitelnosti by pak mohla spočívat v kontrole, zda na daném počítači byla instalovaná daná záplata nebo ne. Existují ale také jiné způsoby, jakými lze identifikovat zranitelný systém - záleží na tom, jakou strategii vyhledávání zranitelností zvolíme, jaký nástroj nebo nástroje k tomu zvolíme.

Secunia Advisory SA51202

Microsoft Internet Explorer Multiple Use-After-Free Vulnerabilities

Secunia Advisory SA51202

Release Date 2012-11-13

Popularity 1,482 view

Comments 0 comments

Criticality level Highly critical

Impact System access

Where From remote

Authentication level Available in Customer Area

Report reliability Available in Customer Area

Solution Status Vendor Patch

Systems affected Available in Customer Area

Approve distribution Available in Customer Area

Remediation status Secunia CSI, Secunia PSI

Automated scanning Secunia CSI, Secunia PSI

Software: Microsoft Internet Explorer 9.x

Secunia CVSS Score Available in Customer Area

CVE Reference(s) CVE-2012-1538 CVSS available in Customer Area
CVE-2012-1539 CVSS available in Customer Area
CVE-2012-4775 CVSS available in Customer Area

Description
Multiple vulnerabilities have been reported in Microsoft Internet Explorer, which can be exploited by malicious people to compromise a user's system.

1) A use-after-free error within the "CFormElement" class can be exploited to dereference already freed memory.

2) A use-after-free error within the "CTreePos" class can be exploited to dereference already freed memory.

3) A use-after-free error within the "CTreeNode" class can be exploited to dereference already freed memory.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

Solution
Apply updates.
Further details available in Customer Area

Provided and/or discovered by
1, 2) The vendor credits Jose A. Vazquez, spa-s3c.blogspot.com via iDefense Labs
3) The vendor credits Cheng-da Tsai (Orange), Sung-ting Tsai, and Ming-chieh Pan (Nanika), Trend Micro

Original Advisory
Microsoft (KB2761451):
<http://technet.microsoft.com/en-us/security/bulletin/ms12-071>

Download CSI

Download PSI

Obrázek 3.11: Secunia Advisory SA51202 (převzato z [18])

Hledání zranitelností můžeme provádět dálkově po síti - jedná se principiálně o stejnou technologii, kterou používáme pro mapování sítě, nebo může probíhat přímo na jednotlivých koncových zařízeních (použít můžeme také kombinaci obou těchto přístupů).

Výhodou skenování po síti je to, že není vyžadována instalace nástrojů do koncových zařízení, nevýhodou pak omezené portfolio informací o zařízení, které jsme schopni tímto způsobem získat - identifikovány jsou pouze ty prostředky (popř. jejich verze), které komunikují po síti a to bez zásahu uživatele. Neodhalený zůstanou případné zranitelnosti jako je výše jmenovaná zranitelnost, která vyžaduje aby uživatel přistoupil pomocí zranitelného MS Internet Exploreru ke speciálně upravené stránce.

Hledání zranitelností přímo na koncových zařízeních proto má mnohem lepší naději tyto zranitelnosti odhalit, protože jej spouštíme až za všemi možnými ochrannými vrstvami.

Kromě zranitelností plynoucích z chyb v SW prostředcích mohou skenery také provádět kontrolu nastavení jednotlivých komponent kontrolovaného systému. Tento typ kontroly je podstatně složitější. V případě, že se zaměřujeme pouze na kontrolu zranitelností plynoucích z chyb v software, obvykle nám stačí identifikovat verzi provozovaného software a zkontrolovat ji proti databázi zranitelností a postižených verzí daného SW.

Pokud kontrolujeme i nastavení, pak tato kontrola je v podstatě unikátní pro každý softwarový prostředek. Její technické zajištění je proto poměrně složité. Z tohoto důvodu, portfolio produktů, u kterých je možné takovou kontrolu provést je relativně omezené, zmínit je možné např. MS Baseline Security Analyser [53] společnosti Microsoft, který je určen pro kontrolu konfigurace operačního systému Windows. Existují ale i nástroje pro kontrolu konfigurace jiných systémů.

V okamžiku, kdy identifikujeme zranitelnost, čeká nás rozhodnutí, co s ní a v jakém časovém horizontu budeme dělat. V ideálním případě nainstalujeme záplatu, která identifikovanou zranitelnost odstraní. Instalace záplat, zejména u programů třetích stran na počítačích s operačním systémem Windows je problém.

Operační systém v sobě až do Windows 8 neobsahoval nástroje umožňující pohodlnou aktualizaci

SW třetích stran, ve Windows 8 už tato funkčnost zavedena je avšak pouze pro aplikace zakoupené přes Windows Store (v prostředí velkých organizací tedy opět o ničem). Sám Microsoft si je tohoto problému vědom a poskytuje nástroj InTune [54], který umožňuje takové instalace provádět dle potřeb, bohužel není dostupný zadarmo a neobsahuje v sobě nástroje pro detekci zranitelností - ty musí být identifikovány externě a InTune slouží pouze pro distribuci (instalaci) případných záplat.

O integrovaných řešeních lze hovořit v případě nástrojů jako je Corporate Software Inspector [39] společnosti Flexera a další, které jsou schopny některé softwarové produkty zaplátovat automaticky. Corporate Software Inspector navíc v sobě integruje některé další nástroje např. pro automatické mapování sítě apod.

Aplikace oprav pro alternativní operační systémy např. na bázi BSD nebo Linux je jednodušší, neboť tyto systémy obsahují rozsáhlé repozitáře SW a pokročilé balíčkovací systémy, které umožňují identifikovat, verzi software, ale také vzájemné závislosti mezi softwarovými balíky. Aktualizace komponent samotného operačního systému nebo software na něm instalovaném pak obvykle probíhá z těchto repozitářů a lze ji nastavit tak, aby se některé typy aktualizací (např. ty označené jako bezpečnostní) instalovaly automaticky.

Tím, že se instalace i aktualizace provádějí ze stejných zdrojů, je správa celého systému velmi pohodlná a také rychlá.

U zařízení společnosti Apple se zaplátování provádí pomocí AppStore pro operační systém a aplikace, které byly přes AppStore zakoupeny. Situace je tedy podobná jako v případě Microsoftu, ovšem s tím, že v AppStore je v současnosti dostupné větší množství nabízených aplikací.

Z pohledu řízení bezpečnosti informací nás obvykle nezajímají jednotlivé zranitelnosti, ale celkový proces, který organizace používá pro identifikaci existujících zranitelností a obecné nastavení způsobu konfigurace a manipulace/použití aktiv, aby se minimalizovala možnost zneužití zranitelností.

Zranitelnosti tak obvykle zobecňujeme do skupin s podobnými bezpečnostními vlastnostmi a na ně následně vyvíjíme opatření vedoucí k minimalizaci možnosti zneužití a případných dopadů, které by mohlo z takového zneužití vyplynout.

Kontrolní otázky: 3.4 Management zranitelností



1. Jakým způsobem můžeme identifikovat zranitelnost?
2. Jak se vypořádáváme se zranitelnostmi?
3. Jaká jsou úskalí aplikace záplat na jednotlivá koncová zařízení?
4. Zhodnoťte rozdíly ve zaplátování mezi operačními systémy MS Windows, Linux a macOS X.



Shrnutí kapitoly

Tato kapitola se podrobně věnuje problematice správy informačních aktiv, která je nezbytným základem pro implementaci norem řady ISO 27000 a získání kontroly nad informační bezpečností. Samotná správa aktiv představuje komplexní proces, který zahrnuje nejen jejich samotnou inventarizaci, ale také management konfigurací (kam spadá helpdesk, evidence poruch či nákup a vyřazování aktiv), správu licencí a řízení zranitelností. Text zdůrazňuje, že z pohledu systému řízení bezpečnosti informací (ISMS) nelze na aktiva nahlížet pouze skrze účetní optiku pořizovací ceny, ale je nutné brát v potaz jejich kritičnost pro organizaci a rozlišovat mezi primárními aktivy (která přímo uchovávají či zpracovávají chráněné informace) a podpůrnými aktivy (jako je hardware, software či budovy, na nichž funkčnost primárních aktiv závisí).

Pro efektivní zachycení složitých vazeb a struktury aktiv doporučuje kapitola využívat standardizované grafické podklady, konkrétně diagramy nasazení (deployment diagramy) z jazyka UML, které popisují rozmístění jednotlivých komponent systému na hardwaru za účasti uživatelů (aktérů). Ke shromažďování dat o IT infrastruktuře lze kromě klasické evidence majetku využít také nástroje pro aktivní sondáž a mapování sítě (např. open-source nástroj Nmap), které dokážou identifikovat běžící zařízení, otevřené porty, operační systémy a verze služeb. Protože však automatizované mapování nepokryje všechny nezbytné informace (např. uživatelská data z nástrojů jako Active Directory), zavádí se centralizovaný management aktiv využívající konfigurační databázi CMDB, jež integruje různorodé datové zdroje organizace.

V rámci managementu aktiv je z bezpečnostního hlediska klíčové stanovení jednoznačného garanta pro každé aktivum, který zodpovídá za jeho chod a řešení případných bezpečnostních incidentů. K udržení dlouhodobé kontroly nad aktivy slouží specializované softwarové nástroje (proprietární jako Evolgen či open-source jako iTOP), které umožňují sledovat změny konfigurací v čase. Důležitou součástí tohoto ekosystému je také správa požadavků realizovaná prostřednictvím helpdeskových systémů. Tyto systémy pokrývají celý životní cyklus hlášení – od zadání uživatelem, přes přidělení specializovanému pracovníkovi až po finální vyřešení – a poskytují cenná statistická data využitelná při následné analýze rizik.

Kapitola 4

Metody a postupy při řízení rizik IT



Průvodce studiem

V této kapitole se podíváme na některé metody a postupy, které je možno použít pro management rizik.

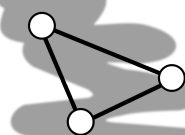
Po přečtení této kapitoly budete

Znáť

- některé méně známé metody analýzy rizik používaných v IT
- zájmové hrozby typické pro IT

klíčová slova: ISO 27000, ISO 31000, analýza rizik, RTP, identifikace rizik, BRA, CARVER, FMEA, cost-benefit analýza

Požadavky na vstupní znalosti: Ideálně byste měli chápat teorii rizik (viz samostatný box). Dále je potřeba zvládnout kapitoly 2.1 a 2.4 z těchto skript.



Předpokládané znalosti

Tato kapitola předpokládá, že čtenář je již obeznámen s definicemi z oblasti řízení „běžných“ rizik a zná a je schopen použít určitou (jím vybranou) metodu analýzy rizika a interpretovat její výsledky.

Pokud tyto znalosti nemáte nebo si nejste úplně jisti, je ten správný čas vrátit se ke studiu některých jiných předmětů, ve kterých jste se s těmito s touto problematikou mohli setkat (stačí kterýkoliv z nich):

- Řízení rizik
- Analýza rizik území
- Analýza nebezpečí a rizik I
- Metody rizikového inženýrství
- Analýza nebezpečí a rizik II
- nebo jiný předmět zaměřený na rizika a práci s nimi



Čas nutný ke studiu

Na prostudování kapitoly budete potřebovat 1-2 hodiny. Pokud ale čtete tento text v rámci studia předmětu *Bezpečnost informačních systémů* je možná žádoucí, abyste se k textu vraceli opakovaně v souvislosti s přípravou semestrálního projektu a také přípravou na zkoušku.

4.1 Obecný postup a odhad velikost dopadů

Zkusme zasadit rizikové analýzy do širšího kontextu řízení bezpečnosti. Jako cíl rizikových analýz obvykle stanovujeme něco ve smyslu *identifikování, zvládnutí, odstranění nebo minimalizace událostí, které mají nežádoucí vliv na aktiva organizace*.

K tomuto účelu je obvykle potřeba stanovit:

- hrozby, kterým jsou jednotlivá zájmová aktiva vystavena,
- výši škod, které vzniknou v důsledku realizace hrozby pro organizaci,
- pravděpodobnost realizace hrozby s určitými škodami
- opatření, kterými se rizika minimalizují

Z výše uvedeného lze říci, že cíle analýzy rizika jsou v obecné rovině stejné bez ohledu na to, co je přesně analyzováno (technologie, území nebo v tomto případě bezpečnost informací).

Podobně i postup analýzy rizik zůstává stejný, jeho jednotlivé kroky jsou ale interpretovány ve světle toho, co je analyzováno:

1. identifikace a ocenění aktiv
2. nalezení zranitelných míst
3. odhad pravděpodobností využití zranitelných míst
4. výpočet očekávaných ztrát
5. přehled použitelných opatření a jejich cen
6. odhad úspor aplikací zvolených opatření

Kroky identifikace aktiv a nalezení zranitelných míst mají pro účely rizikových analýz trochu jiný význam, než jsme zvyklí z běžných rizikových analýz. Běžná rizika např. bezpečnosti nám vyplývají totiž obvykle z fyzické interakce mezi řízenými objekty - např. manipulace se strojem pracovníkem. Oproti tomu my již víme z předchozí kapitoly, že zájmová aktiva v systému **ISMS** nejsou nutně pouze fyzická - musíme třeba extenzivně pracovat také se software.

Vazby mezi zájmovými aktivy jsou tak v případě **ISMS** složitější. Ostatně to je důvod, proč jsme zaváděli systém řízení aktiv, který nám nyní poskytuje údaje potřebné pro realizaci analýz.

Odhad pravděpodobnosti může být také problematický. Odhad lze provést na základě frekvencí výskytu určitého jevu, za předpokladu, že máme dostatečně podrobné vstupní informace, např. z helpdesku nebo nějaké formy monitoringu sítě, popř. zařízení na ní pracující, a jsme schopni z něj potřebné informace dostat. V opačném případě je nutné spolehnout se na buďto převzaté údaje z externích zdrojů nebo provést expertní odhad.

Výpočet očekávaných ztrát a také předpokládaných úspor plynoucích z realizace ochranných opatření je krokem nutným, jeho realizace, ale může v různých společnostech proběhnout odlišně. Kromě běžného požadavku, aby finanční částky byly vyčísleny pro srovnatelné časové období, je potřeba zvolit pro situaci vhodnou metodiku výpočtu očekávaných ztrát.

Lze samozřejmě provést *vyčíslení skutečných ztrát* - jako náklady, které je nutno vynaložit na odstranění následku události. Do těchto nákladů lze začlenit alikvotní část mezd pracovníků, kteří problém řeší. Pokud je s obnovou spojena nutnost dalších investic do hardware nebo nákup specializovaných služeb (např. na obnovu dat z poškozeného disku), jedná se opět o náklady.

Incident může ale také narušit infrastrukturu společnosti tak, že po nějaký čas nebude schopna plně nebo dokonce vůbec vykonávat svou běžnou činnost. Tato situace může nastat při skutečně rozsáhlých výpadcích v infrastruktuře. Takové výpadky u společností, které berou bezpečnost IT vážně se nestávají příliš často, přesto se stávají - jako příklad lze uvést hack a následný výpadek služeb **PlayStation Network (PSN)** společnosti Sony z roku 2011 [69], který způsobil únik informace o 77 mil. účtů uživatelů PSN a měsíční nedostupnost této služby. Celkové náklady společnost Sony vyčísnila na 171 mil. USD (přibližně 4,16 mld. Kč).

Výše uvedený příklad je ale ve svém pojetí nákladů komplexnější. Jelikož Sony PSN využívá jako platformu pro online prodej her a také pro placený přístup k online komponentám her - jsou součástí nákladů také ušlé příjmy, které v důsledku výpadku sítě nemohly být realizovány. V tomto případě je vyčíslení nákladů také poměrně přímočaré, nemusí tomu tak být ale vždy.

Uveďme jiný příklad: v roce 2016 vyšlo najevo, že v minulosti unikly společnosti Yahoo informace o více než miliardě uživatelských účtů [30]. Informace o úniku přišla pro Yahoo v ten nejméně vhodný okamžik, protože právě v této době finisovala jednání o prodeji Yahoo společnosti Verizon. Únik se stal prakticky okamžitě předmětem jednání a způsobil snížení prodejní ceny Yahoo o přibližně 350 mil. USD (přibližně 8,5 mld. Kč).

Dopady incidentu tedy mohou být relativně široké. Kromě přímých nákladů na obnovu po incidentu, je do nákladů možné započítávat také širokou škálu dalších dopadů na společnost, které lze skrýt pod názvy jako náklady ušlé příležitosti, smluvní pokuty vyplývající z nesplnění závazků, poškození dobrého jména společnosti.

Obnova po incidentu v sobě může zahrnovat také komponentu odlišné konfigurace chráněného systému, nebo realizace dodatečných ochranných opatření, které mohou mít pozitivní vedlejší efekty. Tyto je možné začlenit do rozhodování o nastavení celého systému.

K tomuto účelu lze použít řadu různých metod - např. **Cost-Benefit Analysis (CBA)** [7] je založena na přímém porovnání nákladů a přínosů rozhodnutí. Pokud není možné přesně specifikovat náklady, ztráty a očekávané přínosy, je možné použít metody jako je **Multi-Criteria Analysis (MCA)** [78]. V takovém případě je možno zohlednit i jiná kritéria, které je nemožné vyjádřit ve smyslu finančních přínosů nebo nákladů, ale mohou přesto přispět k rozhodnutí (ovlivňují optimalitu řešení).

4.2 Identifikace rizik

ISO 27005 ve verzi z roku 2005 předepisovala metodologii identifikace rizika zaměřenou na identifikaci aktiv, hrozeb a také zranitelností. Tento postup odpovídá pojetí, které jsme použili v předchozím výkladu. V pozdějších revizích normy však tento požadavek již není obsažen.

K identifikaci rizik lze proto přistupovat libovolným způsobem. Zaměřit se je možné třeba na procesy, „vlastníky“ rizika, nebo cokoliv jiného. Rozhodnutí o postupu identifikace by ale mělo být vědomé a dobře zdůvodněné.

Porovnejme identifikaci rizik vycházející z identifikace IT aktiv a postup vycházející z analýzy procesů probíhajících ve společnosti.

Identifikaci aktiv jsme již poměrně extenzivně popisovali v předchozích kapitolách, proto tyto informace pouze shrneme. Pokud identifikaci rizik provádíme směrem od identifikace aktiv postupujeme „zespoda“ od jednotlivých aktiv ke způsobu, jakým jsou využívány. Tyto informace pak použijeme k odhadu hrozeb, kterým jsou aktiva vystavena a následně také k odhadu rizika.

Pokud postupujeme směrem od procesů pak analyzujeme činnosti (procesy), které společnost vykonává a z nich odvozujeme aktiva využívaná v rámci analyzovaných procesů a hrozby, kterým jsou vystaveny. Výhodou tohoto postupu je fakt, že v řadě společností jsou probíhající procesy formálně popsány a mohou tak posloužit jako základ pro identifikaci relevantních rizik.

Z hlediska hrozeb lze vyjít z řady zdrojů, např. BSI zveřejnil katalog základních hrozeb [34] pro IT systémy. Katalog hrozeb má také v jedné ze svých příloh samotné ISO 27005, byť se nejedná o vyčerpávající výčet, ale spíše příklad obsahující nejčastěji identifikované hrozby. Poměrně komplexní přehled hrozeb zveřejnil také Dejan Kosutic [38], ze kterého je sestaven přehled hrozeb níže:

- přístup do sítě neautorizovanými osobami
- porušení smluvních podmínek
- kompromitace důvěrných informací
- škody způsobené třetí stranou, živelní pohromou
- požár, úder blesku
- průmyslová špionáž
- neoprávněné pozměnění uchovávaných záznamů
- krádež
- selhání hardware
- malware
- neautorizované použití materiálů chráněných autorským zákonem (licencování software, neoprávněné použití audiovizuálních materiálů, apod.)
- a další

Obdobné katalogy existují také pro zranitelnosti. Následující přehled je opět adaptován z přehledu Dejana Kosutice [38]:

- ponechání tovární nastavení zařízení
- vyhození přenosných médií bez správně provedeného výmazu dat
- senzitivita zařízení (prach, teplota, vibrace, ...)
- nedostatečnost v procesu (managementu kapacit, klasifikace informací, kontroly vstupu, údržby, zálohování, ...)
- neadekvátně provedené školení zaměstnanců

- a další

Jednou z důležitých otázek, kterou při identifikaci rizik řešíme je také otázka vlastnictví rizika. Vlastnictví rizika by nemělo být zaměňováno s garancí aktiva.

garant aktiva je osoba, která spravuje aktivum. Pokud není taková osoba určena, tak buďto správa aktiva neprobíhá vůbec, nebo probíhá chaoticky (náhodně), což z pohledu ISMS obvykle není považováno za přijatelné.

Vlastník rizika je osoba nebo entita, která je odpovědná a možnost řídit riziko. Pojem entita naznačuje, že vlastníkem rizika by nutně nemusela být fyzická osoba - může to být třeba oddělení, byť obvykle se to nedoporučuje. Připojení rizika k entitě má totiž tendenci rozmělnit odpovědnost. Jedním z předpokladů úspěchu při řízení rizik přitom ale je, aby vlastník aktivně pracoval na minimalizaci tohoto rizika.

K takovému úkolu budou lépe přistupovat vlastníci, kteří se uvědomují riziko a aktivně se mu chtějí vyhnout. Aktivní jsou tedy ty osoby, které jsou „osobně“ zainteresovány na řešení rizika. Zainteresovanost se nutně nemyslí finanční motivace, ale třeba práce, kterou by vlastník rizika musel odvést navíc, pokud by riziko skutečně nastalo.

Silně motivovaní v tomto ohledu bývají lidé, kteří se v minulosti s následky uvažovaného rizika museli potýkat.

Zároveň platí, že vlastník rizika by měl být dostatečně vysoko postaven v řídicích strukturách organizace, aby byl schopen získat prostředky nutné pro řešení rizika.

4.3 Model rizika

Matematicky se riziko obvykle, ve své nejjednodušší podobě, vyjadřuje jako funkce pravděpodobnosti a následků (4.1).

$$R = f(P, N) \quad (4.1)$$

Pro účely hodnocení rizika obvykle potřebujeme hodnotu rizika vyčíslit a pak můžeme použít např. multiplikativní (4.2) nebo aditivní (4.3) model rizika.

$$R = P \cdot N \quad (4.2)$$

$$R = P + N \quad (4.3)$$

Z matematického pohledu jsou vzorce (4.2, 4.3) hrubým zjednodušením rizika, které ale za určitých okolností umožňuje rozhodnout, které riziko je z pohledu chráněného aktiva (zájmu) důležitější. V multiplikativním modelu pravděpodobnost P funguje jako váha předpokládaných následků.

Způsob, jakým odvodíme hodnotu pravděpodobnosti a následků tak bude mít zásadní vliv na výsledek analýzy rizik a ovlivní také, jaké metody analýzy rizika bude možné použít. Pokud použijeme semikvantitativní hodnocení pravděpodobnosti a následků, bude možné výsledek znázornit do matice rizik (viz obr. 2.4).

Zákres rizika do matice rizik pak umožňuje rizika vizuálně srovnat. Zároveň to ale znamená, že takto stanovená hodnota rizika nemůže být dále agregována - např. přes různá rizika jednoho aktiva, aby bylo získáno riziko aktiva. Resp. agregace takto odvozeného rizika nemá smysl.

Proto předtím, než organizace může začít se samotnou analýzou rizik, musí nejprve navrhnout její metodologii.

Metodologie obecně (viz. např. Wikipedie) je *vědní disciplína, která se zabývá metodami, jejich tvorbou a aplikací*. Metodologií rizika v tomto případě organizace kriticky zhodnotí dostupné metody analýzy rizik z hlediska jejich postupů, ale datových potřeb a pevně stanoví způsob provádění analýzy rizik, která tato omezení respektuje.

Různé metody analýzy rizik s sebou přinášejí různá omezení. Tato omezení je potřeba předem identifikovat a respektovat. V opačném případě mohou být výsledky prováděných analýz zavádějící nebo přímo chybné.

Zkusme demonstrovat různé možnosti postupu na příkladu:

Uvažujme aditivní model rizika uvažující pravděpodobnost a následky. Využijeme k tomuto účelu semikvantitativní hodnocení na pěti stupňové škále (0 - 5). Hodnocení budeme provádět zjednodušenou formou - tedy uvažovat budeme pouze následky a pravděpodobnost.

- Hodnocené aktivum: *notebook*
- hrozba: krádež
- zranitelnost: zaměstnanci neví, jak chránit data na přenosných zařízeních
- následky: 3
- pravděpodobnost: 4

Hodnota rizika tak bude 7: $R = P + N = 3 + 4 = 7$.

Některé analýzy k výše uvedenému modelu rizika přidávají ještě hodnotu aktiva, to však není (v tomto případě) správně. Hodnota aktiva by totiž měla být zohledněna v následcích krádeže. Hodnota aktiva by tak byla započítána 2x.

Alternativně lze použít model rizika, který hodnotu aktiva bere v úvahu. Mějme tedy stejný příklad, ale s odlišným modelem rizika. Použijeme opět semikvantitativní hodnocení na pětistupňové škále (0 - 4).

- Hodnocené aktivum: *notebook*
- hrozba: krádež
- zranitelnost: zaměstnanci neví, jak chránit data na přenosných zařízeních
- hodnota aktiva (A): 3
- úroveň hrozby (H): 2
- úroveň zranitelnosti (Z): 2

Hodnota rizika tak bude opět 7: $R = A + H + N = 3 + 2 + 2 = 7$.

Alternativně lze místo sčítání použít násobení.

Všimněte si, že ačkoliv je příklad triviální, není až takový problém v něm udělat chybu. Je tedy potřeba dát si pozor.



Průvodce studiem

V předchozím textu jsme stanovili určitý kontext provádění rizikových analýz. V následujících podkapitolách se budeme věnovat různým metodám analýzy rizik, které nejsou tak známé (existuje reálná možnost, že jste se s nimi dosud nesetkali) a které lze úspěšně použít pro analýzu rizik v systémech ISMS.

Nejedná se nutně o metody, který byste měli použít. V textu jsme již opakovaně řekli, že ISO 27005 nepředepisuje nějaké konkrétní metody analýzy rizik a tedy můžete použít libovolnou metodu, za předpokladu že ji použijete správně (při respektování specifik a omezení metody).

4.4 BRA - Binary Risk Analysis

Binary Risk Analysis (BRA) je zajímavou metodou, která umožňuje určit riziko na základě zodpovězení desíti otázek s odpověďmi ano/ne. Odpovědi se vždy vyhodnocují po dvojicích. Struktura otázek:

1. odhad pravděpodobnosti
 1. Může být útok proveden bez speciálních znalostí?
 2. Může být útok proveden bez nutnosti nasazení značných zdrojů?
 3. Má aktivum implementovány obranné mechanismy?
 4. Jsou v současnosti realizované ochrany aktiva známy zranitelnosti?
 5. Je zranitelnost v aktivu vždy přítomna?
 6. Může být útok proveden bez splnění předběžných podmínek?
2. odhad hrozby
 7. Budou důsledky z vnitřních zdrojů?
 8. Budou důsledky z externích zdrojů?
 9. Má aktivum nebo vytváří aktivum značkou obchodní hodnotu?
 10. Budou náklady na opravu nebo výměnu aktiva značné?
3. odhad rizika - se provádí na základě odhadnuté pravděpodobnosti a hrozby.

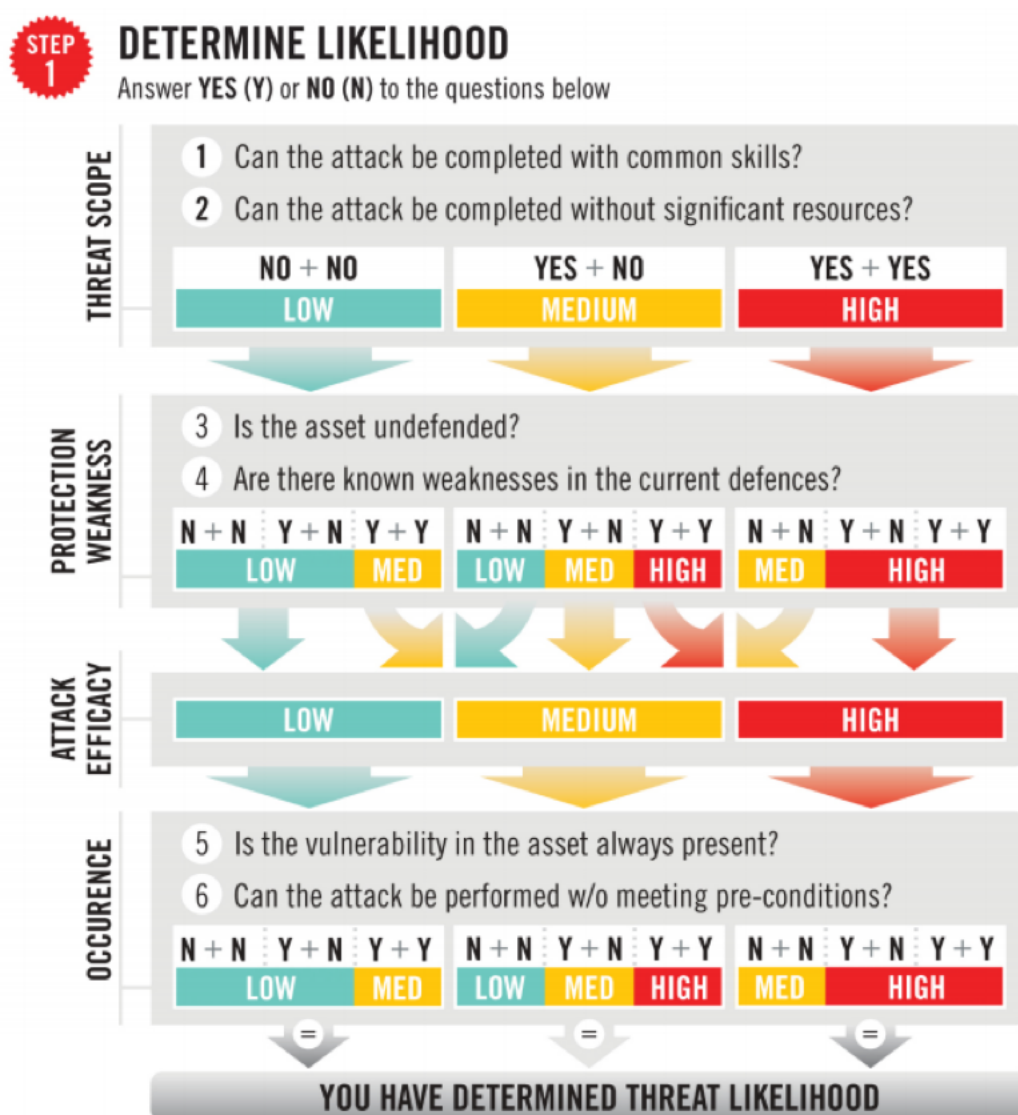
Metoda BRA je zajímavá také tím, že postup metody se celý vleze na dvě stránky A4. Je tam možné jej vytisknout a do tabulek v Excelu (nebo jiném tabulkovém procesoru) přímo zapisovat výsledky hodnocení.

Formálně je BRA semi-kvalitativní metodou analýzy rizika, která pracuje s třístupňovou škálou (nízká, střední, vysoká ... pravděpodobnost).

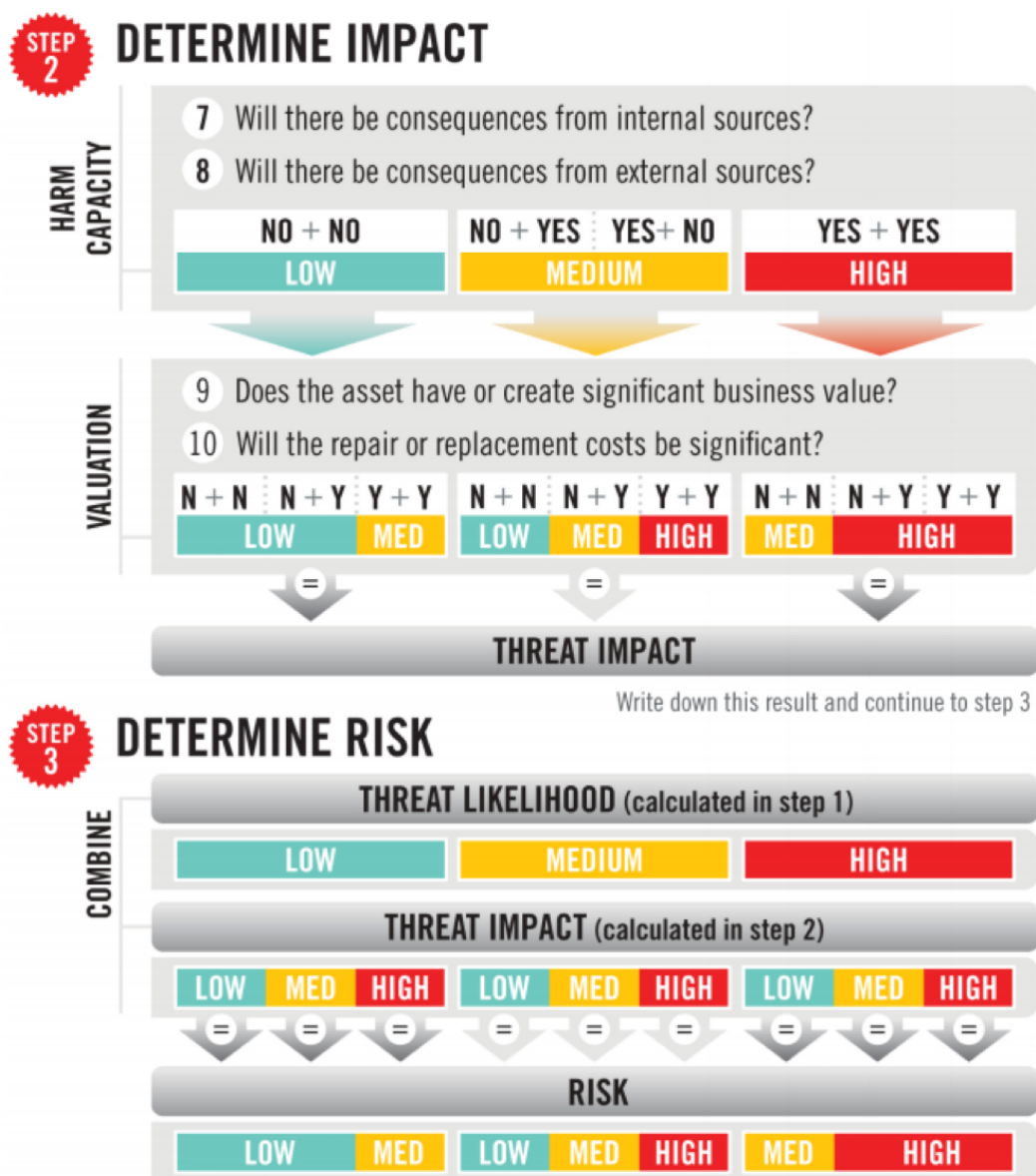
Zkusme podle metody vyhodnotit odpovědi na otázky v kroku pravděpodobnosti (viz obr. 4.1). Příklad je formátu číslo otázky a odpověď A (ano)/N (ne): 1. A, 2. A, 3. A, 4. A, 5. A, 6. N.

První dvojice otázek s odpověďmi A, A vede na nízkou pravděpodobnost - vyhodnocování otázek 3 a 4 proto bude prováděna v levém sloupci obr. 4.1. Odpověď A, A v otázek 3 a 4 vede na střední pravděpodobnost. Vyhodnocování poslední dvojice proto bude prováděno v prostředním sloupci (následujeme šipku). Poslední dvojice otázek má odpovědi A, N proto finální odhad pravděpodobnosti je střední.

Na obr. 4.1 a obr. 4.2 je znázorněn postup metody. Další dokumentace k metodě a jednoduchý software pro vyhodnocování jsou dostupné na domácích stránkách metody: <http://binary.protect.io/> [2].



Obrázek 4.1: BRA - hodnocení pravděpodobnosti (převzato z [2])



Obrázek 4.2: BRA - hodnocení dopadů a rizika (převzato z [2])

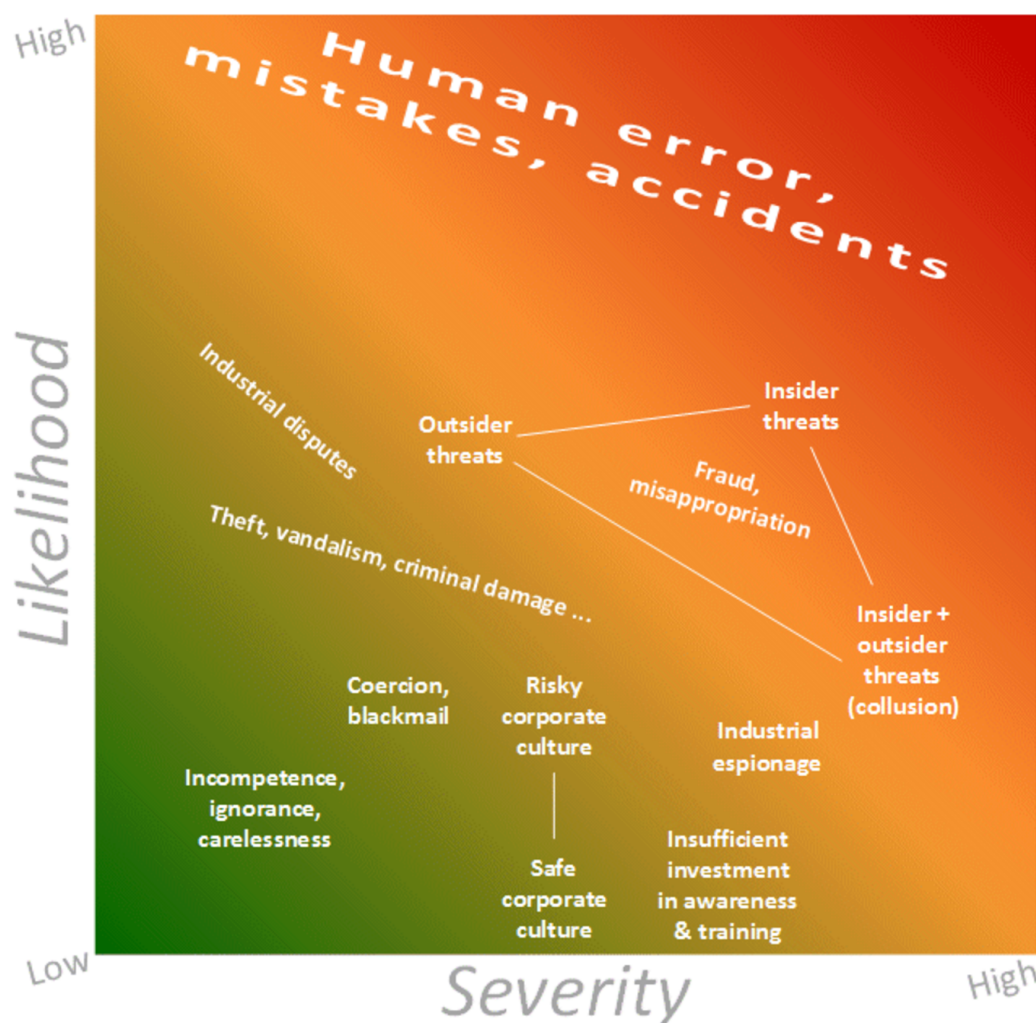
4.5 ARA - Analog Risk Assessment Method

Další velmi jednoduchou metodou, kterou lze použít, je metoda **Analog Risk Assessment Method (ARA)** navržená Gary Hinsonem. Jedná se o metodu, která dává do souvislosti pravděpodobnost a následky realizace rizika, viz obr. 4.3.

Jednoduchost je silnou, zároveň však také slabou stránkou metody. Jednoduchost použití umožňuje provést základní vytipování hrozeb a jejich přibližné ohodnocení z hlediska pravděpodobnosti a závažnosti následků. To je samo o sobě cenný výstup, který může posloužit pro otevření diskuze o rizicích ve společnosti.

Lpění na použití složitých metod, které vyžadují mnohem podrobnější vstupní informace může být také za určitých okolností kontraproduktivní - zejména pokud tyto vstupní informace nejsou přesné. Vzhledem k tomu, že v systémech ISMS obvykle pracujeme s antropogenními riziky, je odhad pravděpodobnosti, motivace útočníka apod. poměrně problematická.

V úvodních fázích práce s rizikem tak může být výhodné použít jednoduchou, rychlou metodu jako je ARA. Podle situace lze pak dále pokračovat nasazením složitějších metod poskytujících podrobnější výsledky.



Obrázek 4.3: ARA - pravděpodobnost vs dopady (převzato z [43])

Tím se také dostáváme ke slabině metody - nelze očekávat, že při použití metody jako je ARA dostaneme kompletní obrázek o rizicích v IT systémech velkých společností.

Použití metody může také vyvolat určitý falešný pocit, že analyzovaným rizikům rozumíme, to však nutně nemusí být pravda, protože tento zjednodušený pohled ignoruje důležité vlastnosti systémů, které k rozhodnutím v oblasti rizik mohou přispívat.

4.6 NIST SP 800-30 rev. 1 - Guide for Conducting Risk Assessments

Jako opak metod opak **BRA** a **ARA** nabízíme postup z NIST SP 800-30 rev. 1, poskytující obecné návody pro realizaci hodnocení rizika. V extenzivních přílohách jsou pak specifikovány některé hrozby, nastavovány škály semikvantitativního hodnocení.

V textu jsou také dostupné šablony tabulek hodnocení, viz např. obr. 4.4.

Jak je z šablony (obr. 4.4) vyplývá je v rámci hodnocení mnohem podrobněji charakterizována samotná hrozba a to z pohledu schopností, úmyslu a cíle.

Výše uvedená šablona je určena pouze pro skupinu rizik vyplývajících z nepřátelských aktivit jednotlivců nebo skupin vůči oprávněným zájmům organizace. Tyto hrozby se vyznačují tím, že útočník se aktivně snaží napadnout chráněný systém za účelem dosažení svých cílů. Kromě této skupiny hrozeb NIST SP 800-30 rev. 1 bere v úvahu také:

- nehody

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Obrázek 4.4: Šablona hodnocení rizik (převzato z [61])

- strukturální hrozby (úložné kapacity, komunikační infrastruktura ...)
- prostředí

Tyto hrozby ale nejsou charakterizovány stejným způsobem - chybí složka aktivního zneužití, proto jsou ostatní typy hrozeb charakterizovány pouze rozsahem následků. Ostatní sloupce (6 - 13) zůstávají stejné, pracuje se:

- relevance hrozby
- pravděpodobnost realizace hrozby
- zranitelnosti a predispozice systému (k realizaci hrozby)
- závažnost a všudypřítomnost
- pravděpodobnost s jakou realizace hrozby bude mít nežádoucí dopady
- celková pravděpodobnost (pravděpodobnost, že hrozba bude realizována a bude mít negativní dopady)
- úroveň dopadu - určení velikosti nežádoucích dopadů
- riziko

Vzhledem ke složitosti metody, není možné postup v tomto textu plně popsat. Standard NIST SP 800-30 rev. 1, je ale dostupný bezplatně online [61] k případnému samostudiu.

4.7 Poznámky k některým běžně používaným metodám analýzy rizik



Průvodce studiem

V průběhu studia dalších předmětů jste měli možnost se seznámit s řadou metod, které je možno použít (aplikovat) i do prostředí počítačové bezpečnosti. Tato podkapitola se nezaměřuje na popis samotných metod, ale spíše diskuzi některých aspektů nasazení a problémům, se kterými se můžete potýkat.

4.7.1 CARVER

Metoda **CARVER** (Criticality, Accesibility, Recuperation, Vulnerability, Effect and Recognizability) byla vyvinuta v průběhu války ve Vietnamu pro účely plánování operací speciálních jednotek - konkrétně pro výběr cílů, jejichž zničení by mělo co možná největší dopad na nepřítele.

Metoda pracuje tak, že každému jejímu parametru, odpovídající jednomu písmenu názvu se přidělí hodnota na škále 1 - 10, kde 10 odpovídá nejvyšší kritičnosti, nejlepší dostupnosti atd. Sečtením hodnot parametrů pak dostaneme celkovou velikost rizika.

Tento údaj nám umožňuje rizika porovnávat a případně vybírat ta, která potřebujeme řešit.

Pro svou jednoduchost schopnost odlišného pohledu na problematiku rizika, se tato metoda postupně rozšířila také do jiných oblastí jako je třeba management nebo také řízení rizik IT.

Při aplikaci metody (nebo některé její varianty) je ale potřeba brát v úvahu také její omezení. Tím základním je původní účel metody - tedy metoda je určena pro identifikaci nejslabšího místa s největším dopadem pro aktivní útok. Metoda proto v oblasti IT je dobře schopna pokrýt hrozby obsahující aktivní element útočníka, který chce napáchat co možná největší škody. Na druhou stranu ale nepokrývá naturogenní hrozby (např. úder blesku), nebo antropogenní hrozby jako jsou běžná selhání hardware apod.

Metoda CARVER tedy není univerzálně použitelná pro všechny hrozby, na to je potřeba pamatovat.

Předtím, než přejdeme na další metody analýz rizik, zkusme pro CARVER rozebrat pravděpodobnostní komponentu rizika. Konečně víme, že riziko je vždy charakterizováno pravděpodobností určitého následku. Podívejte se na začátek podkapitoly 4.7.1 - jaká je zde pravděpodobnost? **(nepokračujte v čtení dokud si neuděláte názor na to, co je pravděpodobnost v CARVER, teprve poté pokračujte ve čtení a porovnejte jestli jste měli pravdu :-)**

Našli jste pravděpodobnost? Napsána tam není... znamená to, že CARVER nebere pravděpodobnost v úvahu? Ne neznamená. U metody CARVER nemáme možnost explicitně nastavit pravděpodobnostní komponentu rizik, problém je, že pravděpodobnost je do metody zavedena implicitně. Tedy je zakomponována přímo do způsobu fungování metody. Pravděpodobnost vyplývá ze způsobu, jakým CARVER chápe riziko.

Metoda vznikla pro vojenské účely jako nástroj pro selekci cílů. Účelem bylo vybrat takové cíle, jejichž zničení by nepříteli způsobilo největší škody. Pro vybraný cíl se pak předpokládá, že skutečně bude vojenskými operacemi zničen. Tedy pravděpodobnost, že nastane následek je 100 % (tedy jistota).

V civilním použití nám základní filozofie zůstává stejná. Na aktiva metoda pohlíží optikou útočníka a předpokládá, že pokud dané aktivum vybere, dokáže jej vyřadit/zničit/ovládnout podle toho, jaký přesně scénář uvažujeme.

Pozor, tento předpoklad ale není pro některé typy hrozeb platný, konkrétně pro naturogenní a neúmyslné antropogenní hrozby. Lze předpokládat, že případným nasazením CARVER pro scénáře rizik vyplývající z takových hrozeb bude pravděpodobnostní komponenta zásadním způsobem nadhodnocená, což způsobí, že management rizik se zaměří na řešení nevhodných rizik, což povede k celkové degradaci bezpečnosti informací (nebo toho, co se snažíme z pohledu rizik řídit).

Nasazení CARVER v takovém případě nemá smysl.

4.7.2 Ishikawův diagram a myšlenkové mapy

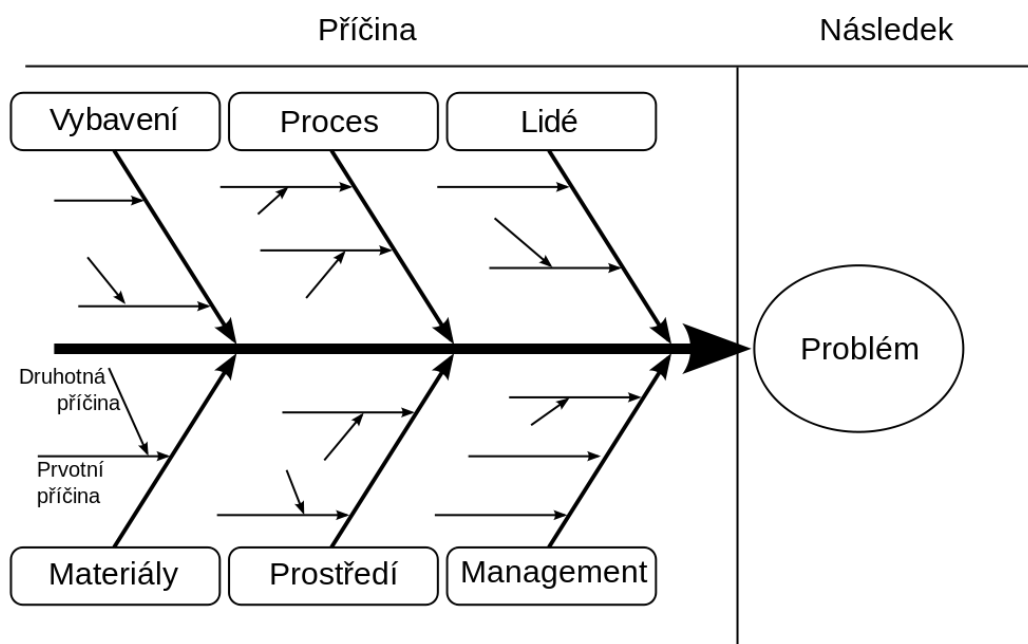
Ishikawův diagram, někdy také označovaný jako diagram příčin a následků je jednou z nejjednodušších metod a zároveň také jednou ze studenty nejoblíbenějších metod.

Metoda umožňuje zkoumat následek a hledat příčiny, které k němu mohly vést. Ishikawův diagram naleznete na obr. 4.5.

Myšlenkové mapy jsou také jednoduchým nástrojem, který je oproti Ishikawu diagramu volnější v tom smyslu že myšlenková mapa není nutně omezena počtem větvení a umožňuje také některé pokročilé funkce, jako jsou odkazy na další zdroje, vytváření dokumentace k jednotlivým uzlům apod., v případě, že je mapa vytvářena v počítači (např. v programu FreeMind [24]).

I myšlenkové mapy jsou notoricky známým nástrojem, který je možno nasadit také při práci s rizikem, viz obr. 4.6.

Obě metody mají společnou jednu věc - jsou primárně určeny pro poznání rizika. Samy o sobě nemají potenciál ho ale celé popsat. Z tohoto důvodu se tyto metody používají na začátku analýzy rizik, pro účely jejich identifikace (identifikace rizika a jeho vlastností) a následně jsou doplňovány dalšími metodami, které jsou schopny riziko v nějaké formě kvantifikovat a umožnit tak účelový výběr rizik k jejich řešení.



Obrázek 4.5: Ishikawův diagram (převzato z [51])

4.7.3 Metoda FMEA

Failure Mode and Effect Analysis (FMEA) je metodou, která umožňuje riziko určit na základě odhadu pravděpodobnosti vzniku nežádoucí události (P), závažnosti jejích následků (N) a odhalitelnosti (H).

Jedná se semikvantitativní metodu pracující obvykle s pětistupňovou škálou. Výsledná hodnota RPN se vypočte dle (4.4) a pohybuje se v rozmezí 0 - 125.

$$RPN = P \cdot N \cdot H \quad (4.4)$$

Postup metody FMEA je standardizován, konkrétně v normě IEC 60812 [21].

Z hlediska vyhodnocování je postup poměrně přímočarý. Rizika se seřadí podle RPN a určí se přijatelná míra RPN oddělující rizika, která je nutné řešit od těch jejichž řešení nebude mít takovou prioritu.

Tato přijatelná míra může být určena libovolně, měla by být ale zdůvodnitelná (mít vnitřní konzistenci). Přijatelnou úroveň lze stanovit předem na škále 0 - 125, nezávisle na provedené analýze. Alternativně lze vybrat např. horních 20 % rizik k řešení (myšleno prvních 20 % rizik z celkového počtu rizik seřazených dle RPN).

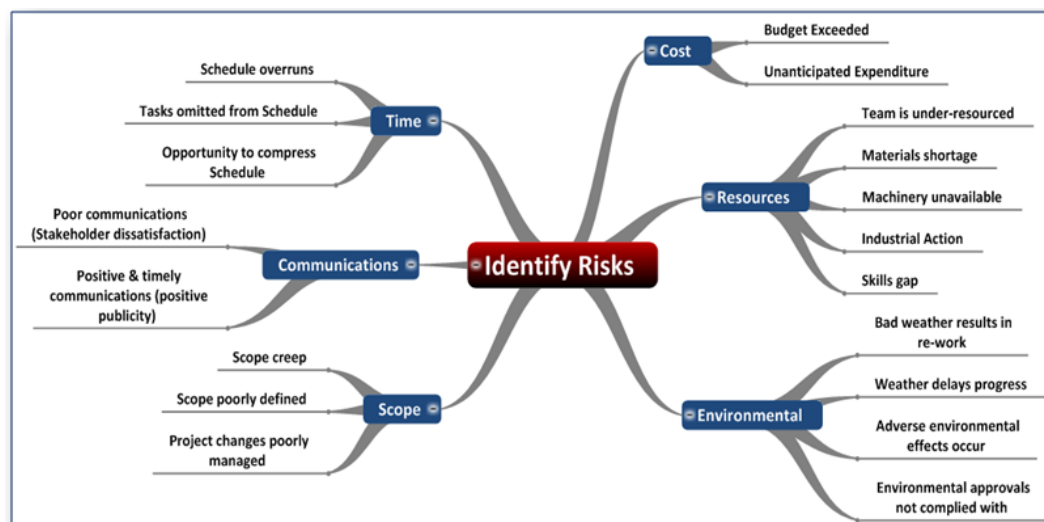
Bez ohledu na způsob určení této hranice nelze postupovat dogmaticky. Pokud postupujeme druhým způsobem (20 % nejzávažnějších rizik) může se stát, že hranice přijatelnosti povede mezi dvěma riziky, které ale mají srovnatelné RPN . Pokud tak jedno z těchto rizik budeme řešit zatímco to druhé ne, bude to nejspíše chyba.

Nevýhodou takového přístupu je, že v každém pořadí jsou vítězové a poražení (někdo je na prvním místě a někdo na posledním). Pořadí samo o sobě nám neposkytuje informaci o závažnosti rizika. Licos může naznačit hodnota RPN - pohybuje se někde v horních patrech (> 100) nebo je hodnota spíše nízká (< 50)?

Jako u každé metody je proto nutné výsledky kriticky zhodnotit - nelze je tedy pouze mechanicky přejímat.

4.7.4 Paretův graf

Paretův princip byl formulován na základě pozorování italského ekonoma Vilfreda Pareta poměru příčin a důsledků, které z nich plynou. Pozorováním zjistil, že obvykle platí, že 20 % příčin je odpovědnou za 80 % následků. Původní poměr byl odvozen pozorováním výrobní linky a zkoumáním příčin výroby zmetků.



Obrázek 4.6: Myšlenková mapa (převzato z [22])

Tento princip má širší implikace a lze jej nasadit např. pro účely oddělení důležitých a méně důležitých rizik. Vizualizaci lze provést pomocí paretova grafu (viz obr. 4.7), který na jedné ose Y (vlevo) je vynášena sledovaná hodnota, např. hodnota rizika, na druhé ose Y (vpravo) je vynášena kumulovaná hodnota sledované veličiny v %.

Tím, že příčiny jsou řazeny sestupně podle hodnoty následku platí, že rizika při postupu zleva doprava představují stále menší podíl na následcích. Určením zájmové procentní hodnoty tak můžeme oddělit podstatné od nepodstatného.

Paretův princí nám říká jednu podstatnou věc a to, že bychom se při řešení problémů měli zaměřit primárně na to podstatné. Poměr 80:20 je ale pouze orientační - proto opět je nutno interpretovat dosažený výsledek tak, aby výsledek analýzy dával logický smysl. Není tedy vhodné řez mezi dvěma riziky, jejichž hodnota je takřka stejná.

Je také potřeba si dávat pozor na vstupní hodnoty analýzy. Zkusmě použít jako vstup pro konstrukci grafu výsledek metody FMEA z předchozí podkapitoly.

Rizika seřadíme podle hodnoty RPN a tuto hodnotu zaznamenáme pomocí sloupcového grafu (levá osa Y). Spočteme $\sum RPN = 100\%$ a na pravou Y-ovou osu vyneseme kumulativní procentní podíl jednotlivých rizik. Nakonec zvolíme zájmovou procentní hodnotu (např. 80 %) a použijeme ji k rozlišení mezi řešenými a akceptovanými riziky.

Našli jste se ve výše uvedeném postupu? Osobní zkušenost autora naznačuje, že většina studentů se ve výše uvedeném najde (takže jste v dobré společnosti). Otázka je: *proč tedy toto dále diskutovat?* Situace je jasná, dostali jsme výsledky ... je vymalováno.

Problém je, že tyto výsledky mohou být zavádějící. Účelem metody FMEA je ohodnotit rizika a seřadit je. Vypočtená hodnota RPN ale nutně nereprezentuje věrně skutečný rozdíl mezi riziky. Zkusme zformulovat jednoduchý příklad, na kterém budeme problém demonstrovat.

Uvažujme dvě podobná rizika se stejnou hodnotou H , $N = 3$, rizika se drobně liší, pravděpodobnosti realizace. Pro R_1 $P = 79\%$, tedy $P_1 = 4$, pro R_2 $P = 81\%$, tedy $P_2 = 5$.

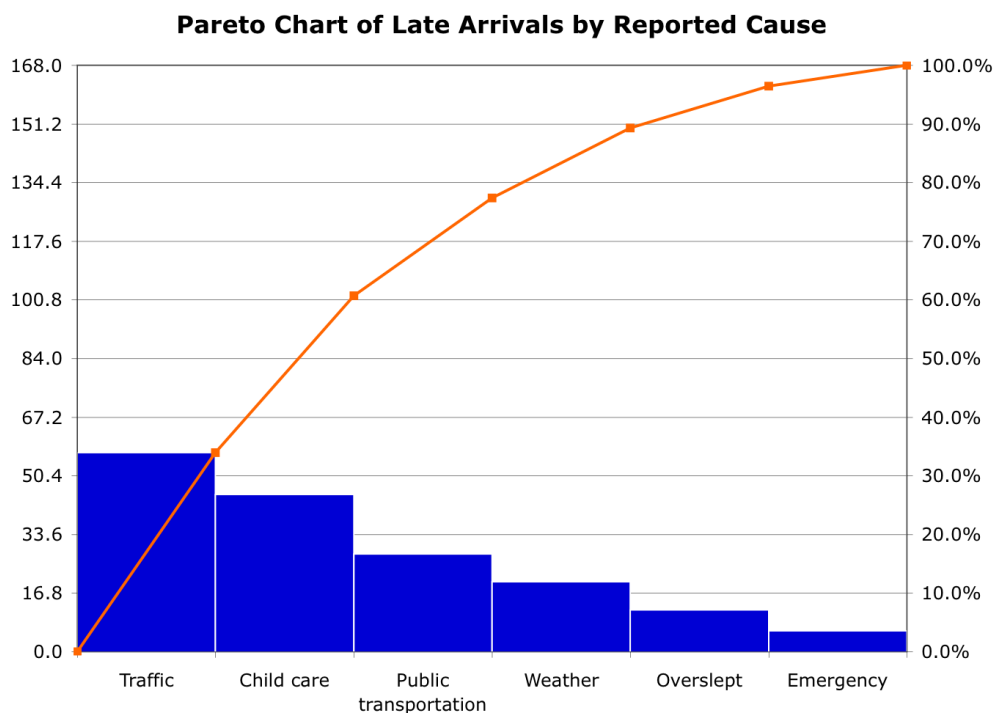
Z uvedených hodnot můžeme spočítat hodnotu RPN:

$$RPN_1 = 4 \cdot 3 \cdot 3 = 36$$

$$RPN_2 = 5 \cdot 3 \cdot 3 = 45$$

Faktický rozdíl mezi oběma riziky je 2 % v pravděpodobnosti realizace. Podle hodnoty RPN je ale rozdíl podstatně větší $RPN_1 = 36$ je 80% RPN_2 . Tedy RPN signalizovaný rozdíl mezi riziky je signifikantně větší než je skutečný rozdíl mezi nimi.

Uvažovat lze i opačný příklad, kdy RPN signalizovaný rozdíl bude menší než skutečný. Stačí abychom pravděpodobnosti stanovili následovně: $P_1 = 61\% \dots P_1 = 4$ a $P_2 = 100\% \dots P_2 = 5$. Ačkoliv se hodnoty RPN nezměnily, hodnoty pravděpodobností jsou signifikantně odlišné.

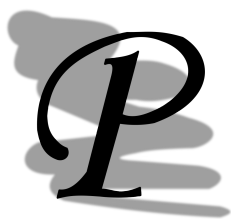


Obrázek 4.7: Paretův graf (převzato z [52])

Výše uvedené není možné považovat za chybu **FMEA**, protože metodou určené pořadí je správné. Přiřazením skutečné hodnoty P, H, N do pětistupňové škály se ale ztrácí část informací o řešeném problému - tyto informace by zrovna při konstrukci Paretova grafu byly užitečné.

Použitý model rizika byl v tomto případě klíčovým faktorem, který ovlivnil přijatelnost výstupu FMEA pro účely konstrukce Paretova grafu.

Obdobný problém lze nalézt u téměř všech kvalitativních a semi-kvalitativních metod. Jako příklad lze zmínit matici rizik, o které jsme se ale bavili již v kapitole 2.



Metody analýzy rizik

Vaše studium se doslova točí okolo rizika ... v různých podobách. Udělejte si seznam metod, se kterými jste se v průběhu studia (i tohoto předmětu) setkali a prozkoumejte předpoklady a omezení, která jsou do těchto metod zabudovaná.



Shrnutí kapitoly

Tato kapitola se věnuje metodám a postupům při řízení rizik v oblasti systémů řízení bezpečnosti informací (ISMS). Obecný postup analýzy rizik zahrnuje identifikaci aktiv, zranitelností, odhad pravděpodobností a výpočet očekávaných ztrát, přičemž v IT prostředí jsou vazby mezi aktivy (zahrnujícími software) složitější než u běžných fyzických rizik. Součástí hodnocení dopadů incidentů, je nutnost započítat nejen přímé náklady na obnovu, ale i ušlé příjmy, smluvní pokuty či poškození dobrého jména organizace, k čemuž lze využít cost-benefit analýzu (CBA) nebo multikriteriální analýzu (MCA). Samotná identifikace rizik může vycházet buď „zespoda“ od jednotlivých IT aktiv, nebo z analýzy firemních procesů, přičemž je klíčové jasně definovat vlastníka rizika jako osobu osobně motivovanou a dostatečně vysoko postavenou, aby dokázala získat prostředky na řešení daného problému.

Mezi velmi jednoduché a rychlé postupy vhodné pro úvodní fáze práce s rizikem patří Binary Risk Analysis (BRA), která umožňuje určit riziko na základě deseti binárních otázek (ano/ne) vyhodnocovaných po dvojicích, a Analog Risk Assessment (ARA), jež dává do souvislosti pravděpodobnost a následky pro rychlé otevření vnitrofiremní diskuse. Jako protiklad k těmto zjednodušeným modelům je uveden robustní standard NIST SP 800-30 rev. 1, který podrobně charakterizuje hrozby z pohledu schopností, úmyslu a cíle útočníka a v rámci hodnocení přísně rozlišuje nepřátelské aktivity od nehod, strukturálních či environmentálních hrozeb.

Bez ohledu na to, kterou metodu analýzy rizika organizace nakonec použije, je vždy nutné pochopit předpoklady a omezení metody. Například metoda CARVER, vyvinutá původně pro vojenské účely, implicitně předpokládá stoprocentní úspěch útoku a nehodí se pro živelní pohromy nebo běžná selhání hardwaru. Ishikawův diagram a myšlenkové mapy zase slouží primárně k prvotní identifikaci a poznání rizik, nikoliv k jejich následné kvantifikaci. U metod FMEA (využívající index RPN) a Paretova grafu autor může dojít ke zkreslení reality, ke tomu dochází při převodu skutečných pravděpodobností na semikvantitativní škály, což může uměle zvětšit nebo zmenšit signalizovaný rozdíl mezi riziky a negativně ovlivnit rozhodování o tom, která rizika budou managementem řešena a která akceptována.

Kapitola 5

Případové studie bezpečnostní dokumentace ISMS



Průvodce studiem

V této kapitole načtneme několik příkladů různých typů dokumentů, které hrají úlohu v systému ISMS.

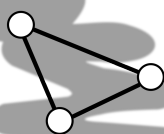
klíčová slova: ISMS, případová studie, Politika ISMS, Politika aktiva, Management aktiv

Požadované vstupní znalosti: text této kapitoly předpokládá, že jste zvládli všechny předchozí kapitoly.



Čas nutný ke studiu

Na prostudování kapitoly budete potřebovat přibližně půl hodiny na dokument. Doporučujeme se studovat příklady před započítím prací na patřičném semestrálním projektu. Dokumenty, které na semestrální projekt nezpracováváte je pak vhodné nastudovat v rámci přípravy na zkoušku.



Šablony dokumentů ISMS

Pro potřeby studia jsme připravili všech základních typů dokumentů, viz [83].. Šablony jsou dostupné také v LMS v kurzu předmětu a na portálu e-výuka tamtéž.

Šablony jsou komentované a jsou výrazně podrobnější než je text této kapitoly. Doporučujeme proto, aby jste je prostudovali také.

Dokumenty diskutované v této kapitole prosím berte pouze jako příklad - v žádném případě se nejedná o úplné dokumenty, které je možno bez úprav aplikovat v různých systémech ISMS. Účelem je tedy poskytnout základní inspiraci a sloužit jako odrazový můstek pro zpracovávání skutečných dokumentů.

Příklady pokrývají následující oblasti:

- politiku ISMS
- management konfigurací
- bezpečnostní politiku aktiva

Naopak příklad rizikové analýzy v tomto textu nenajdete, jelikož jste již v průběhu studia měli možnost se s tímto typem analýz setkat. Každopádně ale doporučujeme prostudovat kapitolu *Metody a postupy při řízení rizik*.

Při čtení pečlivě rozlišujte mezi textem politik a komentářem tohoto textu. Sekce komentáře budou vizuálně odděleny od textu samotného.

5.1 Politika ISMS

Komentář *Politika ISMS je v tomto případě sestavena pro smyšlenou společnost ABCD, s. r. o., která zpracovává řadu citlivých informací o svých zákaznících a jejich potřebách. Problém, který se zavedením politiky ISMS snaží vyřešit je zabránění úniku duševního vlastnictví firmy a neoprávněný přístup k informacím o zákaznících.*

Úvod

Společnost ABCD s. r. o. si je vědoma odpovědnosti, kterou má vůči svým zákazníkům a smluvním partnerům a zavazuje se programově zajistit důvěrnost veškerých informací, které od nich získává, stejně jako dalších údajů a postupů, které společnost ABCD s. r. o. využívá ve své činnosti.

Tato politika ISMS je formálním vyjádřením tohoto závazku a je určena pro nastavení základních pravidel nakládání s údaji v elektronické i papírové podobě a organizace řízení informační bezpečnosti ve společnosti.

Politika je zpracována podle ustanovení norem ISO 27001 a ISO 27002 a je závazná pro všechny zaměstnance společnosti ode dna nabytí účinnosti.

Komentář *V úvodní části je vždy nastolen problém - společnost se hlásí k jeho řešení a specifikuje se podle jakých norem nebo jiných předpisů se bude postupovat. V tomto textu předpokládáme, že se organizace rozhodla systém ISMS implementovat sama. Pokud by ji ale k tomu nutila regulace, např. zákon O kybernetické bezpečnosti, pak by zde měl být také odkaz na tento zákon a jeho prováděcí vyhlášky, kterou se organizace přihlásí k vysoké nebo nízké úrovni regulace.*

Glosář

...

Komentář *Do glosáře, seznamu zkratk, základních pojmů (nebo jakéhokoliv jiného použitého názvu) patří pojmy, u kterých je nutné, aby je uživatel pochopil skutečně jednoznačným způsobem. Používáme proto takové pojmy, které mohou mít různý výklad (v závislosti na použitém kontextu), nebo takové pojmy, u kterých se domníváme, že by uživatel nemusel pochopit jejich správný význam přímo z textu. Zařazujeme pouze takové pojmy, které se vyskytují v textu politiky.*

Organizace informační bezpečnosti

Ředitel společnosti (CEO)

je nejvyšším výkonným orgánem společnosti. V oblasti IT bezpečnosti:

- schvaluje bezpečnostní dokumentaci
- předkládá jednatelem na vyžádání, popř. dle vlastního uvážení informace o bezpečnostních incidentech ve společnosti
- bere na vědomí roční zprávu o stavu informační bezpečnosti ve společnosti
- jmenuje a odvolává ředitele informační bezpečnosti
- jmenuje a odvolává auditory

Ředitel informační bezpečnosti (CISO)

Vede odbor informační bezpečnosti společnosti. V otázkách informační a technické bezpečnosti se zodpovídá řediteli společnosti. V otázkách informační bezpečnosti pak spolupracuje úzce s Radou IT:

- předkládá je schválení roční zprávu o informační bezpečnosti společnosti,
- organizuje analýzu rizik v oblasti informační bezpečnosti a je zodpovědný za dlouhodobé řízení těchto rizik
- předkládá návrhy bezpečnostní dokumentace IT k projednání,
- informuje Radu o závažných bezpečnostních incidentech ve společnosti a hrozbách, kterým společnost v oblasti IT čelí.
- dle vlastního uvážení nebo na doporučení rady zajišťuje služby externích společností konzultačního charakteru (v oblasti bezpečnosti IT) nebo penetračního testování

Ředitel IT (CIO)

Zodpovídá za oblast provozu systémů IT ve společnosti, zejména pak za procesy:

- pořízování, provozu a vyřazování aktiv IT
- správy (administrace) IT aktiv

V těchto otázkách úzce spolupracuje s ředitelem informační bezpečnosti. Ředitel IT zodpovídá také za implementaci opatření obsažených ve schválené bezpečnostní dokumentaci IT.

Komentář: pokud organizace spadá do vysoké míry regulace dle zákona O kybernetické bezpečnosti, musí řešit také požadavky na odbornou způsobilost CISO (a některých dalších rolí) a neslučitelnost rolí CIO a CISO.

Obdobným způsobem definujeme další klíčové bezpečnostní role:

- architekt KB
- garant aktiva
- auditor
- uživatel

*Komentář: většinu rolí byste měli být schopni vymezit na základě znalostí získaných při studiu předchozích kapitol. Pro úplnost ale rozepíšeme **uživatele**, kterým jsme se dosud příliš nezabývali.*

Uživatel

Představuje roli, která plní úlohu příjemce požadavků kladených systémem ISMS. Jedná se o „catch-all“ roli, pro osoby, které neplní v systému ISMS žádnou specifickou roli.

Výbor KB

je poradním orgánem Ředitele společnosti, zřízená předpisem XYZ Statut [odkaz]. Hlavním úkolem výboru je projednávání a řešení strategických otázek v oblasti bezpečnosti informací, zejména pak projednávání a přijímání předpisů v této oblasti. Takto společnost závazně stanovuje svůj postoj k informačnímu riziku.

Složení rady je následující:

- ředitel společnosti (předseda výboru)
- ředitel informační bezpečnosti (místopředseda výboru)
- ředitel IT
- architekt kybernetické bezpečnosti

Výbor KB se schází minimálně 4x do roka, obvykle 1x za čtvrtletí. Body k projednání předkládají členové výboru dle vlastního uvážení.

Předseda, popř. místopředseda (v nepřítomnosti předsedy) má právo k jednání výboru přizvat další osoby dle potřeb výboru, obvykle v souvislosti s projednáváním body. Takto přizvané osoby (hosté), ale nejsou považovány za členy výboru a nemají v něm hlasovací práva.

Přizvaným hostům také pozváním na jednání nevzniká automaticky nárok na seznamování se s důvěrnými informacemi, pokud k těmto informacím neměli přístup už před pozváním z titulu jiných funkcí, které vykonávají pro společnost.

Postup hlasování, archivace záznamů jednání rady jsou podrobně řešeny v předpise XYZ Statut [odkaz].

Komentář Informační bezpečnost je v různých organizacích organizována různě. V této kapitole politiky ISMS je proto stanovováno, jak přesně takové řešení vypadá. Součástí kapitoly může být diagram organizační struktury společnosti, ovšem s tím, že se musí jednat o diagram účelový - tedy reprezentující primárně ty části organizační struktury, které jsou významné pro řízení informační bezpečnosti. Tento diagram jsem v příkladu nezpracoval, inspiraci lze ale najít v kapitole systémy řízení informační bezpečnosti.

Při výkladu se opět neřeší v obecné rovině, jaký úkol daná pracoviště/oddělení apod. mají, v úvahu bereme pouze úkoly, které mají vazbu na řízení informační bezpečnosti.

Tyto úkoly lze popisovat volným textem nebo např. formou odrážek, nebo kombinací obojího, dle potřeby. U pracovišť, která fungují na základě nějakého speciálního vnitropodnikového předpisu je pak potřeba tuto návaznost zaznamenat např. formou odkazu nebo poznámky pod čarou.

Role

S výkonem práce ve společnosti na provozovaných IT aktivech jsou spojovány určité role. Základními rolami v systému ISMS jsou:

- administrátor,
- uživatel,
- auditor.

Kromě těchto základních rolí mohou jednotlivé systémy IT vyžadovat existenci dalších rolí v souvislosti s činnostmi, které systém zajišťuje.

Architekt KB

je osobou zajišťující návrh a implementaci bezpečnostních opatření. Architekt KB musí být ke své činnosti odborně způsobilý. Svou způsobilost prokazuje bezpečnostními certifikacemi a praxí v oboru.

Role architekta KB není slučitelná s jinými bezpečnostními rolami.

Komentář: výše uvedené je pouze naznačením funkcí. Jelikož je tato role vyžadována explicitně pro organizaci ve vyšší míře regulace dle zákona O KB, mohou zde být odkazy na příslušné části vyhlášky 409/2025 Sb., popř. lze z ní převzít definici a požadavky na tuto roli. Lépe se pak prokazuje soulad s legislativou.

Garant aktiva

garantem aktiva je osoba pověřená správou aktiva. Garant je určen pro každé aktivum obvykle během pořizovací fáze životního cyklu aktiva, nejčastěji vlastníkem aktiva, který garanta také zavede do systému evidence aktiv.

V případě IT aktiv vykonává roli garanta administrátor aktiva. Administrátor provádí prvotní konfiguraci aktiva pro použití. V průběhu života aktiva pak provádí administrátor běžnou údržbu aktiva - včetně instalace bezpečnostních záplat, změn v konfiguraci apod. mající za cíl zajistit dlouhodobě bezpečné poskytování služeb aktiva jeho uživatelům.

Pro zajištění chodu aktiva může garant přijímat provozní opatření, které mohou dočasně nebo trvale omezit některé služby nebo způsob jakým tyto služby uživatelé využívají. Uživatelé jsou povinni tato omezení akceptovat, popř. poskytnout součinnost při jejich naplňování, mají ale právo na to, aby jim účel těchto nařízení/omezení byl sdělen a vysvětlen.

Uživatel má právo oslovit garanta s žádostí o pomoc v případě, že při práci s aktivem se setká se závadou, podezřením na bezpečnostní incident nebo jiným problémem, který narušuje schopnost uživatele využívat aktivum. Administrátor se takovými žádostmi musí zabývat bezodkladně (obvykle do 3 pracovních dnů), nemusí však této žádosti vyhovět. Uživatel má právo být informován o způsobu vyřízení jeho žádosti, ať už kladném nebo záporném. V případě zamítnutí požadavku musí být zamítnutí doprovázeno zdůvodněním.

Přesné povinnosti a postupy garanta jsou popsány v „Bezpečnostních politikách“ těchto aktiv.

Auditor

Auditorem se v tomto textu rozumí interní pracovní pozice organizace odpovědná za provádění auditů. Úkolem auditora je kontrola způsobu použití jednotlivých zájmových aktiv IT a procesů, které je využívají. Auditři jsou jmenováni vedením společnosti (ředitelem společnosti) s vymezením oblasti, které se auditor bude věnovat.

Audity probíhají v pevně stanovených časových intervalech, zaznamenanými v plánu auditů (plánovaný audit) a také nepravidelně (neplánovaný audit) - např. na vyžádání ředitele společnosti nebo Výboru KB.

Úkolem auditora je kontrola jestli jsou aktiva využívána předepsaným způsobem (dle procesů) a také, zdali jsou tyto procesy efektivní. Výsledkem auditu je Zpráva z auditu, která především dokumentuje zjištěné rozpory, problémy, ale také další postřehy, jako jsou např. nevyužití příležitosti a doporučení k dalšímu rozvoji auditovaných systémů.

Auditní zprávu předává auditor řediteli společnosti a vedoucímu útvaru, jehož aktiva/procesy byly auditovány.

Vedení společnosti má právo zadat externí audit svých aktiv popř. procesů. Průběh a předání výsledků takového auditu se neřídí ustanoveními předchozích odstavců (ty se týkají pouze auditorů - zaměstnanců společnosti), ale smlouvou mezi společností a externím auditorem.

Uživatel

Uživatelé jsou povinni při práci s aktivem řídit se pokyny administrátora a také postupy využití aktiva popsané v dokumentaci procesů využívajících aktivum.

Uživatel má právo na to být pro využití aktiva proškolen v případě, že uživatelská obsluha aktiva vyžaduje specifické znalosti, u kterých se nedá automaticky předpokládat znalost ze strany uživatele¹.

Uživatel má právo oslovit administrátora s žádostí o pomoc v případě, že při práci s aktivem se setká se závadou, podezřením na bezpečnostní incident nebo jiným problémem, který narušuje schopnost uživatele využívat aktivum. Administrátor se takovými žádostmi musí zabývat bezodkladně (obvykle do 3 pracovních dnů), nemusí však této žádosti vyhovět. Uživatel má právo být informován o způsobu vyřízení jeho žádosti, ať už kladném nebo záporném. V případě zamítnutí požadavku musí být zamítnutí doprovázeno zdůvodněním.

Všichni uživatelé musí být při nástupu proškoleni v oblasti nakládání s informacemi a základní orientaci ve vnitropodnikových předpisech. Za provedení školení je zodpovědné personální oddělení, které také výsledky školení (prezenční listiny), společně s podepsanými prohlášeními o mlčenlivosti archivuje.

Komentář *Porovnejte formulace ve stati týkající se garanta aktiva a uživatele. Všimněte si, že řada ustanovení je symetrických - tedy na jedné straně vznikají práva, na druhé straně jsou pak povinnosti. (Jeden odstavec se dokonce v obou částech opakuje.) Interakci obou rolí nelze řešit pouze u garanta aktiva nebo uživatele z důvodu pochopitelnosti textu.*

Lze předpokládat, že při studiu předpisu budou čtenáři věnovat zvýšenou pozornost ustanovením, která mají přímou souvislost s výkonem jejich práce. Je proto nutné zajistit, aby statě jednotlivých rolí poskytovaly úplný obrázek o požadavcích, které na ni klademe.

Vyvážení práv a povinností je také strategickým krokem, kterým zjemňujeme psychologicky požadavky kladené na jednotlivé skupiny pracovníků. Pokud povinnost konat určitým způsobem s sebou nese určitá práva, psychologicky působí povinnosti lépe, než když stojí osamoceně.

Management aktiv

Pro zajištění požadované úrovně informační bezpečnosti je nutno získat kontrolu nad všemi zájmovými informačními aktivy.

V této oblasti rozlišujeme především primární aktiva zajišťující běh kritických činností organizace a aktiva podpůrná ať už technického charakteru (hardware, software, apod.), tak jiná technická zařízení jako jsou budovy a to včetně jejich obsluhy, které zajišťují funkci primárních aktiv.

Aktiva obou typů je procesem potřeba identifikovat a určit jejich garanty. Výstupem procesu je Soupis aktiv a jejich garantů, který udržuje CISO.

Proces se řídí předpisem [XYZ].

Soupis aktiv slouží jako podklad pro provedení rizikových analýz. Obsah a rozsah o aktivech evidovaných údajích je stanoven v předpisu *Evidence IT aktiv*.

Komentář *Evidence aktiv je v politice ISMS řešena pouze ve smyslu základních principů a zařazení do systému ISMS. Vše ostatní je řešeno ve specializovaném předpisu, který je v textu pouze odkazován.*

Management rizik

Management rizika zájmových aktiv IT je základním nástrojem systému řízení informační bezpečnosti k získání kontroly nad riziky a jejich možnými následky. Součástí managementu rizik jsou procesy:

- identifikace rizik (proces SPR-15-123456)
- evaluace (hodnocení) rizika (proces SPR-15-123457)
- vypořádání se s rizikem (proces SPR-15-123458)

Procesy managementu rizik spravuje CISO.

Identifikace rizik probíhá najednou pro celou společnost a všechna její zájmová aktiva identifikovaná v seznamu aktiv. Hodnocení rizik aktiv provádí s použitím *Metodologie hodnocení rizik společnosti* [XYZ] oddělení informační bezpečnosti ve spolupráci s guaranty aktiv.

¹Za běžný standard znalostí lze např. považovat základní obsluhu počítače a kancelářských produktů (MS Word, MS Excel). Naopak znalost způsobu přípravy tiskových sestav agend vedených v informačním systému SAP nelze automaticky předpokládat, proto tyto znalosti bude potřeba systematicky budovat formou školení.

Výstupem je plán zvládání rizik schvalovaný Výborem KB.

Všechny aktivity managementu rizik musí být pro každé aktivum řádně provedeny a zdokumentovány, viz podrobněji předpis *Management rizik systému ISMS společnosti XYZ*.

Komentář *V celé stati managementu rizik jsou extenzivně odkazovány další dokumenty, ať už dokumentace procesů, tak specializovaný předpis pro Management rizik. Účelem politiky ISMS není podrobně rozepisovat principy managementu rizik, pouze vymezení, že existuje, nastínit základní princip a jak je řízení rizik zapojeno do systému řízení informační bezpečnosti a vše ostatní je řešeno podrobně v navazujících předpisech.*

Bezpečnostní incident

Jsou veškeré incidenty, které mají potenciál narušit důvěrnost, integritu nebo dostupnost uchovávaných informací v systémech společnosti. Ačkoliv zabránit vzniku bezpečnostních incidentů úplně nejde, lze realizovat procesy a postupy, které výskyt bezpečnostních incidentů minimalizují.

Opatření jsou obvykle navrhována na základě provedených rizikových analýz a jsou realizována procesy v bezpečnostních politikách jednotlivých aktiv.

V případě, že bezpečnostní incident skutečně nastane - je nutné minimalizovat jeho dopad na chod organizace, co možná nejrychlejší obnovou funkce IT aktiv, jejichž činnost byla narušena. Za provedení procesu obnovy činnosti aktiva je zodpovědný garant aktiva, k obnově přistupuje až po shromáždění informací o incidentu.

O průběhu a řešení incidentu musí administrátor zpracovat zprávu, Rozsah zprávy je přímo úměrný závažnosti bezpečnostního incidentu. Zpráva se vkládá na Help Desk - zadá Bezpečnostní incidenty. Při zpracování zprávy používá garant aktiva šablonu: *Hlášení bezpečnostního incidentu*. V případě závažných bezpečnostních incidentů musí být informován také CISO, který bude informovat Výbor KB o následcích a průběhu řešení bezpečnostního incidentu, popřípadě mohou být realizovány další opatření s cílem zamezení opakování incidentu.

Komentář *Celá sekce bezpečnostního incidentu mohla napsána zcela jinak a mohla také být umístěna jinde. Tato sekce by např. mohla poměrně dobře fungovat na začátku textu (za Úvodem). Konečně, jsou zde základní principy informační bezpečnosti a celková snaha zabránit vzniku a minimalizovat následky bezpečnostních incidentů.*

V tomto případě jsem se ale rozhodl umístit sekci až skoro na konec a to proto, že zde nastiňuji také základní principy řešení incidentů a k tomu potřebuji použít některé role. Sekce proto musí v mém případě následovat až za specifikací těchto rolí. Sekci ale šlo napsat také jinak. Jednotlivá opatření mohla být zapsána do jednotlivých rolí a funkcí.

Obecně platí, že neexistuje jeden správný způsob jak psát tento typ dokumentů. Vždy proto usilujte o to, aby výsledek Vaší práce byl konzistentní - měl určitou vnitřní logiku. Opatření tedy neplácáme dohromady náhodně - vždy sledujeme určitý cíl.

Všimněte si, že v textu se objevuje pojem závažný bezpečnostní incident, tento pojem ale v textu není vysvětlen. Tento problém lze řešit dvěma způsoby - buď jej nadefinujeme přímo v textu (pravděpodobně někde na začátku sekce Bezpečnostní incident, alternativně lze pojem nadefinovat v pojmech.

Závěrečná ustanovení

Vzhledem k rychlým změnám v oblasti informační bezpečnosti musí být tento předpis a předpisy z něj odvozené (např. bezpečnostní politiky jednotlivých aktiv) revidovány minimálně 1x ročně.

Tento dokument vstupuje v platnost podpisem statutárního zástupce společnosti.

5.2 Organizace informací o aktivech IT

Úvod

Tento předpis slouží pro stanovení obsahu a rozsahu informací shromažďovaných o primárních a podpůrných aktivech společnosti a způsobu jejich shromažďování.

Účelem shromažďování informací o aktivech je především:

- identifikace všech aktiv, které společnost používá pro zpracování chráněných informací
- určení garantů těchto aktiv

Komentář: výše uvedené dvě položky jsou povinné. Bez nich nemůže ISMS fungovat, protože bez nich nelze postavit analýzy rizik.

- získání informací nutných pro provedení rizikových analýz
- získání některých provozních informací umožňujících vyhodnocení efektivity investic do IT a efektivnější plánování investic nových
- slouží jako podklad pro evidenci některých druhů majetku ve společnosti
- správu licencí software společnosti
- slouží jako podklad pro identifikaci osob pracujících s aktivy a plánování školení

Komentář *Všimněte si, že celý dokument není pojmenovaný inventarizace aktiv. Důvodem bylo zdůraznění širšího účelu získání kontroly nad aktivy než je pouhá kontrola existence/přítomnosti aktiva na stanoveném místě.*

Klasifikace IT aktiv

Informační aktiva rozlišujeme především na primární a podpůrná. Primární aktiva představují klíčové agendy a informační systémy, které zajišťují činnosti potřebné k chodu společnosti. Podpůrná aktiva jsou podpůrné prostředky, které umožňují provoz primárních aktiv. Podpůrná aktiva jsou především:

- hardware (především počítače, notebooky, mobilní telefony, tablety a obdobná zařízení)
- softwarové prostředky (především operační systémy, kancelářský software, informační systémy a další software)
- lidé (evidence zaměstnanců a jejich rolí při práci s aktivy)
- budovy
- a další

Každý druh aktiva má vlastní způsob označování (evidence) a je s ním spojen jiný rozsah evidovaných údajů.

Pro každé aktivum je určuje garant.

Garantem se rozumí osoba, která je zodpovědná za provoz aktiva. V případě primárních aktiv se jedná obvykle o manažera zodpovědného za agendu vedenou tímto aktivem. V případě technických aktiv jako např. hardware a software je garantem obvykle administrátor aktiva. V případě ostatních aktiv (např. budovy) je garantem obvykle správce.

Seznam aktiv s informací v požadovaném rozsahu s přidělovanými guaranty vede CIO na základě podkladů od garantů aktiv.

Evidence údajů

Seznam aktiv a jejich garantů je technicky implementován v systému CMDB. Evidence údajů probíhá zpravidla musí proběhnout souběžně s jakoukoliv provozní změnou aktiva (např. pořízení/-vyřazení, změna vlastníka, přijetí do pracovního poměru a další).

Evidence je realizována systémem CMDB ve správě oddělení IT společnosti. Záznam provádí v případě hardware a software garant aktiva (v případě převodu aktiva provádí záznam původní garant aktiva), v případě zaměstnanců provádí záznam o zaměstnanci personální oddělení.

Dodatečné informace, jako je např. přiřazení pracovníka k určitému aktivu jako administrátor/uživatel nebo v jiné roli probíhá zadáním identifikátoru zaměstnance z informačního systému personalistiky do databáze CMDB k danému aktivu se specifikací role.

Komentář *V textu o bezpečnostních politikách (bezpečnostní dokumentaci obecně) bylo napsáno, že předpisy by se měly psát co možná nejobecněji tak, aby v případě jejich změny nebylo potřeba provádět rozsáhlejší revize bezpečnostní dokumentace. Všimněte si, že tento principi jsem v předchozích odstavcích porušil tím, že jsem se přihlásil k používání CMDB, mohl bych dokonce specifikovat konkrétní produkt.*

V tomto případě, pokud chci využít nějaký systém CMDB, pak pokud evidence nemá být pouze formou tabulek, tak musím být konkrétní - databáze CMDB nejsou standardizovány. Fakt, že společnost implementuje takový nástroj znamená, že bude investovat nemalé finanční prostředky do realizace datových pump a přejímání informací např. ze systému personalistiky nebo jiných. Systém CMDB je tak poměrně úzce svázan s tímto předpisem a nemá smysl to nějak zastírat.

Primární aktiva

se evidují názvem garantem, účelem provozu a odkazy na podpůrná aktiva v evidenci, která zajišťují jeho provoz.

*Podpůrná aktiva**PC, servery a notebooky²*

Název se skládá z označení PC (osobní počítače), NTB (pro notebook) nebo SRV (pro servery), označením místnosti, kde se nachází (A04) a pořadovým číslem zařízení tohoto typu v místnosti - např. „PCA0404“.

Z dalších údajů musí být evidováno zejména:

- umístění aktiva (místnost, ve které je aktivum umístěno nebo místnost, kterou má přidělenou vlastník aktiva v případě notebooků).
- informace o software, který je na prostředku instalován (viz sekce software)
- hardware podpora pro některé senzory s prostředky jako je např. čtečka otisků prstů nebo vPro a další dle požadavků předpisu *Bezpečnostní politika PC a notebooků a obdobných zařízení*. Evidována je zda technologie je nebo není přítomna.
- datum posledního softwarového scanu
- datum poslední provedené údržby aktiva

Tiskárny

V systému CMDB jsou evidovány všechny ve společnosti používané tiskárny. Evidovány jsou zejména údaje:

- typ tiskárny (síťová, lokální, lokální sdílená)
- umístění tiskárny
- vlastník tiskárny
- specifikace uživatelů tiskárny
- další informace popisující omezující podmínky použití tiskárny

Pro síťové tiskárny se volí jména ve formátu PRTČísloMístnostiPořadovéČísloZařízeníVMístnosti - např. PRTA0401 (první tiskárna v místnosti A04).

Mobilní telefony, tablety a obdobná zařízení

Všechny zařízení tohoto typu zaměstnanců společnosti, která využívají služeb sítě společnosti musí být evidována v CMDB databázi a to bez ohledu na to zda zařízení je ve vlastnictví společnosti nebo soukromým majetkem zaměstnance.

Účelem evidence je zajištění minimální bezpečné konfigurace zařízení, umožňující bezpečnou práci s informacemi zpracovávanými ve společnosti. Účelem naopak není získání přístupu k soukromým datům jako jsou např. fotky, soukromé e-maily, kontakty, obsah sociálních sítí zaměstnance apod.

Soukromé telefony a tablety, které zaměstnanec používá (i v zaměstnání) aniž by využil služeb služeb sítě společnosti nejsou předmětem evidence. Příklady:

- zaměstnanec se připojuje svým mobilním telefonem k Wi-Fi síti společnosti - zařízení nutno evidovat bez ohledu na to, jakým způsobem síť využívá
- zaměstnanec využívá datové přenosy LTE k zpřístupnění rozhraní informačního systému společnosti pomocí mobilní aplikace - zařízení je nutno evidovat.
- zaměstnanec používá datové přenosy LTE k přístupu ke svým sociálním sítím - zařízení není nutné evidovat.

V CMDB databázi jsou evidovány především:

- IMEI kód telefonu (týká se také tabletů se SIM kartou)
- MAC adresa Wi-Fi adaptéru zařízení
- operační systém zařízení
- vlastník zařízení

Komentář *Ve výše uvedeném textu jsem se pokusil nastínit situaci, kdy se společnost snaží získat kontrolu nad bezpečností všech zařízení používajících služby sítě, i těch, které jsou v soukromém*

²týká se také tabletů s operačním systémem MS Windows, vyjma tabletů s operačním systémem MS Windows RT (evidence těchto tabletů probíhá dle pokynů v sekci věnované tabletům)

vlastnictví zaměstnanců. To samo o sobě může být považováno za kontroverzní záležitost, která se setká s nevolí zaměstnanců. Společnost tak má více méně dvě možnosti - buď použití takových zařízení (v soukromém vlastnictví) zcela zakáže - pak ale pravděpodobně bude muset investovat do firemních mobilních telefonů a tabletů, nebo omezí jejich použití v případě, že nejsou pod kontrolou a nesplňují bezpečnostní požadavky.

Zaměstnanec tak na výběr - buďto strpí určitý zásah do svého soukromí, nebo své zařízení nebude v práci používat.

Všimněte si také, že v textu výše nejsou bezpečnostní požadavky konkrétně specifikovány. Specifikace bezpečnostních požadavků je záležitostí samostatné bezpečnostní politiky těchto zařízení.

Software a informační systémy

Software se pro účely tohoto předpisu rozumí samostatně funkční komponenta instalovatelná na zařízení (hardware) společnosti.

Evidence obsahuje především:

- název software
- evidenční číslo instalačního nosiče (v případě instalace z fyzického média)
- evidenční číslo a umístění hardwarového klíče (pokud je takový klíč vyžadován k provozu software)
- umístění instalačního média v elektronické podobě
- licence k software (podmínky použití software)
- počet licencí software
- vlastník licence
- společnost, u které byla licence zakoupena

Informačním systémem se pro účely tohoto předpisu rozumí softwarové komponenty, které společně zajišťují poskytování služeb systému jeho uživatelům.

- název informačního systému
- seznam samostatně instalovatelných komponent informačního systému
- licence k systému
- vlastník licence
- společnost, u které byla licence zakoupena

V případě, že je software (nebo informační systém) vyvíjen „in house“ (ve vlastní režii) eviduje se také, kdo je za vývoj tohoto software (IS) odpovědný.

Vazby hardware - software

Pro účely řízení bezpečnosti zájmových aktiv IT je nutné evidovat také dodatečné informace popisující způsob nasazení software a informačních systémů ve společnosti. Těmito dodatečnými informacemi jsou především informace o tom kam (na jaký hardware) proběhla instalace a v jaké verzi je software využíván.

Mapování vazeb je prováděno primárně automatizovaně s využitím specializovaných nástrojů pro správu licencí software společnosti. Proces mapování je popsán v předpisu *Správa licencí software*.

5.3 Bezpečnostní politika notebooků

Komentář: pro demonstraci bezpečnostní politiky aktiv jsem vybral notebooky. Jelikož se jedná o přenosná zařízení, měla by se opatření soustředit na prevenci ztráty notebooku a minimalizaci možných následků takové ztráty - především pak minimalizace možnosti zneužití na notebooku uložených informací.

Úvod

Předpis *Bezpečnostní politika notebooků* je závazný pro všechny zaměstnance, kteří pro svou práci využívají přenosné počítače. Cílem předpisu je zajistit vysokou úroveň bezpečnosti zpracovávaných informací ve společnosti u zařízení, která jsou přenosná a jejich bezpečnost tak nelze zajistit pouze ochranou vnějšího perimetru společnosti.

Politika je zpracována dle principů norem řady ISO 27000, zejména pak ISO 27001 a 27002 a *Politiky ISMS* společnosti.

Požadavky na hardware

Notebooky pořizované pro nasazení ve společnosti musí splňovat následující požadavky na konfiguraci:

- podpora biometrie pro autentizaci
- hardware podpora virtualizace (Intel vPro nebo obdobná technologie)
- kensington lock

Komentář Z hlediska konfigurace se předpis zaměřuje pouze na požadavky, které mají vazbu na bezpečnost. Biometrie je jasná, vPro je řešení pro přímou kontrolu hardware (v tomto případě notebooku) virtualizovaným počítačem. Kensington lock umožňuje zamknout notebook na místě a zabránit tak jeho krádeži, např. během výstavy apod.

Tyto požadavky jsou pak používány společně s dalšími technickými požadavky, které ale už nejsou bezpečnostního charakteru jako podklad pro specifikaci parametrů výběrového řízení na pořízení notebooků

Požadavky na software

V případě, že notebook má být provozován na platformě MS Windows je nutné aby se jednalo o verzi podporující šifrování disku pomocí Bitlocker.

Proces počátečního pořízení a konfigurace notebooku

Proces pořízení a počáteční konfigurace je znázorněn na obr. 5.1.

1. specifikace požadavků na notebook

Požadavky specifikované v sekci *Požadavky na hardware* musí být vždy splněny, dle požadavků budoucích uživatelů notebooků ale tyto požadavky mohou být dále rozšířeny, aby nakupovaná zařízení lépe vyhovovala pracovním požadavkům, které na ně budou kladeny.

Specifikaci požadavků kompletuje oddělení IT ve spolupráci se zástupci oddělení, které vznesly požadavek na nákup.

2. vypisání tendru

Tendr vypisuje ředitel IT na základě specifikace požadavků na notebook (viz 1.) a to obvykle 2x do roka (na jaře a na podzim).

Zadání tendru musí být zpřístupněno on-line na stránkách společnosti a musí být obesláni minimálně 3 dodavatelé výpočetní techniky.

Ředitel IT může provést zveřejnění znění zakázky na specializovaných portálech veřejných zakázek k zajištění širší nabídky notebooků pro společnost.

3. vyhodnocení tendru

Hodnotící komise (jmenování probíhá dle procesu X.Y, viz předpis AB123) nejprve hodnotí splnění požadavků specifikovaných v kroku 1. procesu.

V případě, že žádná z nabídek nesplňuje požadavky je celý tendr zrušen a celý proces se vrací do prvního kroku, v rámci kterého se vyhodnocují jednotlivé požadavky a analyzují se důvody jejich nesplnění ze strany možných dodavatelů. V případě potřeby může být specifikace upravena a následně pak vyhlášen nový tendr.

4. vyhodnocení předložených nabídek a výběr notebooku

V případě, že alespoň jedna nabídka splňuje požadavky specifikace, přistoupí hodnotící komise k hodnocení obsahu nabídek a výběru té nejvýhodnější.

5. realizace koupě

Notebooky z vybrané nabídky jsou zakoupeny u vybraného dodavatele. Uzavření smlouvy a administrativní záležitosti okolo nákupu řeší účtárna.

6. dodání notebooků

Vybraný dodavatel dodá vybrané notebooky a to konkrétně na oddělení IT, které notebooky zkontroluje a převezme. V případě zjištění závad nebo problémů jiného typu (např. dodání jiného typu notebooku než byl v nabídce) zajistí řešení problémů přímo s dodavatelem.

7. počáteční instalace a konfigurace notebooku

Pověřený zaměstnanec oddělení IT (administrátor) provede prvotní instalaci požadovaného software

a jeho nastavení dle požadavků jednotlivých útvarů. Z pohledu bezpečnosti musí konfigurace splňovat *Minimální požadavky na konfiguraci softwarových komponent notebooku*.

Po provedení instalace a konfigurace provede administrátor tzv. „zahoření“ notebooku - tedy zátežový test, během kterého by se mohly objevit do té doby skryté závady dodaného zboží. V případě zjištění problémů se notebook reklamuje u dodavatele, v opačném případě se pokračuje dalším krokem procesu.

8. zavedení do evidence

Připravený notebook zavede administrátor do evidence majetku a také databáze CMDB včetně informací o:

- hardware notebooku
- na notebooku používaném software
- uživatelích
- popřípadě další informace dle potřeby

9. předání uživatelům k používání

Připravený, nakonfigurovaný notebook je předán jeho oprávněnému uživateli. Administrátor uživatele poučí o specifikách daného modelu nebo konfigurace, pokud se výrazně liší od předchozího notebooku uživatele nebo o to uživatel požádá. Předání probíhá proti podpisu (viz *Formulář převzetí majetku do užití*).

Administrátor naskenuje podepsaný formulář a zaeviduje jej v databázi CMDB k předanému notebooku. Originál formuláře archivuje sekretariát pracoviště vlastníka.

Minimální požadavky na konfiguraci softwarových komponent notebooku

Notebook musí:

- být nakonfigurován tak, aby vyžadoval přihlášení při zapnutí a také po delší době nečinnosti (vice než 5 minut)
- být nakonfigurován tak, aby minimálně data na disku byla šifrovaná (lépe aby šifrovaný byl celý disk)
- mít nainstalovaný antivirus a osobní firewall a to tak, aby
 - antivirus prováděl automaticky on-access kontrolu souborů, se kterými uživatel pracuje
 - 1x denně prováděl automatizovaně svou aktualizaci a
 - 1x týdně prováděl úplnou kontrolu disku
 - osobní firewall musí být nastaven tak, aby bez zásahu uživatele blokoval nežádoucí síťový provoz
- operační systém musí být nakonfigurován tak, aby umožňoval vzdálenou správu
- operační systém musí být nastaven tak, aby umožnil vzdálené smazání důvěrných dat, v případě že operační systém tuto funkcionalitu nepodporuje, musí být nainstalován dodatečný software pro zajištění této funkčnosti

Změna konfigurace notebooku, bezpečnostní incident

Proces pořízení a počáteční konfigurace je znázorněn na obr. 5.2.

1. změna v aktivu

V aktivu (notebook) došlo ke změnám (např. v důsledku bezpečnostního incidentu) nebo je potřeba provést změny v konfiguraci, např. ve smyslu instalace nového software, nebo změna v nastavení stávajícího software.

Dle charakteru změn se postupuje dále v procesu buď krokem 2. v případě, že uživatel požaduje provedení směn v konfiguraci, nebo krokem 6. v případě, že došlo k bezpečnostnímu incidentu.

2. žádost o změnu

Uživatel zformuluje žádost o změnu a projedná ji s administrátorem. Žádost může být předána ústní formou nebo prostřednictvím helpdesku.

Administrátor vyhodnotí žádost a rozhodne, zda je možno žádosti vyhovět nebo ne. Pokud žádosti není možné vyhovět informuje administrátor uživatele notebooku buďto ústně a nebo písemně (obvykle pokud si to uživatel notebooku vyžádá). Změna v konfiguraci v tomto případě není provedena a proces končí.

V případě, že změnu je možné provést, informuje administrátor uživatele notebooku a proces pokračuje krokem 3.

3. Předání notebooku administrátorovi

Uživatel předá notebook administrátorovi a to buď fyzicky nebo strpěním vzdáleného přístupu administrátora k systému za účelem provedení změn.

4. provedení požadovaných změn v konfiguraci

Administrátor dálkově nebo osobně provede potřebné změny v konfiguraci notebooku a otestuje, zda zařízení funguje správně.

5. Předání notebooku uživateli

Administrátor předá notebook uživateli. V případě že změna konfigurace probíhala dálkově, odhlásí se administrátor z notebooku a upozorní administrátor uživatele o ukončení své práce, popř. informuje uživatele o specifikách spojených s používáním změněného zařízení.

6. Informování o bezpečnostním incidentu

Uživatel informuje administrátora o zaznamenaném bezpečnostním incidentu co možná nejdříve po jeho zjištění. Dle charakteru bezpečnostního incidentu se postupuje dále buďto krokem 7. v případě, že došlo ke ztrátě notebooku (ať už se jednalo skutečně ztrátu nebo krádež zařízení), nebo krokem 9. v případě že bezpečnostní incident je jiného charakteru (počítačový vir, hack notebooku apod.).

7. Vzdálený výmaz notebooku

Po ohlášení ztráty notebooku provede administrátor pokus o vzdálený výmaz notebooku.

8. Dokumentace bezpečnostního incidentu

Poznatky o bezpečnostním incidentu shrne administrátor do zprávy o incidentu. Zaměří se především na to, zda mohly dojít k narušení důvěrnosti uchovávaných údajů. Podle závažnosti incidentu se následně volí další postup dle ustanovení *Politiky ISMS*.

9. Předání notebooku administrátorovi a popis incidentu

Uživatel předá notebook administrátorovi a popíše znaky bezpečnostního incidentu tak, jak je zaznamenal.

10. Analýza incidentu

Administrátor analyzuje notebook s cílem zjistit příčinu a rozsah problémů. Při analýze vytváří podklady pro pozdější zpracování zprávy a bezpečnostním incidentu.

11. Obnova po incidentu

V okamžiku, kdy všechny potřebné informace o bezpečnostním incidentu byly zaznamenány - provede administrátor obnovení funkce notebooku. Dle závažnosti incidentu může být vyžadováno prosté „odvirování“ notebooku, obnova ze zálohy nebo přestavování celého zařízení.

Po dokončení obnovy administrátor předá zařízení zpět jeho běžnému uživateli a v procesu se pokračuje krokem 8.

Vyřazení notebooku

Vyřazením notebooku končí životní cyklus notebooku. Při vyřazování se postupuje dle procesu 5.3.

1. Žádost o vyřazení notebooku

V případě, že uživatel notebooku a jeho vedoucí pracovník rozhodnou, že pro pracovní účely již notebook nepostačuje. Vyplní pracovník žádost o vyřazení notebooku z evidence a vedoucí pracovník ji schválí a předá spolu s notebookem administrátorovi.

Administrátor provede zhodnocení, zda se pro notebook nenajde ve společnosti nějaké využití - pokud ne, postupuje krokem 2. procesu, pokud ano, postupuje krokem 5. procesu.

2. Smazání důvěrných dat

V neupotřebitelném notebooku administrátor odstraní **nevratně** všechna důvěrná data společnosti a smaže také programy, licencované společností.

3. vyřazení notebooku z evidence

Administrátor provede změnu v databázi CMDB - notebook označí za vyřazený a licence software původně instalované na notebooku označí jako dostupné (uvolní licence).

4. Prodej nebo ekologická likvidace zařízení

Vyřazený notebook se dle stavu buďto předá k prodeji nebo likvidaci.

Prodej probíhá podle předpisu *Prodej neupotřebitelného majetku*. Likvidace probíhá podle předpisu *Ekologická likvidace látek, přípravků a výrobků*.

5. Změna vlastníka v evidenci

V případě, že notebook je ve společnosti ještě upotřebitelný, administrátor nabídne notebook dalšími uživateli, jehož potřeby mohou být tímto zařízením lépe pokryty než zařízením stávajícím.

Pokud oslovený pracovník souhlasí, provede administrátor změnu v databázi CMDB (notebook přepíše na osloveného pracovníka).

6. Změn v konfiguraci dle požadavků nového uživatele

Administrátor přizpůsobí konfiguraci notebooku požadavkům nového uživatele. Přizpůsobená konfigurace ale musí stále splňovat minimální požadavky na konfiguraci software notebooku.

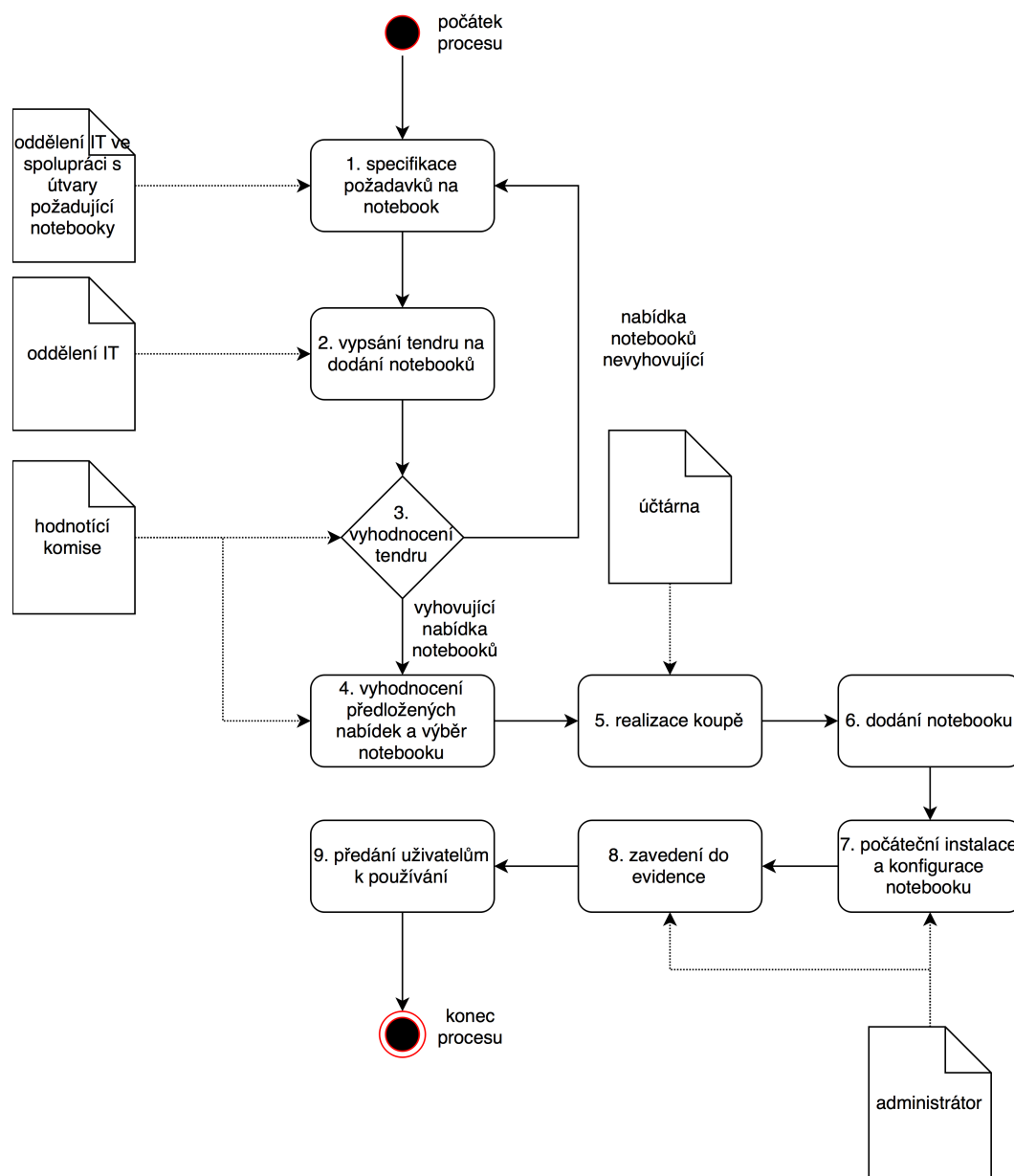
Administrátor provede instalovaný software administrátor registruje v databázi CMDB jako nainstalovaný na daném notebooku.

7. Předání notebooku novému uživateli

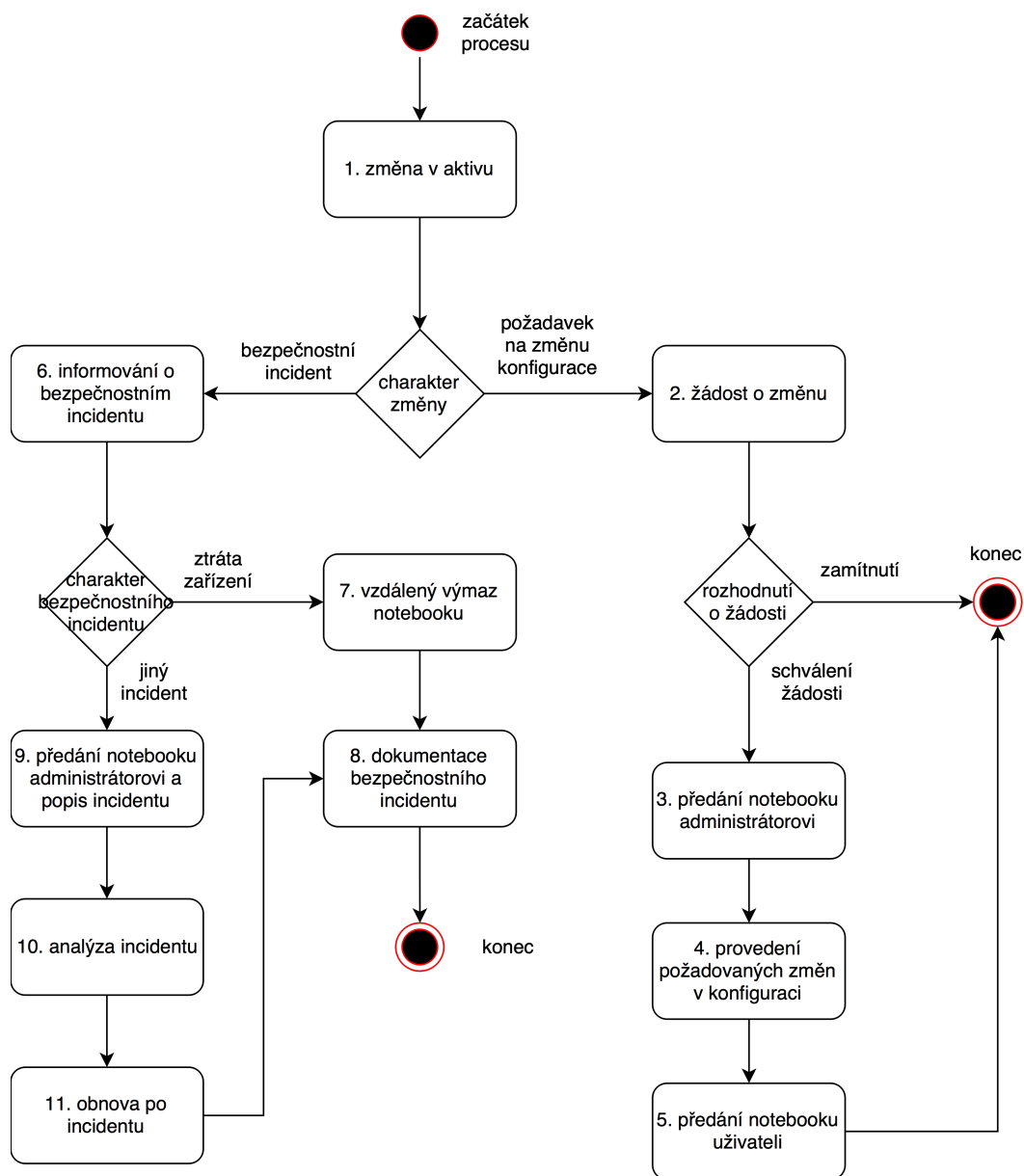
Připravený notebook předá administrátor novému uživateli. Administrátor uživatele poučí o specifikách daného modelu nebo konfigurace, pokud se výrazně liší od předchozího notebooku uživatele nebo o to uživatel požádá. Předání probíhá proti podpisu (viz *Formulář převzetí majetku do užití*).

Závěrečná ustanovení

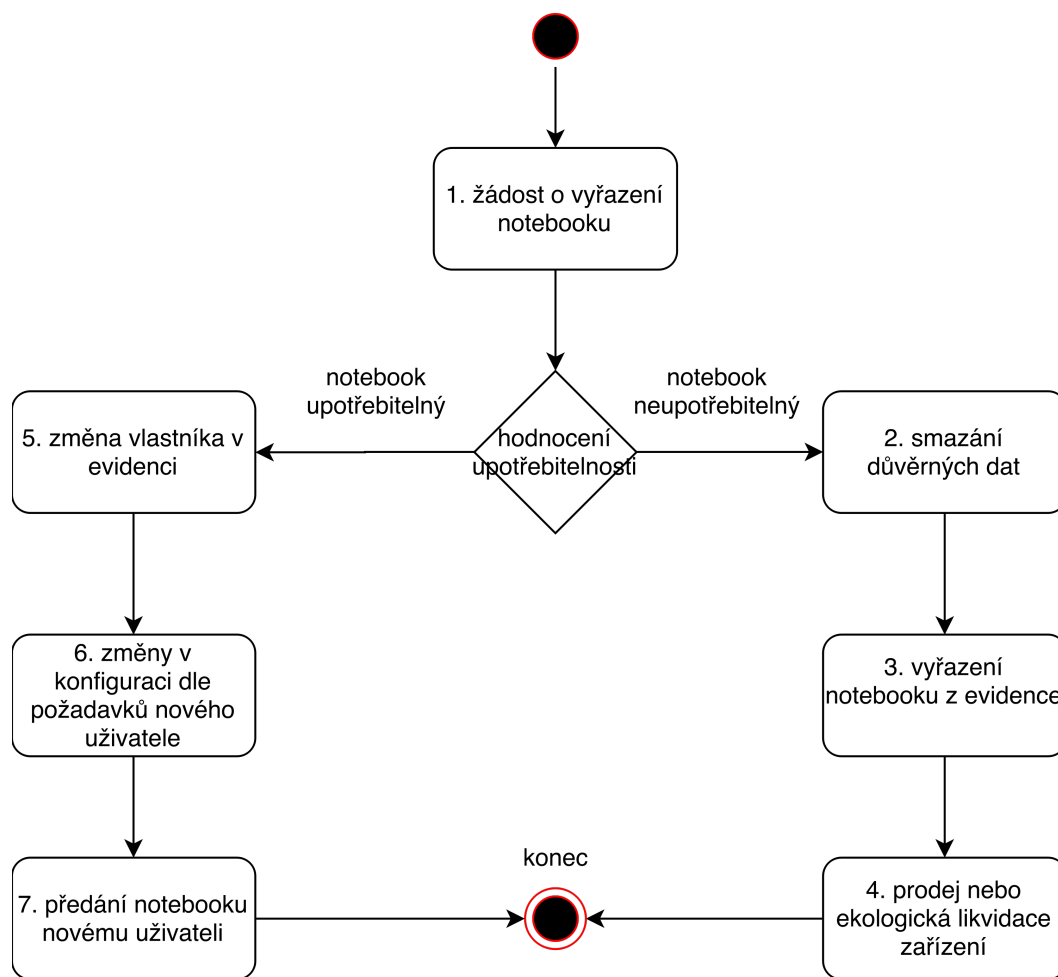
Tento předpis vstupuje v platnost podpisem statutárního zástupce společnosti. Revize předpisu probíhá minimálně jedenkrát ročně. Za provedení revize tohoto předpisu zodpovídá ředitel informační bezpečnosti.



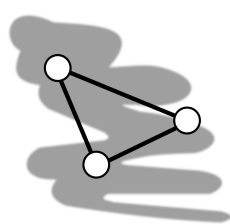
Obrázek 5.1: Proces pořízení a počáteční konfigurace notebooku



Obrázek 5.2: Proces realizace změn konfigurace notebooku a bezpečnostní incident



Obrázek 5.3: Proces vyřazení notebooku z evidence

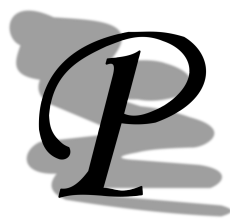


Odlišná forma bezpečnostní politiky

Způsob, jakým je napsána bezpečnostní politika výše, není jediným možným. Pokud se podíváte do skript předmětu Počítačové sítě a ochrana dat [?], naleznete tam jinou formu bezpečnostní politiky. Bezpečnostní politika výše je zaměřena spíše na procesní stránku řízení informační bezpečnosti.

Postupovat lze ale také odlišně a zaměřit se na realizaci opatření vedoucích k dosažení plánované úrovně informační bezpečnosti.

Rozhodnutí, kterou formu použít je tak na autorovi politiky a cíli, který má politika naplnit.



Semestrální projekty

Úspěšně jste došli až na konec části skript věnovaných ISO 27000. Přišel čas, aby jste se pokusili nabyté znalosti aplikovat v praxi zpracováním zadaných semestrálních projektů. Připomínám, že jsou čtyři:

- Politika ISMS
- Management aktiv
- Management rizik (nebo analýza rizik ve smyslu případové studie)
- Bezpečnostní politika zvoleného aktiva

Kapitola 6

COBIT



Průvodce studiem

V této kapitole opustíme svět norem řady ISO 27000 a zaměříme se na obecnější problematiku řízení IT ve společnostech. Jedním z uznávaných standardů pro tento účel je COBIT a mi s tímto rámcem řízení trochu seznámíme.

Po přečtení této kapitoly budete

Znát

- jakým způsobem se řízení IT začleňuje do řízení podniku jako celku
- některé výhody zavedení kontroly nad IT

Umět

- použít některé nástroje řízení, jako je např. model dospělosti procesu

Klíčová slova: IT governance, COBIT, Val IT, RISK IT, doména

Požadavky na vstupní znalosti: nejsou požadovány, zejména pokud jste zvládli alespoň základy ISO 27000 z předchozích kapitol.



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 3 hod.

6.1 Stručná historie norem COBIT

Control Objectives for Information and Related Technologies (COBIT) je zkratka pro kontrolní cíle pro informační a související technologie. Jedná se o rámec publikující postupy good-practice pro získání kontroly nad provozem a investicemi do IT společností.

Normy vyvinula mezinárodní asociace **Information Systems Audit and Control Association (ISACA)**, která se zaměřuje na problematiku IT governance. ISACA vyvinula např. také normy zabývající se problematikou bezpečnosti průmyslových řídicích systémů (**Industrial Control System (ICS)**) a další.

První verze normy COBIT vyšla v roce 1996. Zaměřovala se přitom na problematiku finančního auditu IT projektů, pro které navrhovala sady měřitelných, kontrolovatelných cílů, které mohly sloužit jako podklad pro řízení. Otázka financování a jeho efektivity. V minulosti (ještě relativně nedávno) se předpokládalo, že investice do IT firmám automaticky přinášejí konkurenční výhodu a tedy, že se automaticky vyplátí.

Praxe ale ukazuje, že investice do IT sice může přinést pozitivní změny ve fungování organizací, ale z žádném případě se tak nestane automaticky. Investice do IT tak musí vhodně naplánována a její realizace a následný rutinní provoz zavedených systémů pak musí být manažersky dobře zvládnutý.

Tuto situaci dobře popsal Nicholas G. Carr v provokativním článku *IT doesn't matter* [35], ve kterém popisuje relativně malé přínosy pokračujících investic a také různé aspekty provozu IT systémů, vytvářejících náklady včetně např. spotřeby elektriny apod.

Finanční audit je tedy pouze malou částí problému. ISACA na situaci reagovala rozšířením rámce (1998) v COBIT 2 doplněním cílů pro další oblasti a v roce 2000 pak v COBIT 3 přidala i průvodce pro management.

Ve verzi 4 (2005) a 4.1 pak zohlednila některé procesy v IT zodpovědné za vytváření hodnot ve firmě normou Val IT a také otázky managementu rizik normou Risk IT a také další. Tyto normy jsou ale samostatné - nikoliv v integrované podobě.

Verze 5 pak obsah těchto norem integruje do rámce COBIT. Z norem COBIT se tak stává ucelený rámec pro řízení prakticky všech aspektů IT.

COBIT 2019 je evolucí COBIT 5 zaměřenou na integraci s případnými dalšími systémy řízení jako je ITIL, TOGAF, ale také do oblasti řízení vývoje (DevOps).



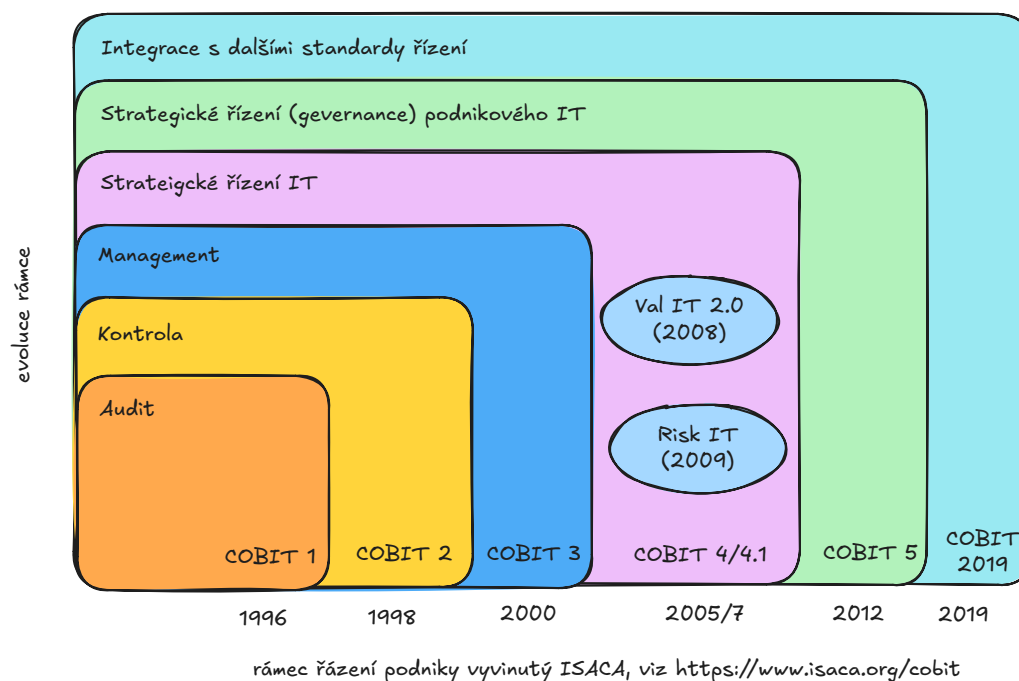
Komu je COBIT určen

COBIT je určen především auditorům, pro management IT v organizacích, řízení bezpečnosti a rizika IT. Filozoficky COBIT funguje jinak než ISO 27000. Tam, kde ISO 27000 se zaměřuje spíše na celkové procesy fungování IT v organizacích, tam se COBIT zaměřuje primárně na problematiku řízení (managementu).

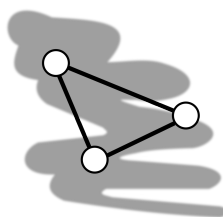
COBIT a ISO 27000 jsou proto určeny jiným skupinám uživatelům a lze je považovat za vzájemně komplementární (doplňující se).

Zároveň COBIT pokrývá širší problematiku než ISO 27000, které se zaměřuje pouze na problematiku informační bezpečnosti.

Představu o vývoji COBIT si lze udělat také z obr. 6.1.



Obrázek 6.1: Evoluce COBIT (adaptováno z Garsoux [42])



Efektivita investic ...

Otázka hodnocení efektivity investic není omezena pouze na oblast IT. Stejnou otázku si můžeme položit např. v oblasti investic do bezpečnosti jako takové. Zde lze investovat prakticky neomezené množství finančních prostředků, podobně jako do IT. Otázka ale je jaký přínos taková investice má.

Obecně pro investice platí, že s každou další investicí do určité oblasti, je dosaženo stále menšího přínosu. Představit si to lze tak, že prvotní investice pokryje tzv. „nízko visící ovoce“ - přínos je maximální, další investice se už zaměřují na stále užší („menší“) problémy a jejich přínos je tak logicky menší.

6.2 Principy COBIT

COBIT je založen na pěti základních principech:

1. Plnění potřeb stakeholderů
2. Pokrytí všech částí podniku
3. Používá je jeden integrovaný rámec řízení
4. Důraz na holistický přístup
5. Oddělení governance a managementu

Tyto principy spadají do oblasti **Governance of Enterprise IT (GEIT)**

Pojem *stakeholder* se extenzivně používá v managementu. Do češtiny se obvykle nepřekládá. Používá se pro označení osob a institucí, které s organizací mají něco do činění - mají na určitém způsobu fungování firmy zájem. Mezi stakeholdry můžeme řadit majitele (např. akcionáře) firmy, zaměstnance, management organizace, odběratele, dodavatele, stát a další dle činnosti organizace.

Zájmy stakeholderů jsou různé - majitelé obchodních společností preferují zvyšování ceny společnosti a zisk, stát preferuje soulad fungování společnosti s platnou legislativou. Zaměstnanci preferují maximální výši platu a jiné benefity související s výkonem práce. Zájmy stakeholderů tak mohou být a často také jsou vzájemně v rozporu, ve smyslu, že očekávání všech stakeholderů nelze zcela uspokojit.

Obecně lze potřeby stakeholderů shrnout do věty, že organizace musí vytvářet hodnoty. Co je to hodnota se ale z pohledu jednotlivých stakeholderů liší.

Vytváření hodnot je dosaženo získáním a udržením rovnováhy mezi realizací benefitů (např. zisk, zvýšení hodnoty společnosti, intelektuální vlastnictví apod.), optimalizací zdrojů a optimalizací rizik. Dohadování a vyvažování jednotlivých zájmů se realizuje pomocí governance a managementu kaskádou cílů COBIT:

1. motivace stakeholderů (stakeholder drivers)
2. potřeby stakeholderů (stakeholder needs)
3. cíle organizace (enterprise goals)
4. cíle související s IT (IT related goals)
5. komponenty (informační toky, kompetence, procesy, politiky, organizační struktury)

Kaskáda postupuje směrem dolů ke stále konkrétnějším cílům, které je možno měřit. Poslední z nich nemá v češtině úplně přesný ekvivalent a zároveň je také poměrně obtížně představitelný, z pohledu interpretace. Komponenty představují faktory, které umožňují dosažení cílů.

COBIT definuje sedm faktorů dosažení cílů:

1. Principy, politiky a rámce
2. procesy
3. organizační struktury
4. podniková kultura, etika a chování
5. informace
6. služby, infrastruktura a aplikace
7. lidé, schopnosti a kompetence

Tyto faktory lze také rozčlenit jinak na *kontextové* jako jsou podmínky v organizaci, hrozby, atd., které organizace nemá možnost přímo ovlivnit a *strategické faktory*, které přímo vyplývají ze strategických rozhodnutí organizace a různých priorit přiřazovaných různým aspektům podnikového IT.

Taktické faktory se soustředí na rozhodnutí okolo používaných technologií, metod a rozhodnutí o tom co bude řešeno interně a co bude outsorcováno, tedy nakupováno od externího dodavatele.

Všechny výše uvedené faktory přispívají k dosažení cílů. Z pohledu managementu k nim lze definovat měřitelné cíle a ty použít k řízení - měřit splnění cílů a přijímat korekční opatření. Stanovení cílů a jejich prokazatelné plnění je typický přístup, který je používán v managementu. To znovu prokazuje, že COBIT skutečně je nástrojem pro management.

Z pohledu řízení je také zajímavé důsledné oddělení problematiky governance a managementu. Oba pojmy by do češtiny bylo možné přeložit jako řízení, ale v COBIT znamenají něco jiného a proto použití jednotného pojmu „řízení“ v tomto kontextu není přípustné.

V COBIT governance a management mají jiný účel, pojí se s ním jiné odpovědnosti, jiné aktivity a také jiné podpůrné organizační struktury. Governance hodnotí, řídí a monitoruje. Management pak plánuje, buduje, provozuje a monitoruje.

Zjednodušeně řečeno tedy managementem rozumíme opakované činnosti spojené s „běžným“, každodenním řízením. Zatímco governance představuje spíše strategické řízení.

Konkrétněji v rámci governance se hodnotí, zda potřeby stakeholderů jsou v souladu s cíli, které organizace musí dosáhnout. Řízení probíhá pomocí nastavení priorit a procesu rozhodování. Monitorování probíhá proti výkonu společnosti a souladu se stanovenými cíli.

Managementem zajišťuje, že všechny potřebné aktivity jsou realizovány a monitorovány a jsou také v souladu se směrem nastoleným v rámci governance.

Za účelem dosažení výše uvedených cílů nasazuje COBIT řadu manažerských technik a nástrojů, se kterými se postupně seznámíme.

6.3 Nástroje podpory řízení

6.3.1 Balance Score Cards

Nástroj **Balance Score Cards (BSC)** je česky označován systém vyvážených ukazatelů výkonnosti podniku. BSC vyvinuli a publikovali Kaplan a Norton [48] formalizující měření a vyhodnocování výkonnosti jednotlivých částí podniku. Myšlenka měření výkonnosti a její hodnocení není ale nová a v managementu se používá dlouhodobě. BSC ale specifikuje přesně jakým způsobem má měření a následné hodnocení probíhat.

Svoji schopností provádět hodnocení pro organizaci jako celek a výsledky dávat do souvislosti s strategií organizace řadíme BSC mezi nástroje tzv. *strategického řízení*.

BSC poskytuje čtyři perspektivy:

1. finance a finanční ukazatele,
2. interní obchodní procesy,
3. zákazníci,
4. učení a růst.

Financemi se v tomto případě rozumí běžné účetní ukazatele. Perspektiva *interních obchodních procesů* umožňuje hodnotit, jakým způsobem a v jaké kvalitě (např. ve smyslu rychlosti) jsou realizovány procesy ve společnosti.

Perspektiva *zákazníků* je taktéž tradiční. Zákazník odebrá zboží popř. služby generované organizací. Jeho spokojenost tak nepřímo ovlivňuje finanční ukazatele, image organizace apod.

Přidání perspektivy *učení a růstu* bylo ve své době považováno za novátorský počín. Poučení se z vlastních chyb je ale logickým krokem, který je v současnosti používán i při řízení bezpečnosti. Do této oblasti jsou zařazovány např. systémy vzdělávání zaměstnanců, apod.

COBIT implementuje BSC formou IT informační dimenze a souvisejících technologických cílů, kterou lze následně mapovat podnikové cíle (ve struktuře BSC) jako takové.

- finance
 1. soulad strategie IT a strategie podniku
 2. soulad IT a podpora souladu fungování podniku s požadavky vzešlých právních předpisů a norem
 3. závazek výkonného vedení při rozhodování o IT
 4. řízení rizika podnikání související s IT
 5. realizované výhody z investic do IT a portfolia služeb
 6. transparentnost IT nákladů, přínosů a rizik

- zákazník
 7. poskytování IT služeb dle požadavků podniku
 8. adekvátní nasazení aplikací, informací a technologií
- vnitřní
 9. agilita IT
 10. bezpečnost informací, infrastruktury jejich zpracování a aplikací
 11. optimalizace IT aktiv, zdrojů a schopností
 12. zavedení a podpora podnikových procesů integrací aplikací a technologií
 13. dodávky IT služeb včas, v souladu s rozpočtem a při splnění požadavků na kvalitu
 14. dostupnost spolehlivých a užitečných informací pro rozhodování
 15. soulad IT s vnitřními předpisy
- učení a růst
 16. kompetentní a motivovaní zaměstnanci
 17. znalosti a iniciativy pro inovace

Mapování lze provést také cíle governance v oblastech realizace přínosů, optimalizace rizika a optimalizace zdrojů. V rámci mapování jsou identifikovány primární a sekundární vazby, které pak následně umožňují lépe pochopit jakým způsobem IT přispívá k dosahování cílů organizace.

COBIT obsahuje přednastavené mapování, s tím, že implementující organizace vazby upraví dle vlastních potřeb, tak aby byly pokryty všechny IT aktivity organizace.

Příklad mapování BSC IT na podnikové cíle je na obr. 6.2.

			<i>Enterprise Goal</i>			
			Stakeholder Value of Business investments	Customer - oriented service culture	Optimisation of business process functionality	Skilled and motivated people
			1	6	11	16
<i>IT-Related Goal</i>			<i>Financial</i>	<i>Customer</i>	<i>Internal</i>	<i>Learning and Growth</i>
<i>Financial</i>	1	Alignment of IT and business strategy	P	P	P	S
<i>Customer</i>	7	Delivery of IT services in line with business requirements	P	P	P	S
<i>Internal</i>	9	IT agility	S	S	P	S
<i>Learning and Growth</i>	16	Competent and motivated business and IT personnel	S	S		P

Obrázek 6.2: Mapování BSC IT cílů na podnikové cíle (převzato z Garsoux [42])

Mapování se provádí také na jednotlivé procesy COBIT. Organizaci procesů COBIT ale probereme v samostatné podkapitole.

6.3.2 Domény a procesy COBIT

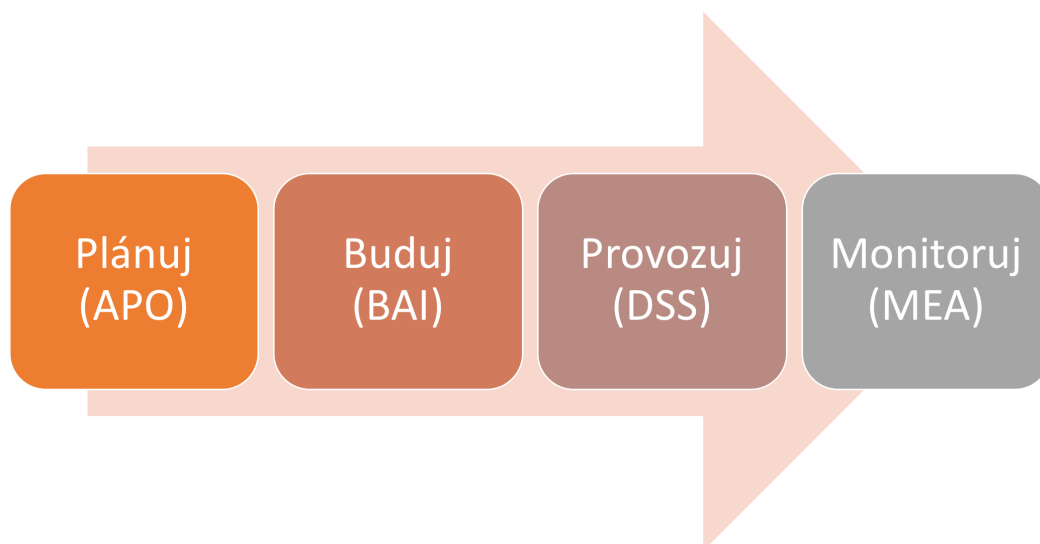
Jádro COBIT je realizováno okolo procesů zajišťujících IT služby v organizaci. Procesy jsou organizovány do čtyř domén:

1. APO - dej do souladu, plánuj a organizuj (align, plan and organize)
2. BAI - vybuduj, získej a implementuj (build, acquire and implement)
3. DSS - dodej, udržuj a podporuj (deliver, service and support)
4. MEA - monitoruj, hodnot a posuzuj (monitor, evaluate and assess)

V výše uvedeným doménám, které jsou přiřazovány k managementu pak COBIT používá ještě doménu EDM - hodnot, říd a monitoru (evaluate, direct and monitor), která pokrývá governance.

Domény jsou pojmenovány podle činností, které jsou v rámci nich vykonávány. Pojmenování tvoří tři slovesa, jejichž počáteční písmena v angličtině tvoří zkratku domény. Zkratky jsou používány pro označování jednotlivých procesů. Např. APO01 je proces Řízení rámce řízení IT (první proces domény APO).

Jednotlivé domény na sebe navazují, viz obr. 6.3.



Obrázek 6.3: Návaznost domén COBIT

Tedy na základě potřeb organizace používající COBIT nejprve plánujeme způsob, jak tyto potřeby pokrýt v požadovaném rozsahu a kvalitě, následně toto řešení postupně budujeme. Vybudované řešení dlouhodobě provozujeme k prospěchu organizace a provádíme monitoring provozovaných IT služeb, abychom odhalili problémy, nedostatky a nové možnosti pro další rozvoj IT.

Aby nad výše uvedeným postupem bylo možné získat kontrolu pracuje COBIT s 37 procesy, které zařazuje do jednotlivých domén. Procesy nejsou rozděleny rovnoměrně (EDM - 5 procesů, APO - 13 procesů, BAI - 10 procesů, DSS - 6 procesů a MEA - 3 procesy).

Jednotlivé procesy jsou vztahovány k 17-ti BSC IT cílům a hodnoceny. Hodnocení probíhá pomocí metrik, které COBIT pro jednotlivé cíle a procesy navrhuje. Výsledkem hodnocení je:

- posouzení stav procesu (procentní vyjádření vyspělosti procesu)
- hodnocení stavu splnění IT cílů v taxonomii BSC IT cílů
- procentní vyjádření vyspělosti domény

COBIT pro některé segmenty (např. školství, státní správa apod.) poskytuje pro domény doporučenou úroveň vyspělosti, vůči které lze porovnávat současný stav řešení. Lze také formulovat plán na cílový stav. Srovnání skutečného stavu a plánu lze znázornit např. jako na obr. 6.4.

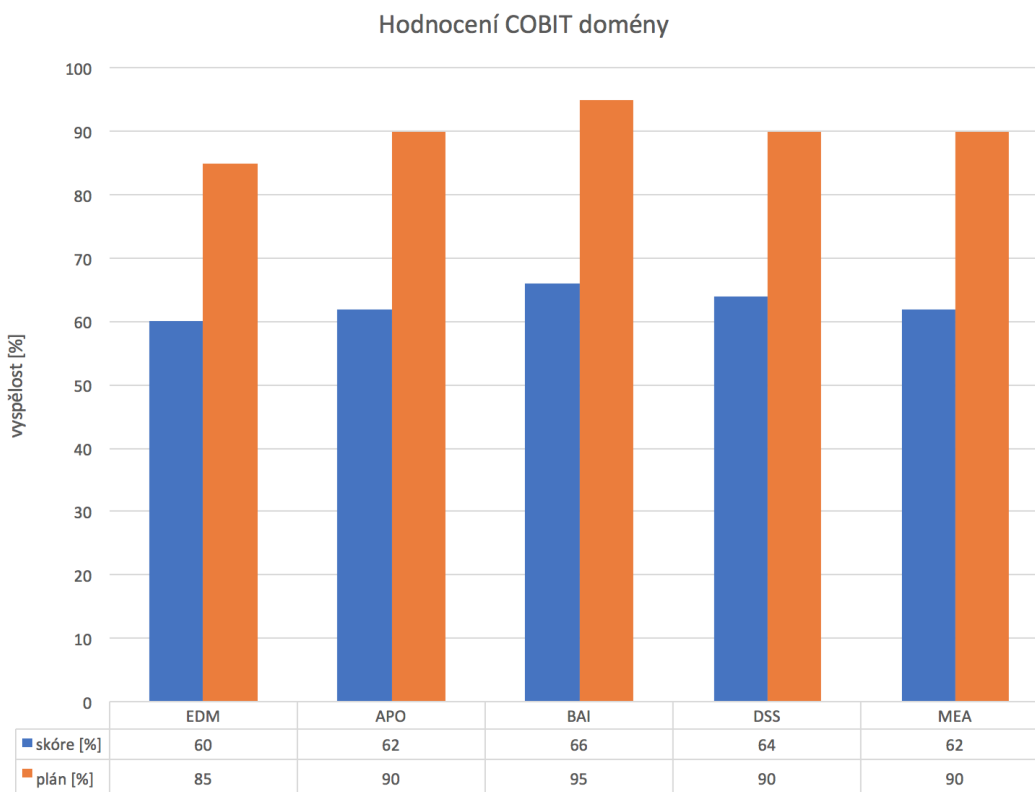
Vzhledem k tomu, že hodnocení domén se počítá jako aritmetický průměr hodnocení jednotlivých procesů přináležejících k doméně. Lze tedy zpětně relativně jednoduše identifikovat ty procesy, které nejvíce pozitivně přispívají k hodnocení i ty, které organizace nejhůře zvládá a k zlepšení celkové hodnocení je má největší smysl optimalizovat.

6.3.3 Matice RACI

Matice RACI, někdy označovaná také jako model RACI, tabulka lineární odpovědnosti (**Linear Responsibility Chart (LRC)**). V češtině se také používá název matice odpovědnosti. Jedná se o nástroj, který umožňuje k jednotlivým rolím, úlohám, popř. procesům popsat způsob participace zainteresovaných osob.

Právě úroveň participace je charakterizována jednotlivými písmeny:

- R (responsible) - odpovědný osoba/osoby, které na úkol/procesu pracují
- A (accountable) - osoba/osoby, které jsou zodpovědné za úkol/proces jako celek



Obrázek 6.4: Hodnocení domény COBIT (adaptováno z [46])

**Marginální přínos zlepšení monitorovaných procesů**

Při realizaci nápravných a zlepšujících opatření v organizačních procesech je potřeba brát v úvahu, že aktivity na počátku zkvalitňování procesů jsou nejjednodušeji realizovatelné a také nejméně finančně náročné. S každou další úrovní se ale finanční a často také časové nároky realizace opatření výrazně zvyšují, opatření samotné pak přináší stále menší užitek (na cestě vzhůru zvládnutím procesu).

Z tohoto důvodu je při zlepšování potřeba soustředit se na „slabá místa“, popř. tam kde existuje největší rozdíl mezi plánovaným a skutečným stavem.

- C (consulted) - osoba nebo osoby, které mohou přispět k realizaci úkolu nebo procesu konzultací
- I (informed) - osoba nebo osoby informované o výsledku nebo průběhu realizace úkolu nebo procesu

Zastavme se u odpovědnosti R vs A. Rozdíl je zásadní, byť v češtině responsible i accountable překládáme stejným slovem. R popisuje odpovědnost za vykonávání běžné práce - tedy odvedeme práci a za práci, kterou jsme odvedli si stojíme - jsme za ni odpovědní.

A - odpovídá spíše manažerské odpovědnosti. Accountable osoba tak mohla, ale se nemusela nutně podílet na , ale za správnost úkolu nebo procesu jako celku odpovídá.

Konzultace (C) jsou obvykle realizovány pro složitější úlohy nebo procesy, jejichž úspěšné dokončení závisí na odborných znalostech které nejsou v organizaci dostupné. Organizace si za tímto účelem najímá konzultanta. Konzultanté nejsou považováni za kmenové pracovníky organizace a nenesou tak přímou odpovědnost za plnění úkolů.

Informovaný (I) jsou osoby, které jsou informovány o výsledku realizace úkolu nebo procesu. Důvod pro informování může být dvojitý - buď jako součást kontrolního procesu řízení vyšší úrovně (A nad A), nebo jako součást spuštění navázaného procesu nebo procesů.

Příklad RACI matice pro oblast projektového řízení je v tab. 6.1.

V COBIT se RACI matice používá primárně pro deskripci procesů.

Tabulka 6.1: Příklad RACI matice projektového řízení (adptováno z [25])

kód	popis	sponzor projektu	business analytik	projektový manager	architekt technologií	vývojář aplikací
A	řízení prodeje					
B	hodnocení práce					
C	zahájit projekt					
C04	security governance	C	C	A	I	I
C10	funkční požadavky	A	R	I	C	I
C11	kritéria přijatelnosti	A	R	I	C	I
D	návrh řešení					

6.3.4 Model dospělosti

Zajímavou možností, kterou lze využít pro posuzování mezer v systému řízení IT je nasazení tzv. modelu dospělosti (maturity model).

Modelem dospělosti rozumíme hodnocení vyspělosti řízených procesů. Tento model byl poprvé nasazen v COBIT 4 a v COBIT 5 pak doznal značných změn. Vzhledem k tomu, že oba přístupy mají širší aplikaci, budou v této kapitole popsány oba.

COBIT 4 využívá šestistupňový model dospělosti, od úrovně 0 - neexistující procesy po úroveň 5 - optimalizované procesy.

- Úroveň 0 - *neexistující* - absence znatelných procesů
- Úroveň 1 - *počáteční* - procesy jsou vyvíjeny ad hoc - tedy případ od případu
- Úroveň 2 - *opakovatelný* - procesy jsou natolik specifikované, že je možné používat opakovaně, různými lidmi v podobných situacích. Tato úroveň nepředpokládá existenci formálního školení o procesech.
- Úroveň 3 - *definovaná* - procesy jsou formálně specifikované (dokumentované). Procesy jsou založené na předchozí praxi, ale bez ručení za tyto procesy.
- Úroveň 4 - *řízená* - proces je stále monitorován a je měřena shoda s nastavenou úrovní procesu. Procesy jsou neustále zlepšovány. Některé aspekty procesů jsou automatizovány.
- Úroveň 5 - *optimalizován* - proces je optimalizován na úroveň nejlepších ověřených postupů.

Existuje více možností, jak provést hodnocení. Hodnocení lze provést třeba na úrovni domén COBIT. Vizualizace management domén APO - 1, BAI - 2, DSS - 3, MEA - 2 by mohla vypadat podobně jako na obr. 6.5.

Papřskový graf umožňuje velmi jednoduše identifikovat domény, ve kterých organizace procesů zaostává a kde tedy investice do získání kontroly má největší smysl. Papřskové grafy lze vytvářet také samostatně pro jednotlivé domény a získat tak podrobnější informaci k tomu, kde je problém.

Alternativně lze provést porovnání vůči okolí. Na obr. 6.6 je znázorněno porovnání současného stavu procesu s cíli organizace, konkurencí a doporučením.

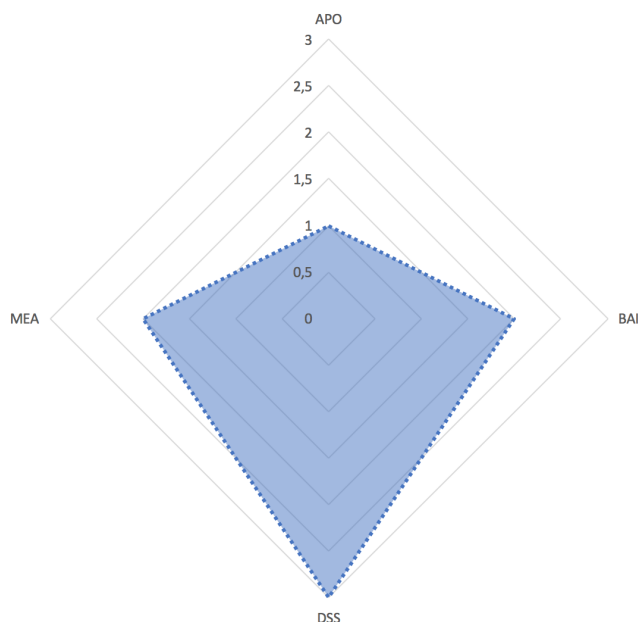
Porovnání tohoto typu ale vyžaduje dostupnost informací o dospělosti procesů mimo organizaci, existenci doporučení relevantních pro oblast ve které organizace působí apod., které mohou, ale také nemusí být dostupné.

COBIT 5 z výše uvedeného modelu dospělosti přešel k modelu podle ISO 15504 [12]. ISO 15504 je primárně určeno pro hodnocení procesů v oblasti IT, ale uvedené postupy lze aplikovat univerzálně. Ve skutečnosti ISO 15504 bylo přeznačeno a rozvinuto do podoby normy ISO 33001 [13]. ISO 15504 je tak zmiňováno v tomto textu pouze z toho důvodu, že o něm hovoří COBIT.

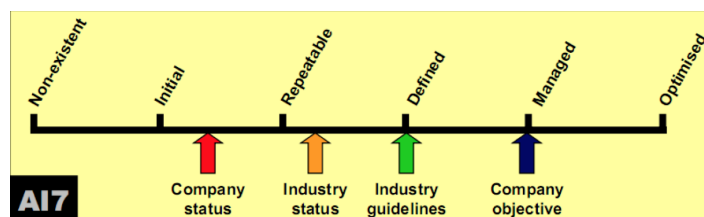
Podobně jako v předchozím případě jsou procesy zařazovány do jedné z šesti úrovní. Tyto úrovně se ale v obou případech neshodují.

- Úroveň 0 - *nekompletní procesy* - proces není implementován nebo není dosahováno jeho účelu
- Úroveň 1 - *prováděné procesy* - implementované procesy dosahují stanovených cílů
- Úroveň 2 - *řízené procesy* - procesy jsou implementovány řízeným způsobem (naplánovány, monitorovány a upravovány) a jejich nastaveny a kontrolovány
- Úroveň 3 - *zavedený proces* - proces je přesně definován, a zaveden tak aby byl schopen dosahovat stanovené cíle
- Úroveň 4 - *predikovatelný proces* - funguje v definovaných limitech umožňujících dosahování procesních cílů

PAPRSKOVÝ GRAF DOSPĚLOSTI DOMÉN COBIT



Obrázek 6.5: Vizualizace modelu dospělosti paprskovým grafem



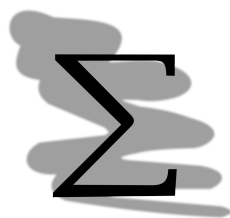
Obrázek 6.6: Porovnání stavu vyspělosti procesu s konkurencí, doporučeními a cíli společnosti.

- Úroveň 5 - *optimalizace procesu* - proces je vylepšen tak, aby byl schopen dosáhnout relevantní současné a budoucí obchodní cíle

Pokud srovnáme model dospělosti COBIT 4 a stupnici používanou ISO 33001 zjistíme, že úrovně jsou pouze podobné, viz tab. 6.2. Rozdíly jsou především na nižších úrovních modelu

Tabulka 6.2: Srovnání modelu dospělosti v COBIT 4 a 5 (podle ISO 33001)

COBIT 4	ISO 33001
5. optimalizovaný	5. optimalizace procesu
4. řízený a měřitelný	4. predikovatelný proces
3. definovaný proces	3. zavedený proces
	2. řízený proces
2. opakovatelný	1. prováděný proces
1. počáteční	
0. neexistující	0. neúplný proces



Shrnutí

COBIT je sada norem určených pro získání kontroly nad systémy IT a jejich optimální řízení. Norma obsahuje domény, v nich pak relevantní procesy, pro které stanovuje měřitelné cíle. Formou zpracování a nástroji, které poskytuje svým uživatelům je tak norma určena vedoucím pracovníkům oddělení IT. Odlišnost zaměření umožňuje také dosahování synergických účinků při implementaci dalších systémů řízení např. na bázi ISO 27000 nebo ITIL.

Z nástrojů, které COBIT používá je možno zmínit především:

- **BSC**
- model odpovědnosti na bázi matice RACI
- model dospělosti

BSC umožňuje měřit výkonnost v doménách COBIT.

RACI matice umožňuje k jednotlivým procesům ve společnosti přiřazovat různé role nebo osoby a specifikovat jako úroveň odpovědnosti v rámci procesu mají.

Model dospělosti slouží pro porovnání procesů ve společnosti z hlediska jejich vyspělosti. Umožňuje tak rychle identifikovat procesy, které ve srovnání s ostatními zaostávají a kde investice do zlepšení má potenciál být nejefektivnější.



Kontrolní otázky: 6 COBIT

1. Vysvětlíte rozdíl mezi management a governance.
2. Vysvětlíte rozdíl mezi odpovědnosti - responsible vs accountable.
3. Co jsou BSC a jak se používají?
4. Co je model dospělosti a jaké informace může poskytnout?
5. Co je RACI matice a k čemu se v rámci COBIT používá?

Kapitola 7

ITIL



Průvodce studiem

Naši exkurzi po rámcích podpory řízení IT zakončíme krátkým rozebráním knihovny ITIL.

Po přečtení této kapitoly budete

Znát

- co je ITIL a jaké výhody (a nevýhody) má jeho nasazení v praxi

klíčová slova: ITIL, IT governance, služba, SLA

nároky na předchozí znalosti: nejsou, k pochopení ale může pozitivně přispět základní znalost managementu.



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 3 hod.

ITIL je zkratka pro IT Infrastructure Library. Tento standard, podobně jako COBIT a významné části ISO 27000 vznikl ve Velké Británii a postupem času se pak rozšířil do zbytku světa. ITIL na rozdíl od ISO 27000 nemá charakter normy ale spíše doporučení.

Z tohoto pohledu tak připomíná COBIT, který taktéž není normou v pravém slova smyslu, byť zaměření COBIT a ITIL je odlišné.

ITIL je procesně orientovaný rámec managementu IT, který umožňuje/motivuje implementátory tohoto rámce zavádět nejlepší, dobře dokumentované postupy z praxe a dosáhnout tak na vyšší efektivitu s minimem vynaloženého úsilí a investic.

Z tohoto zaměření je právě odvozen název ITIL - konkrétně *L* - library, tedy knihovna nejlepších postupů. Implementací nejlepších postupů do řízení IT v organizaci je možno poměrně rychle posunout efektivitu provozu a řízení IT na novou úroveň, aniž by bylo nutné vyvíjet postupy a procesy „od píky“.

Použitím ITIL (nebo obdobných rámců) tak může organizace minimalizovat rizika spojená s vlastním vývojem procesů a postupů na míru, především pak riziko, že implementované postupy nebudou účinné.

Z pohledu zaměření a formy rámce lze konstatovat, že ITIL je napsán spíše konkrétně a poskytuje vysoce relevantní poznatky pro provoz IT, tím se také liší jak od ISO 27000 tak COBIT, které jsou obecnějšího charakteru.

Připomeňme si, že ISO 27000 je obecný rámec určený pro řízení informační bezpečnosti v organizaci. Pro zavedení tak organizace musí vyvinout procesy, politiky apod. COBIT proti tomu poskytuje primárně vodítka pro efektivní řízení IT v organizaci. Poskytuje tak především metriky a postupy pro

jejich kontrolu s cílem získat kontrolu nad investicemi do IT a jejich užitím v organizaci a to jak po stránce finanční, tak po stránce např. bezpečnosti.

COBIT je tak mnohem více konkrétní i relevantní z hlediska IT než obecné ISO 27000, zároveň je však mnohem méně konkrétní (a IT relevantní) než ITIL.

Ačkoliv mezi výše uvedenými rámci existují jisté přesahy, je očividné, že ISO 27000, COBIT i ITIL jsou výrazně odlišně zaměřeny a řeší tak odlišné části problému řízení IT a bezpečnosti obecně. To je také důvod, proč řada organizací implementuje několik rámců zároveň, aby dosáhla co možná největšího pokrytí problémů.

Takovému přístupu pak nahrávají také rámce samotné tím, že často obsahují přesně specifikované návaznosti, mapování funkcí na další rámce/systémy řízení.

7.1 Stručná historie ITIL

Počátek vývoje ITIL lze vysledovat do roku 1980, kdy jsou pro státní správu Velké Británie připravována doporučení pro nasazování a provoz IT. Britové pro taková doporučení zřídila **Central Computer and Telecommunication Agency (CCTA)**. Správa a vývoj rámce pak zůstal v různých formách po patronaci vlády Velké Británie.

Původní sada doporučení byla v roce 1989 formalizována do první verze ITIL, která obsahovala přibližně 30 publikací. Druhá verze standardu vyšla v roce 2000, kdy došlo ke konsolidaci do osmi publikací, ve verzi 3 pak konsolidace do pěti základních knih.

Verze 3 je používána dosud, byť v lehce aktualizované verzi (z roku 2011). V současnosti je vlastníkem společnost AXELOS (join venture společností CAPITA a Úřadu vlády Velké Británie) [32].

Jádro ITIL tedy tvoří tzv. *klíčové publikace*, které jsou doplňovány tzv. *doplňkovými publikacemi* zaměřenými na specifikace vybraných odvětví, popř. návaznosti na další rámce. ITIL poskytuje také některé aktuální informace na webu, tak aby zajistil maximální aktuálnost poskytovaných informací a zároveň nemusel měnit, popř. znovu vydávat zejména klíčové publikace.

Klíčové publikace jsou následující:

- Strategie služeb (Service Strategy)
- Návrh služeb (Service Design)
- Přechod služeb (Service Transition)
- Provoz služeb (Service Operation)
- Průběžné zlepšování služeb (Continual Service Improvement)

Všimněte si, že v názvu každé klíčové publikace je **služba**. To je nové pro verzi 3 standardu, která byla trochu jinak organizována - byť samotný obsah rámce jako celku zůstal v zásadě zachován.

Dle ITIL je **služba** [32]: *prostředek dodávání hodnoty zákazníkovi (odběrateli služby)*. V kontextu ITIL předpokládáme, že služba bude zahrnovat nějakou IT komponentu. Je přitom irelevantní, zdali odběratel služby je interní (odběratelem je tedy organizace samotná), nebo externí. Vždy platí, že odběratel odebírá službu jako takovou - tedy výsledek procesů IT, ale sám se přímo nepodílí na nákladech a také rizicích, která jsou s poskytováním spojena.

Prosím, toto neznamena, že zákazník nenese náklady - zákazník obecně platí službu. Provozovatel služby pak těmito příjmy pokrývá náklady na její provoz. Podobně je to u rizik. Ty sice nemá možnost zákazník ovlivnit, ale i tak zůstává jejich příjemcem. Pokud se riziko projeví, pak následek, např. ve smyslu nedostupnosti služby, úniku citlivých informací, apod. dopadne také na zákazníka.

Služba IT z pohledu ITIL, tak jsou všechny explicitně popsání funkce zajišťované prostředky IT využívané v rámci jakéhokoliv procesu v organizaci nebo jakékoliv činnosti organizace.

Služba tedy stojí ve středu zájmu ITIL. *Strategie* se zaměřuje na sladění potřeb organizace a celého životního cyklu služeb. Služba by se tak měla stát strategickým aktivem organizace a jejího řízení. Strategie je tak primárně určena pro management a neřeší technické aspekty zavádění a provozu služeb.

7.2 Strategie služeb

Z hlediska procesů, které by strategie služeb měla pokrývat lze zmínit především řízení:

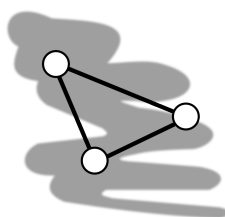
1. portfolia služeb
2. požadavků popř. potřeb

3. financí

Jinými slovy - účinná strategie musí umožnit organizaci pochopit, jakým způsobem jsou provozovány jednotlivé služby v rámci organizace (co přesně je nabízeno). Provozované služby pak nejsou v čase konstantní, jejich nabídka musí reagovat na změny v organizaci jako takové stejně jako v širším prostředí, ve kterém organizace funguje.

Takové změny se obvykle projevují ve změně požadavků, které odběratelé služby kladou na jejího dodavatele. Řízení požadavků pak umožňuje takové informace shromažďovat na jednom místě a programově na ně reagovat. Tady je patrný výrazný posun ve vnímání IT.

Změny v IT si nevymýšlí „ajťák“, ale jsou vyvolávány tlakem útvarů organizace zajišťující její běžné činnosti. Tento posun ve způsobu myšlení je nezbytný také z řady dalších důvodů - např. bezpečnosti informací, osobních údajů (GDPR), atd. Úspěch v takových případech vyžaduje integrovaný přístup, napříč organizací.



Vaše postavení vs ajťák

Z pohledu bezpečnosti by v praxi měl být postup takový, že v aktivitách řešících bezpečnost se specialista na „klasickou“ bezpečnost sejde na půl cesty se specialistou na IT.

V dnešní době nelze řešit bezpečnost činností provozovaných organizací a zároveň nezohlednit IT složku, která je zajišťuje.

Výše uvedené se pak musí dít v rámci finančních možností organizace - je potřeba zajistit prostředky na pořízení i provoz služeb. Finanční plánování se týká nejen provozních výdajů na energie, hardware, ale také práci personálu, která služby udržuje v chodu.

7.3 Návrh služeb

Na základě současných a předpokládaných budoucích požadavků jednotlivých zákazníků jsou navrhovány jednotlivé služby. Návrh se týká nově realizovaných služeb, ale také služeb stávajících. Návrh v takovém případě by měl danou službu inovovat ve smyslu *zlepšení charakteristik* poskytované služby.

Takové charakteristiky přitom mohou nabývat mnoho různých podob. Může se jednat o úpravu služby, ve smyslu zvýšení její kvality nebo rozsahu. Inovace může ale také vést k zvýšení efektivity poskytování služby. Služba může být poskytována levněji, zajišťuje ji menší tým apod.

Procesně do této oblasti patří řízení:

1. úrovně služeb
2. dostupnosti
3. kapacit
4. kontinuity služeb IT
5. informační bezpečnosti
6. dodavatelů
7. katalogu služeb

Kapacita, dostupnost a úroveň služby jsou obvykle předmětem zájmu smlouvy **SLA**. *Dostupnost* rozumíme schopnost zákazníka připojit se a využít službu ve stanovené době. Dostupnost se obvykle udává v procentech sjednaného času.

Čas samotný je dohadován obvykle dle kritičnosti služby. Čím je tedy služba kritičtější, tím vyšší požadavky na její dostupnost obvykle máme.

Jako kritické z hlediska provozu služeb jsou obvykle vnímány základní síťové služby umožňující uživatelům využít síť jako takovou. U tohoto typu služeb pak naše očekávání mohou být až někde v blízkosti 100 % 24 hodin denně, 7 dní v týdnu, jinými slovy činnost těchto služeb by měla být pokud možno nepřerušovaná.

Pokud takové služby porovnáme např. se službami poskytovanými nějakými informačními systémy. Pak většina činností bude pravděpodobně omezena na pracovní dobu, popř. pracovní dobu + vymezená servisní okna služby. Plánovaná doba tak může být např. 7 - 17 nebo 7 - 20 v pracovní dny.

Hodnota 99,9 % dostupnosti pak pro kritickou službu bude znamenat v kalendářním roce celkem 525 600 minut s možným výpadkem 526 minut, tedy něco okolo 8,8 hodin.. Při plánované dostupnosti 99,99 % to znamená, že služba může být nedostupná pouze 53 minut.

Pokud uvážíme informační systém s plánovaným provozem 7 - 17 v pracovních dnech, s dostupností 99 % znamená plánovaný počet minut provozu v roce okolo 150 000 minut, při dostupnosti 99 % bude systém dostupný 148 500 minut, tedy výpadek 1 500 minut - tedy více než jeden den.

Pokud však k výpadku služby dojde mimo stanovený čas (7 - 17), pak se délka výpadku do nasmlouvané délky výpadku nezapočítává.

S dostupností úzce souvisí *kapacita*. Kapacita může nabývat opět různých podob. Hovořit lze např. o přenosových kapacitách, nebo kapacitách současné práce určitého množství uživatelů. Plánování kapacit je obtížné také z toho důvodu, že intenzita užití služeb nemusí být v čase konstantní. Pokud poskytované služby pokrývají agendy zatížené pevně stanovenými termíny plnění, lze předpokládat, že těsně před takovým termínem bude intenzita užití služby nejvyšší.

U kapacit přitom platí, že při jejich vyčerpání dochází ke zhoršování dostupnosti, nebo kvality služby jako takové, např. ve smyslu neúměrného zpomalení služby.

S touto problematikou také úzce souvisí *řízení dodavatelů*. Služba totiž nutně nemusí být dodávána interním poskytovatelem, ale může být poskytována dodavatelem externím. Toto je typická situace u služeb typu SaS (Software as Service), PaS (Platform as Service) nebo cloudových služeb obecně.

Popularita takových řešení v posledních letech výrazně roste, zejména díky velmi příznivým cenám. Organizace by ale i v takovém případě měla vztahy s takovými dodavateli řídit, aby zajistila požadovanou úroveň služeb, které bude využívat.

Všimněte si také několika zajímavostí - v návrhu služeb se nám objevuje také *řízení informační bezpečnosti*. Jedná se ale pouze o jeden z mnoha procesů, které se v rámci ITIL dějí. Oproti tomu systém **ISMS** dle ISO 27000 více méně nic jiného, než informační bezpečnost neřeší.

Katalog služeb v návrhu služeb poskytuje odlišný pohled na tuto problematiku než podobně pojmenovaný proces ze strategie služeb, která řešila *portfolio služeb*. Zatímco strategie pohlíží na tuto problematiku z pohledu samotné existence takového portfolia. Návrh služeb řeší spíše způsob, jakým je katalog udržován a jak se zajistí, že obsahuje aktuální informace o službách.

7.4 Přechod služeb

řeší problematiku skokové transformace systémů poskytujících služby. V praktických podmínkách lze uvažovat o problematice řízení změn a také řízení nasazování systémů.

Změnami v kontextu přechodu služeb rozumíme veškeré změny v konfiguraci nebo v systémech provozujících služby. Kromě konfigurace (změna v nastavení software), může být změna také ve oblasti hardware - např. výměně serveru apod.

Účelem řízení změn je zajistit, aby realizované změny měly pouze minimální negativní dopady během realizace a v provozu pak byly maximálně přínosné. Kontrola nad změnami je také důležitá z toho důvodu, že každá změna představuje zároveň příležitost ke zlepšení služby, ale také riziko pro službu, např. z důvodu nekompatibility nového zařízení s provozovaným systémem.

Řízení nasazování systémů se týká primárně organizací, které služby vyvíjejí ve vlastní režii. Nasazování nových verzí např. informačních systémů se řídí poměrně přísnými pravidly. Nová verze se obvykle nasadí v testovacím režimu, kdy jsou identifikovány možné problémy a ideálně odstraňovány předtím, než je systém nasazen v běžném provozu.

Z typických procesů přechodu služeb lze zmínit např.:

1. řízení nastavování služeb a řízení konfigurací
2. validace a testování
3. řízení uvolňování verzí a jejich nasazování
4. řízení změn
5. řízení znalostí

K výše uvedeným procesům by bylo možná žádoucí uvést, co se rozumí *řízením znalostí*. Rozumí se jím programové shromažďování informací souvisejících s fungováním systémů provozujících jednotlivé služby. V průběhu života služby budou vznikat situace vyžadující servisní zásahy, opravy, rekonfigurace apod. vyžádané změnami v hardware nebo software složce služby.

Vzhledem k tomu, že možných kombinací hardware a verzí software je takřka nekonečné množství, mohou při provozu služby vznikat atypické situace, pro které je pak potřeba najít řešení na míru. Při absenci řízení znalostí jsou taková řešení obvykle přítomna pouze v hlavách pracovníků, kteří se na nalezení takového řešení podíleli.

Vzhledem k tomu, že dochází k fluktuaci zaměstnanců, nelze v takovém případě zajistit, že za nějakou dobu bude taková znalost ještě v rámci organizace dostupná. Pokud nebude, bude atypický problém potřeba řešit znovu - s plnou investicí času a práce vyčleněných pracovníků. Navíc, pokud je problém závažný může být ohrožen provoz služby samotné - ať už z pohledu kvality nebo dokonce úplného výpadku.

Řízení znalostí si klade za cíl shromažďovat takové poznatky na jedno místo tak, aby byly dostupné později, až bude organizace řešit obdobný problém. Charakter systému řízení znalostí může být velmi různorodý - od neformálních poznámek o provozu jednotlivých služeb na sdíleném disku až po komplexní systém umožňující práci se zprávami o bezpečnostních incidentech, s integrací na helpdesk apod.

7.5 Provoz služeb

se koncentruje především na dodávky služeb, jejich provoz a s nimi související procesní aktivity. Obsah této části ITIL je patrnější z procesů, které jsou s ním spojovány:

1. řízení událostí
2. řízení incidentů
3. řízení problémů
4. naplňování požadavků
5. řízení přístupu

Z pohledu řízení IT se poměrně často (ne však vždy) rozlišuje mezi *událostmi* a *incidenty*. Události jsou z určitého pohledu významné momenty v provozu služby. Může se jednat např. o naplnění plánované kapacity datových přenosů, vyčerpání diskové kvóty, a řada dalších. Incidenty proti tomu jsou obvykle spojovány s negativní odchylkou v provozu služby.

I incidenty mohou být různého typu, např. u *bezpečnostních incidentů* je předpoklad narušení bezpečnosti spravovaných informací. Pokud však náhodně selže disk na serveru - jedná se nepochybně o incident, ale nutně ne o bezpečnostní incident.

Tyto procesy často využívají různé logy, popř. automatizované detekční systémy (**IDS**, **IPS**) k detekci událostí a incidentů a umožňují shromáždit k nim analytické informace.

Všimněte si také procesu *řízení přístupu*. Tento proces je kritický pro řízení informační bezpečnosti, umožňuje proto řídit kdo má přístup k jakým datovým zdrojům apod.

V oblasti provozu služeb proto existují významné překryvy jak na systémy ISMS, tak na COBIT.

7.6 Průběžné zlepšování služeb

se zaměřuje na dodávání konzistentních a opakovatelných procesních aktivit. V této oblasti existuje určitý překryv s COBIT, všimněte si např. modelu dospělosti, který pracuje s procesy obdobným způsobem.

Služby by se v čase měly postupně zlepšovat. Zlepšení se obvykle soustředí na některou ze tří základních oblastí kritických pro provoz služeb:

- procesní prvky
- organizační struktury
- finanční toky

Zlepšení mohou být realizována změnami ve správě služeb, popř. ve smyslu identifikace a odstranění problémů. Cílem je tedy identifikovat problémy, popř. úzká hrdla v systému a odstranit je. Takové problémy mohou být buďto v procesech - např. jejich nastavení, ale také v organizačních strukturách.

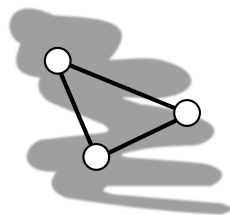
Realizace změn v organizační struktuře je obvykle časově náročnější a nese s sebou jistá rizika, v některých případech však může mít potenciál pro výrazné zefektivnění provozu služby. Reorganizační lze

např. centralizovat využití IT infrastruktury organizace na jednom místě, což může přinést jednorázové posunutí kvality poskytované služby směrem nahoru a mít také dlouhodobé finanční úspory.

Reorganizace se ale také nemusí povést, pak v lepším případě nové řešení je pouze finančně náročnější, v horším případě se reorganizace může negativně projevit také na kvalitě poskytované služby, popř. její dostupnosti.

Do této oblasti lze zařadit následující procesy:

1. řízení úrovně služeb
2. hodnocení služeb a reportování
3. kontinuální zlepšování služeb



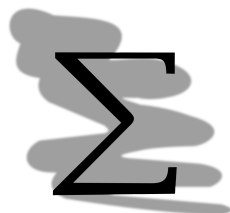
Mapy procesů

Pro ITIL je dostupný také poměrně hezky zpracované mapy procesů, které umožňují vysledovat vzájemné závislosti mezi jednotlivými procesy a to i v grafické podobě, viz IT Process Wiki [26].



Porovnání

Projděte si alespoň v rychlosti systém ISMS řešený pomocí ISO 27000, a rámce řízení COBIT a ITIL. Zkuste specifikovat v čem se liší a také kde se překrývají.



Shrnutí

ITIL poskytuje doporučené postupy pro získání kontroly nad provozem IT. Standard je organizován do 5-ti základních oblastí (core publikací) zaměřených na služby. Službami se v kontextu ITIL rozumí vše, co je z pohledu IT poskytováno vnějšímu, nebo vnitřnímu zákazníkovi.

ITIL, podobně jako COBIT, představuje širší regulační rámec než např. ISO 27000, které je zaměřené pouze na řízení informační bezpečnosti.

Základní publikace zaměřené na strategii služeb, návrh služeb, přechod služeb, provoz služeb a průběžné zlepšování služeb jsou doplňovány dalšími publikacemi řešící některé specifické oblasti a problémy, jako např. zavádění v určitém sektoru (např. státní správa, školství) a také mapování na další rámce řízení (např. COBIT, ISO 27000) apod.



Kontrolní otázky: ITIL

1. Definujte pojem služba v kontextu ITIL.
2. Jaký je rozdíl mezi pojmy - událost, incident a bezpečnostní incident.
3. Co rozumíme řízením znalostí?
4. Co je SLA?

Kapitola 8

Integrace forenzních technik do systému reakce na incidenty



Průvodce studiem

Vhodná reakce na incident umožní organizaci minimalizovat následky a také se z nastalé situace poučit do budoucna. K shromažďování informací o incidentu lze použít forenzní nástroje. Jejich efektivní užití je ale determinováno způsobem jakým jsme se na toto užití připravili procedurálně.

Po přečtení této kapitoly budete

Znát

- co je reakce na incident
- jak fungují forenzní techniky
- jaké otázky je potřeba řešit při integraci těchto technik do celkového systému řízení informační bezpečnosti

klíčová slova: forenzní techniky, forenzní proces, reakce na incidenty, ISMS, obnova

nároky na předchozí znalosti: Forenzní techniky budeme integrovat do systému ISMS, z tohoto důvodu by bylo žádoucí, abyste z úvodních kapitol pochopili, jak tento systém funguje. Zaměřit byste se měli také na bezpečnostní politiky, jako místo, kde tyto techniky integrujeme.



Čas nutný ke studiu

Pro prostudování této kapitoly budete potřebovat přibližně 4 hod.

8.1 Otázky integrace forenzních technik do systému ISMS

V předchozí kapitole jsme již definovali pojmy *incident* a *bezpečnostní incident*. Tyto definice odpovídají také způsobu, jakým tyto pojmy budou užívány v této kapitole. Vzhledem k tomu, že v důsledku incidentu dochází k poklesu kvality poskytovaných služeb nebo dokonce k přerušení poskytování takových služeb je očividné, že organizace na takové incidenty musí reagovat.

Reakce sice může přistoupit ke vzniklému problému ad hoc a řešit jej případ od případu - takový přístup však není příliš efektivní. Čím je organizace větší, tím častěji se potýká s incidenty různého

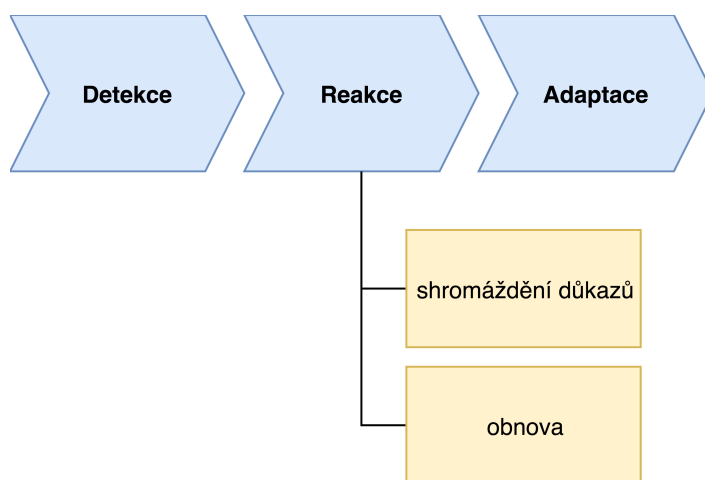
typu. Řada incidentů se přitom v čase opakuje. Vyvíjet proto ad hoc řešení znovu a znovu v takovém případě odpovídá snaze znovu vynalézt kolo. Střední a velké organizace proto zavádějí systémy *reakce na incidenty*, které jim umožňují konsolidovat na jednom místě znalosti, ale také nástroje nutné pro řešení vybraných typů incidentů.

Reakce na incident si obvykle klade za cíl minimalizovat následky působení incidentu, popř. pak také zamezit opakování takového incidentu do budoucna.

Základním nástrojem pro získání informací o incidentu jsou *forenzní techniky*. Kromě tohoto názvu se často používá také názvy jako počítačová forenzní věda, počítačová forenzika, digitální forenzní vědy a řada dalších. Bez ohledu na název se jedná o postupy pomocí kterých hledáme důkazy v počítačích, serverech a jiných zařízeních a na datových médiích.

Forenzní vědy mají zejména díky filmu a televizi silnou konotaci na úkony orgánů činných v trestním řízení - toto ale není kontext, ve kterém budeme o těchto nástrojích hovořit v této kapitole skript. Nás tyto techniky budou zajímat z hlediska použití pro vnitřní potřeby organizace (byť základní principy jsou stejné).

Základní schéma reakce na incidenty je znázorněno na obr. 8.1.



Obrázek 8.1: Základní schéma reakce na incidenty v organizaci

Aby na incident bylo možné reagovat, je nejprve nutné detekovat, tzn. zjistit, že nastal. Detekce přitom nemusí být snadná. To se projevuje zejména u dlouhodobých, profesionálně realizovaných průniků do sítí organizací motivovaných snahou získat intelektuální vlastnictví, nebo jiné citlivé údaje. Takové útoky často probíhají týdny nebo dokonce měsíce bez povšimnutí.

Oproti tomu útoky ransomware popř. jiných typů škodlivého kódu jsou často detekovány velmi rychle, jelikož jsou následky takového incidentu viditelnější.

Reakce v obecné rovině spočívá ve dvou momentech - *shromáždění důkazů* o povaze a průběhu incidentu a provedení obnovy problémového aktiva do provozuschopného stavu. Obnova se provádí až po dokončení shromažďování dat o incidentu. Provedení obnovy totiž obvykle vede k nevratnému poškození důkazů na daném aktivu.

Při shromažďování důkazů a obnově se tedy střetávají dva protichůdné oprávněné zájmy. Na straně jedné má organizace zájem co možná nejrychleji obnovit funkci postiženého aktiva. Na straně druhé proti tomuto zájmu jde pak snaha poučit se, adaptovat a do budoucna se opakování události vyhnout nebo alespoň zmenšit následek její realizace. K tomu jsou ale potřeba informace a k jejich shromáždění je potřeba čas.

S přihlédnutím k závažnosti, ale také novosti/zkušenosti s incidentem tak organizace volí kompromis mezi těmito zájmy.

U rutinních incidentů, se kterými se organizace vypořádává dnes a denně tak např. nemá smysl nějaké informace vůbec shromažďovat a rovnou přistoupit k obnově. Naopak u závažných incidentů s velkými dopady je očividný potenciál k poučení se a organizace proto shromažďuje o takovém incidentu podstatně více informací i za cenu toho, že postižené aktivum nebude určitou dobu dostupné.

Z incidentu se potenciálně lze poučit do budoucna a fungování aktiv, služeb, popř. organizace jako celku (nebo její jednotlivé části) adaptovat s cílem předejít opakování incidentu nebo do budoucna minimalizovat jeho následky.

Výše uvedený postup ilustruje pouze základní schéma reakce na incidenty - existuje celá řada metodik, které lze k tomuto účelu implementovat a které podrobněji rozebírají tuto problematiku.

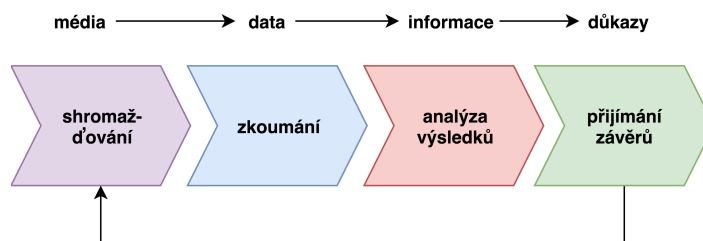
Jako jeden z přístupnějších standardů lze doporučit např. NIST SP 800 - 86 [49].

Řada speciálních publikací NISTu je určena pro použití zejména ve státní správě a na úřadech. Formálně jsou jednotlivé publikace psány spíše volnou formou umožňující se v problematice poměrně rychle zorientovat a případně přijmout opatření k zlepšení stavu.

Kromě NIST SP 800-86, jsou v řadě 800 dostupné také další předpisy:

- NIST SP 800-72 Guidelines on PDA Forensics (2004)
- NIST SP 800-101 rev. 1 Guidelines on Mobile Device Forensics (2014)
- NIST SP 800-202 Quick Start Guide for Populating Mobile Test Devices (2018)

Forenzní proces doporučený SP 800-86 je znázorněn na obr. 8.2. Tento proces se orientuje přitom pouze na fázi *reakce*, tak jak je znázorněna na obr. 8.1.



Obrázek 8.2: Schéma forenzního procesu (převzato z NIST SP 800-86 [49])

Všimněte si práci se údaji na obr. 8.2. Ve fázi shromažďování se pracuje s médii, která mohou obsahovat cenné údaje. Takové údaje je nutno z média přenést pro další analýzu, tím získáváme data. Vytěžením dat v kontextu zkoumaného incidentu získáváme z dat informace. Interpretací informací pak získáme důkazy použitelné pro přijímání závěrů a reportování.

Pro potřeby provádění forenzních analýz je potřeba si připravit půdu. Vzhledem k tomu, že v průběhu analýzy shromážděných dat budeme pracovat s možná citlivými údaji (podle toho, co bylo uloženo na analyzovaném zařízení). Je potřeba možnost provádění takových analýz do systému řízení informační bezpečnosti nebo obecně do předpisového rámce dané společnosti, pokud systém ISMS implementován nebyl.

Informace, které v budoucnu budeme pomocí forenzních technik chtít zpracovat je také potřeba předem shromažďovat - v okamžiku, kdy nastane incident je pro rozhodnutí o shromáždění informací zpravidla pozdě. Pokud např. systém nebyl konfigurován tak, aby logoval některé typy událostí - informace o takových událostech prostě nebudou dostupné.

Rozhodnutí o rozsahu a způsobu zpracování je tak důležitou součástí systému ISMS. Ne nadarmo je jednou z doporučených bezpečnostních politik, politika zaměřená na zpracování dat.

Další poměrně důležitou součástí nastavení systému ISMS a jeho integrace se systémem reakce na incidenty je rozhodnutí zda, popř. kdy kontaktovat třetí stranu. Touto třetí stranou může být třeba Policie ČR, nebo Národní úřad pro kybernetickou bezpečnost, případně Úřad pro ochranu osobních údajů. Nutnost kontaktovat takové instituce obvykle vychází z legislativně stanovené povinnosti tak v určitých případech učinit.

Tyto případy je potřeba přesně popsat a specifikovat, kdo bude stanovenou instituci kontaktovat a v jakém rozsahu bude předávat informace.

Podobná omezení mohou být aplikována na dodávky služeb soukromých subjektů. V souvislosti s forenzními technikami se nabízí:

- služby pro obnovu dat na poškozených pevných discích
- práce konzultantů
- provádění specializovaných analýz
- právní pomoc
- a další

Forenzní techniky ale mohou být přínosné v řadě dalších oblastí. Mohou např. pomoci v identifikaci a odstraňování běžných provozních chyb. Takové chyby vznikají prostými nekompatibilitami, chybami v konfiguraci apod. a nelze je tak považovat za incidenty.

Podobně mohou také tyto techniky napomoci při:

- logování a monitoringu funkce vybraných systémů organizace
- obnově nebo záchraně dat
- získávání dat o provozu systémů - např. pro účely analýzy efektivity
- prokazování bdělosti/připravenosti organizace chránit svá citlivá data (např. v souvislosti s GDPR)

Pro zajištění funkce zvolených (organizací podporovaných) forenzních technik je potřeba kromě technického zázemí budovat také zázemí personální. Nasazení takových technik tak vyžaduje vybavení pověřeného personálu příslušnými znalostmi.

Uvažovat lze o třech základních specializovaných zaměřeních takových pracovníků:

1. vyšetřovatelé
2. incident handlers - pracovníci zaměřeni na zvládnutí incidentu
3. IT profesionálové

IT profesionálové nám představují skupinu běžného personálu zajišťujícího běžný provoz IT. jedná se tedy o administrátory, správce webu organizace, správce informačních systémů, technickou podporu apod. Tyto osoby musí být seznámeny se základními požadavky které na ně budou kladeny v souvislosti s vyšetřováním a zvládáním incidentů.

Vyšetřovatelé se zaměřují na shromažďování a vyhodnocování údajů o incidentu. Součástí jejich práce může být také formulace doporučení jednak pro incident handlers, jednak pro management společnosti, popř. další osoby, nebo skupiny osob v organizaci. Taková doporučení by měla vždy směřovat k vyhnutí se opakování incidentu nebo alespoň minimalizace jeho následků.

Incident handlers pak zajišťují obnovu činnosti aktiva postiženého incidentem. Práce těchto pracovníků na obnově mohou začít až v okamžiku, kdy k tomu vydají souhlas vyšetřovatelé, jelikož obnova obvykle znemožní další shromažďování dat o incidentu.

Veškeré činnosti nutně nemusí být realizovány interními zaměstnanci organizace. Existuje řada specializovaných firem, které takové služby poskytují za úplatu. Vodítkem pro rozlišení činností, které je vhodné realizovat interně mohou být náklady na vytvoření odpovídajících kompetencí zaměstnanců a technického zázemí nutného pro realizaci takových postupů.

Pokud jsou k realizaci potřebné pokročilé znalosti a drahé specializované nástroje, popř. technologie - může být pro organizaci zajímavé takové služby outsourcovat.

Vodítkem může být také frekvence předpokládaného použití takových nástrojů. Pokud lze očekávat časté použití, může být výhodné realizovat danou činnost interně.

Interně realizované činnosti je také obvykle možno realizovat rychleji - alespoň ve smyslu času reakce.

Vodítkem může být taktéž důvěrnost dat, která by mohla u externího subjektu uniknout. Některé informace mohou být natolik citlivé, že pro organizaci může být výhodnější připustit ztrátu takových dat (ve smyslu zničení) spíše než riskovat únik dat. Nicméně organizace, které se specializují na obnovu dat mají bussiness založen na důvěře - unik dat by takovou důvěru nevratně narušil.

Takový problém lze tak považovat za spíše minoritní.

Použití forenzních nástrojů by v rámci organizace mělo být také omezené. Tyto nástroje jsou mocné a umožňují jejich uživateli získat podrobné informace o analyzovaném zařízení a to často včetně informací týkajících se jejich uživatelů. Tyto informace pak mohou být zneužitelné.

Při nasazování nástrojů bychom se proto měli řídit *principem úměrnosti*. Jinými slovy při řešení banálních incidentů není nutné nasazovat sofistikované forenzní nástroje.

Také ačkoliv jsou přínosy nasazení forenzních technik v organizaci poměrně široké - ne všichni pracovníci by měli mít možnost s nimi pracovat. Nástroje tak mohou používat např. pouze pracovníci s přidělenými určitými rolemi v organizaci. U takových pracovníků můžeme efektivněji kontrolovat, zda nedochází ke zneužívání nástrojů.

8.2 Forenzní proces

V předchozí podkapitole jsme se zaměřili na otázky související s rozsahem realizace nasazení forenzních technik v organizaci. Takové otázky je potřeba řešit institucionálně vhodným nastavením procesů a předpisové základny organizace.

Jednotlivými kroky forenzního procesu, tak jak je specifikován na obr. 8.2, jsme se ale dosud nezabývali. Vraťme se proto k jednotlivým krokům *forenzního procesu* a zkusme rozebrat momenty a omezení, která jsou s ním spojena.

Prvním krokem forenzního procesu je *sběr dat*. Tento krok realizují obvykle osoby pověřené vyšetřováním incidentu. K tomuto účelu je nutno identifikovat všechny možné zdroje dat a také vyvinout plán pro získání dat.

V rámci takového plánu se obvykle řeší předpokládaná hodnota (přínos) dat pro pochopení incidentu, volatilita dat a také cena aktiva jako takového. Zohlednit je potřeba také úsilí, které je nutné vynaložit na získání dat - *vyplatí se to?* Takový plán není možné připravit předem, neboť každý bezpečnostní incident je jiný a plán je tak potřeba připravit na míru situace.

Měřítka předpokládaného přínosu pro analýzu situace je poměrně jasné, co se ale rozumí *volatilitou dat*? Jedná se o rozlišení dat podle jejich stálosti. Např. data v RAM při vypnutí počítače budou smazána. Obsah paměti RAM je také průběžně měněn v souvislosti s provozem zařízení. Jedná se tedy o data vysoce nestálá - volatilní.

Podobný charakter může mít stav různých připojení k zařízením na síti - při určité době nečinnosti mohou být ukončena, DHCP server přiděluje IP adresy také na omezenou dobu apod.

Oproti tomu, data uložená na disku volatilní nejsou.

Všimněte si také otázky ceny aktiva jako takového - pokud aktivum zajišťuje kritickou službu, lze předpokládat velký tlak na co možná nejrychlejší obnovu činnosti aktiva. Jelikož obnova s vysokou pravděpodobností zabrání dalšími sběru údajů ze zařízení je shromáždění údajů z tohoto zařízení potřeba dát vyšší prioritu.

Shromážděná data podrobujeme *zkoumání*. Shromažďování údajů přináší obvykle podstatně více údajů než je potřeba pro provedení analýz v plánovaném rozsahu. Proto je potřeba identifikovat to co je skutečně relevantní.

Při zkoumání je nutno se vypořádat také s řadou dalších faktorů spojených se způsobem, jakým jsou data uložena - např. komprese dat, šifrování, případně obfuskace. Pro zajímavost obfuskace je proces, kterým programátor smaže tzv. bílé znaky (znaky konce řádků, tabulátory apod.) ze zdrojového kódu a přejmenuje názvy proměnných z názvů popisujících funkci proměnné na neutrální názvy, jako např. a, b, c, ... Cílem je obvykle úspora místa. Z hlediska analýzy kódu např. podezřelého skriptu se ale jedná o překážku, která takovou analýzu značně znesnadňuje.

Problémem může být také použití diskových polí - kdy jsou data organizována napříč disky apod.

Ve fázi zkoumání maximálně nasazujeme analytické nástroje k extrakci cenných dat, pokud je máme k dispozici.

Zkoumáním byly získány výsledky - důkazy, které je potřeba v kontextu incidentu interpretovat. To se provádí ve fázi *analýzy*.

V rámci analýz koreluje data z různých zdrojů, abychom získali ucelený obraz o průběhu a rozsahu incidentu. Na základě takto shromážděných údajů lze již přijímat závěry a doporučení pro budoucí úpravu postupů.

Reportování pak zakončuje celý proces. Účelem je připravit zprávu o incidentu a jeho řešení. Součástí zprávy mohou být také alternativní vysvětlení. Analyzovaná data totiž nutně nemusí vést k jednoznačnému vysvětlení všech zjištěných skutečností.

Forma zpracování zprávy by měla brát v úvahu to, pro koho je určena. Pokud zpráva má být určena managementu, pak je nutné aby byla spíše stručná a méně technická. Měla by také obsahovat informace potřebné pro dlouhodobé řízení organizace (pokud je např. potřeba v důsledku incidentu věci řešit jinak).

Pokud je zpráva určená pro IT specialisty je naopak žádoucí vysoká míra podrobnosti v oblasti technických záležitostí.

Zpráva by v každém případě měla obsahovat „*akční informace*“. Tyto informace jsou zaměřeny na případné další činnosti, které mohou být realizovány, např. možnost získání dalších doplňkových dat a co by jejich analýzou mohlo být případně získáno, informace umožňující zabránit vzniku obdobného incidentu do budoucna, doporučení na změny v procesech apod.

Vzhledem k výše uvedenému může být potřeba zpráv napsat více, pro různé příjemce. Sestavení takové zprávy je ale časově i finančně náročné, proto zdůrazňujeme (opět po čase) princip úměrnosti. Zprávy tedy zpracováváme v minimálním potřebném rozsahu.

**Shrnutí**

forenzní techniky umožňují získání širokého spektra informací o provozovaných aktivech organizace a způsobu jejich využití. Tyto informace je vhodné využít jednak při reakci na incidenty, jednak při řešení běžných problémů provozního charakteru.

S nasazením takových nástrojů je ale spojována také řada problémů, které je potřeba řešit institucionálně v rámci vnitropodnikových předpisů a procesů - mimo jiné: rozsah nasazení forenzních nástrojů, možnosti využití externích subjektů, personální zabezpečení celého procesu apod.

Samotný forenzní proces v obecné rovině se děje ve čtyřech fázích - shromažďování dat, jejich zkoumání, provádění analýz a reportování výsledků.

**Kontrolní otázky: 8 Forenzní techniky**

1. Co je forenzní proces a jaké má fáze?
2. Co rozumíme volatilitou dat?
3. Jaké otázky řešíme při rozhodování o začlenění použití forenzních technik do procesů organizace?
4. Vysvětlete vztah shromažďování dat o incidentu a obnovy funkce aktiva po incidentu.

Kapitola 9

Řešení kontrolních otázek



Odpovědi: 1.1 Úvod do prostředí organizace a ISMS

1. Mikroekonomické prostředí představuje běžný trh, tedy vztahy s konkurencí, dodavateli a zákazníky (v oblasti bezpečnosti jde např. o riziko průmyslové špionáže či únik klientských dat). Makroekonomické prostředí je tvořeno vlivem vlád, samospráv a regulačních orgánů, které organizaci diktují legislativní povinnosti a požadavky na certifikace.
2. Okolí úřadu tvoří občané (koncoví uživatelé služeb), dodavatelé softwarových řešení a hardwarové infrastruktury, externí servisní organizace provádějící údržbu a jiné státní instituce (např. Policie ČR), které s registrem datově komunikují.
3. Informační aktivum je jakýkoliv systém zpracovávající informace (primární aktivum) nebo prostředek, který spolehlivý běh těchto informačních systémů zajišťuje (podpůrné aktivum). Příklady: Databázový server s klientskými údaji, síťový firewall, nebo samotná budova datového centra.
4. ISMS (v ČR SŘBI) je Systém řízení informační bezpečnosti. Jde o ucelený filozofický a manažerský přístup sloužící k systematickému řízení rizik a k získání plné kontroly nad bezpečností citlivých informací napříč celou organizací.



Odpovědi: 1.2 Organizační struktura a manažerské pozice

1. Zkratky vedoucích pozic a jejich pracovní náplň:
 - **CISO** (Manažer informační bezpečnosti): Odpovídá za celkovou informační bezpečnost, řízení rizik, soulad s legislativou a řešení bezpečnostních incidentů.
 - **CIO** (Ředitel IT): Má na starosti klasickou správu, rozvoj, údržbu IT infrastruktury a podporu koncových uživatelů.
 - **CSO** (Ředitel bezpečnosti): Zodpovídá za vývoj a implementaci celkové bezpečnostní vize organizace, přičemž je primárně zaměřen na fyzickou a objektovou bezpečnost (ochranu majetku a osob).
2. Jejich pracovní náplně se prakticky nepřekrývají, a proto ke slučování těchto dvou pozic nedochází (CIO řeší IT provoz, CSO řeší fyzickou bezpečnost). CSO však často úzce spolupracuje s CISO (bezpečností IT), protože technické zabezpečení přímo ovlivňuje ochranu dat a také řada prostředků používaných k zabezpečení se integruje do počítačové sítě organizace a propojuje s dalšími systémy, jako např. IDM
3. VŠB má zřízeny pozice architekta KB, CIO, CSO i CISO. Za schvalování předpisů v oblasti bezpečnosti informací zodpovídá Výbor KB. Podrobné informace o informační bezpečnosti je možno nalézt v interních předpisech VŠB-TUO na <https://innet.vsb.cz>. Důvodem je, že VŠB-TUO podléhá regulaci zákonem o kybernetické bezpečnosti a to ve vyšším režimu povinností.
4. *(Metodické vodítko pro studenty)*: V projektu je nutné jasně rozdělit kompetence do tří pilířů: klasická správa IT, technologická bezpečnost IT a fyzická ochrana/zabezpečení budov, a těmto oblastem přiřadit konkrétní odpovědné role (CISO, CIO, CSO).
5. Pozice CISO není určena pro čistého informatika. Vyžaduje přesah do managementu rizik, práva (shoda s legislativou) a schopnost komunikovat s nejvyšším vedením podniku. Každý z Vás má ale jinou strukturu nepovinných předmětů a také jiné zájmy. Tuto otázku tudíž zcela univerzálně v tomto místě nemohu zodpovědět - je to spíše otázka na Vás. *Co chcete, čím se chcete zabývat?*



Odpovědi: 1.3 Plánování, mise a vize

1. Dlouhodobé plány vytyčují strategické cíle a rozsáhlé transformace (např. fúze, zavádění nových technologií) a jsou méně konkrétní. Krátkodobé plány jsou velmi detailní a slouží k zajištění běžného chodu a alokaci operativních zdrojů.
2. Mise a vize společnosti jsou základní dokumenty společnosti stanovující účel její existence (mise) a cíl, kterého chce dosáhnout (vize).
3. Délka plánovacího cyklu úzce souvisí s rychlostí změn v daném oboru. Pro obory s rychlým vývojem technologií (např. IT) jsou plánovací cykly kratší než např. v oborech tzv. těžkého průmyslu.



Odpovědi: 1.4 Bezpečnostní dokumentace

1. Projekt je jednorázové, časově omezené úsilí, jehož cílem je vytvořit unikátní produkt, službu nebo výsledek. Má jasně stanovený začátek a konec, definovaný rozpočet a konkrétní cíle, kterých chce dosáhnout.
2. Projektová bezpečnostní dokumentace řeší bezpečnostní aspekty realizace projektu. Po dokončení projektu pozbývá smysl. Provozní dokumentace proti tomu pokrývá rutinní provoz systému a má význam až do okamžiku, kdy je systém vyřazen z provozu.
3. Monolitickou dokumentací rozumíme přístup k tvorbě předpisů, který se maximálně snaží konsolidovat všechny aspekty řízení bezpečnosti informací do jednoho předpisu.
4. Politika je vnitropodnikový předpis, který stanovuje základní filozofii řešení určitého problému. Postup je podrobné doporučení, jak postupovat při řešení problému. Postup nemá charakter vnitropodnikového předpisu.



Odpovědi: 1.5 Schvalovací procesy

1. Zajistit, že schválený předpis obsahuje vymahatelná ustanovení a neexistují, žádné institucionální překážky v tom, aby předpis mohl fungovat očekávaným způsobem.
2. Nikdy. Bezpečnostní dokumentace se musí vyvíjet společně s organizací tak, aby reagovala na změny v organizaci samotné i vlivy vnějšího mikro- i makro- ekonomického prostředí.
3. Cíle specifikují, kam se v budoucnu chce dostat organizace. Dosažení těchto cílů obvykle vyžaduje transformaci organizace a ta s sebou nese bezpečnostní otázky, které je nutno řešit.



Odpovědi: 1.6 Formálnost a restrikce politik

1. U racionálního, kde začínáme s nulovými právy (deny all) a teprve postupně povolujeme práva, která uživatel skutečně potřebuje ke své práci.
2. Ve velmi malých, dobře komunikujících týmech, kde jednotliví členové týmu jsou schopni dodržet neformální dohody (takže téměř nikde).
3. Jedná se stavy počáteční konfigurace práv k systému - allow all povoluje vše, zatímco deny all zakazuje vše (viz také první otázka, resp. odpověď na ni).
4. Bohužel žádný :-).



Odpovědi: 1.7 Základní principy bezpečnostní dokumentace

1. úměrnosti, integrity, aktuálnosti, ...
2. Aby závazná ustanovení v předpisu bylo možno vymáhat, musí být pracovníci, kteří mají toto ustanovení vykonávat být prokazatelně s ním seznámeni (tedy znát jej).
3. Bez vymahatelnosti nebude mít předpis schopnost vynutit to, co říká - bude mít charakter nezávazného doporučení.
4. Podle rychlosti změn v oblasti, kterou pokrývá.

**Odpovědi: 1.8 Audit a revize politik**

1. na jedné straně jsou to specialisté na IT a bezpečnost informací, na straně druhé jsou to představitelé významných skupin uživatelů, kteří budou podléhat ustanovením přijímaných předpisů. Účelem je nalezení rovnováhy mezi funkcí a bezpečností.
2. V ceně, dostupnosti a rychlosti (vyšší u interních auditorů), odbornosti, zkušenosti a dostupnosti specializovaných nástrojů (vyšší u externích auditorů)?
3. Např. audit pro oficiální certifikaci může provést pouze externí auditor, který je k tomu sám certifikován.
4. Řídit provozní aspekty bezpečnosti informací?
5. Projednávat otázky bezpečnosti informací a také schvalovat předpisy v této oblasti
6. Spravovat svěřené aktivum z pohledu funkčnosti, ale také bezpečnosti?

**Odpovědi: 2.1 Systém ISMS**

1. ISMS je systém řízení zaměřený na řízení bezpečnost informací. Umožňuje organizaci získat kontrolu nad chráněnými informacemi.
2. Specifikovat, co je předmětem zájmu systému ISMS.
3. PDCA představuje řídicí smyčku, která umožňuje organizaci porovnat skutečný stav se stavem žádoucím, identifikovat rozpory a tyto rozpory vyřešit. Postupná aplikací těchto jednoduchých kroků umožňuje organizaci postupně systém ISMS zlepšovat až dosáhne požadované úrovně výkonu.
4. RTP představuje plán na zvládání rizik ve kterém organizace rozhoduje co a kdy bude dělat s identifikovanými riziky.
5. SOA představuje Prohlášení o aplikovatelnosti. Základ prohlášení představují kontroly z přílohy A normy ISO 27001. Organizace do seznamu může doplňovat dle potřeb další kontroly. V rámci SOA organizace rozhoduje, zda-li je daná kontrola relevantní (aplikovatelná) v kontextu organizace. Pokud ano, pak specifikuje v které části systému ISMS je kontrola nasazena.

**Odpovědi: 2.2 Bezpečnostní politiky a prohlášení o aplikovatelnosti**

1. SOA představuje Prohlášení o aplikovatelnosti. Základ prohlášení představují kontroly z přílohy A normy ISO 27001. Organizace do seznamu může doplňovat dle potřeb další kontroly. V rámci SOA organizace rozhoduje, zda-li je daná kontrola relevantní (aplikovatelná) v kontextu organizace. Pokud ano, pak specifikuje v které části systému ISMS je kontrola nasazena.
2. Politika systému ISMS stanovuje základní organizační struktury, role a procesy systému ISMS. Bezpečnostní politika aktiva proti tomu implementuje tyto požadavky do kontextu konkrétního typu aktiv.
3. Protože bezpečnost informací není statická. Mění se postupně používané systémy, požadavky, které na ně máme, mění se legislativa, objevují se nové hrozby a mění se náš pohled na ty existující. V průběhu času se mění také apetit organizace k riziku. Vše výše uvedené vede k nutnosti revidovat politiky.
4. Řídíme se podle zákona o utajovaných skutečnostech. Naše nároky na zabezpečení v takovém případě budou nesrovnatelně vyšší.



Odpovědi: 2.3 Řízení rizik

1. Jedná se o dokument, který se vytváří na základě analýz rizik a obsahuje rozhodnutí o způsobu jakým se vypořádat s rizikem.
2. Opakovatelností rozumíme schopnost vykonat analýzu rizik na daném aktivu jinou osobou s dosažením srovnatelných výsledků.
3. Specifikuje jak podstupovat při analýzách rizik.
4. fyzické (např. nevhodné umístění), fyzikální (postranní kanály), antropogenní (útok hackera).
5. Vyplyvají z fyzické realizace aktiva. Aktivum musí např. odebírat elektrickou energii, nějakou dobu trvá výpočet apod. Tyto veličiny lze měřit a použít jako podklad pro prolomení použitého algoritmu.
6. Zranitelnost, která je aktivně zneužívána, ale není pro ni dostupná záplata.
7. Objevit, popsat, exploit, záplata.



Odpovědi: 3.1 Inventarizace aktiv

1. Slouží k popisu způsobu (hardware, software, zapojení) jakým je systém nasazen do provozu.
2. uzel, komponenta, asociace
3. Proces umožňuje identifikovat všechna primární a podpůrná aktiva, která organizace používá pro manipulaci s chráněnými informacemi.
4. Umožňuje automatizovaně po síti identifikovat počítače on-line.
5. Jméno zařízení, IP adresu, operační systém, seznam síťových služeb, které zařízení poskytuje.
6. Jako zdroj lze použít celou řadu dalších systémů a evidencí, např. IDM, účetnictví, záznamy skenů sítě, atd.



Odpovědi: 3.2 Management aktiv

1. Správou požadavků rozumíme proces, který programově shromažďuje (eviduje) požadavky, přiděluje je k řešení a sleduje průběh řešení tak, aby bylo zajištěno, že všechny požadavky budou zpracovány.
2. Požadavky je vhodné rozdělovat podle toho, jakého problému nebo oblasti se týkají. Pro každou z takových oblastí vytváříme řadu, např. řada instalace software, bezpečnostní incident, ...
3. Rozhoduje to, jaké systémy a funkce organizace provozuje a vykonává.
4. Managementem změn rozumíme proces, který zajišťuje že všechny změny v infrastruktuře budou evidovány, kontrolovány, testovány tak aby bylo zajištěno, že změna nepůsobí při své realizaci organizaci problémy.
5. CMDB databáze umožňuje na jednom místě shromáždit informace o aktivech společnosti. Tato DB se pak může stát vhodným zdrojem informací pro efektivní management těchto aktiv, analýzy rizik, popř. další analytické procesy v rámci organizace.
6. Nejprve určíme rozsah informací, které bude potřeba zpracovávat a místa, kde se tyto informace nacházejí. Následně pořídíme nebo implementujeme CMDB a vytvoříme datové pumpy, které informace z jejich původního umístění načerpají do CMDB. Celý proces musí být formalizován procesem nebo politikou, aby byla zajištěna jeho dlouhodobá udržitelnost.

**Odpovědi: 3.3 Správa licencí**

1. Získat kontrolu nad software, který se v organizaci využívá a zajistit a prokázat, že se používá v souladu s autorským zákonem.
2. Osoba, která má přehled o licencovaném software a jeho nasazování v organizaci. Mimo jiné přiděluje licence.
3. Proveďte se sken veškerého IT organizace s cílem identifikovat instalovaný software. Výsledné seznamy se pak porovnávají se seznamy licencovaného software a řeší se rozpory.
4. Zkoumá se příčina nesrovnalostí. Příčina může být v chybné detekci, ale také v tom, že se používá nelicencovaný software. V takovém případě je potřeba dokoupit licenci nebo takový software odinstalovat.

**Odpovědi: 3.4 Management zranitelností**

1. Existují repozitáře zranitelností, proti kterým je možno provést manuálně nebo s použitím specializovaného software kontrolu.
2. Ideálně instalujeme záplatu od výrobce software, která příčinu zranitelnosti odstraňuje. Alternativně lze také dělat další opatření, která znesnadňují možnost zneužití zranitelnosti.
3. Je to časově náročné, pokud je vykonáváno ručně. Existuje šance, že některá zařízení v takovém případě budou vynechána a zůstanou tak zranitelná.
4. Primárně používáme vestavěné nástroje operačních systémů, např. App Store (Apple), Microsoft Store. Tyto doplňujeme dalšími doplňkovými nástroji pro instalaci dalšího software. V případě Linux jsou dostupné robustnější repozitáře software, které činí instalaci a údržbu software obvykle jednodušší.

**Odpovědi: 6 COBIT**

1. Managementem rozumíme rutinní, každodenní manažerskou práci. Governance rozumíme spíše strategickou úroveň řízení.
2. Obojí se do češtiny překládá jako odpovědnost ale význam je jiný. Responsible je odpovědnost něco udělat, zatímco accountable je odpovědnost za výsledek. (V tomto případě by se na tento typ odpovědnosti dalo nahlížet jako na manažerskou odpovědnost)
3. Business Score Cards. Jedná se o manažerský nástroj, který umožňuje kombinovat business cíle a schopnosti organizace.
4. Model dospělosti umožňuje organizaci porovnávat procesy s dalšími organizacemi nebo standardy výkonnosti procesů pro dané odvětví. Poskytují informaci o tom jak vyspělé je zavedení procesu v organizaci, což je informace použitelná pro plánování práce na procesech.
5. Matice odpovědností. V COBIT se používá jako všude jinde - pro jednoduchou a rychle komunikaci odpovědností různým rolím.

**Odpovědi: 7 ITIL**

1. Služba v ITIL je jakýkoliv výkon realizovaný pomocí IT, poskytovaný vnějšímu nebo vnitřnímu zákazníkovi.
2. Událostí rozumíme situaci kdy řízený systém společnosti čelí nějakému potenciálnímu problému bez dopadu na bezpečnosti. Incident je pak událost, která vyeskalovala až do té míry, že způsobuje škody. Bezpečnostní incident pak znamená, že tento dopad je na bezpečnost.
3. Programové budování know-how v oblasti provozu služeb IT.
4. Dohoda o úrovni služeb. Udává se obvykle jako procento zájmové doby, po které musí být systém dostupný ve sjednané kvalitě.

**Odpovědi: 8 Forenzní techniky**

1. Slouží ke shromáždění informací o události nebo incidentu. Základní fáze jsou: shromažďování důkazů, jejich zkoumání, analýza výsledků a přijímání závěrů.
2. Nestálost dat - některá data jsou silně volatilní, jako např. obsah paměti, který se po vyplnutí počítače smaže.
3. Co nás to bude stát, jaké přínosy zavedení organizaci přinese a jaká rizika jsou s nasazením spojena.
4. Jedná se o dva protichůdné zájmy organizace - po dokončení obnovy nebude možné shromáždit jakákoliv další data o incidentu.

Literatura

- [1] 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- [2] Binary Risk Analysis. URL: <http://binary.protect.io/>.
- [3] Common Criteria. URL: <https://www.commoncriteriaportal.org/>.
- [4] Dia draws your structured diagrams: Free Windows, Mac OS X and Linux version of the popular open source program. URL: <http://dia-installer.de/>.
- [5] Draw.io. URL: <https://www.draw.io/>.
- [6] Dropbox. URL: <https://www.dropbox.com/>.
- [7] F01 - Analýza nákladů a přínosů. In *Sourcebook II: Metody a techniky*, pages 388–397. MVČR, Praha. URL: www.mvcr.cz/soubor/analyza-nakladu-a-vynosu-cba-pdf.aspx.
- [8] Google Drive. URL: <https://drive.google.com/>.
- [9] Home :: Bugzilla :: bugzilla.org. URL: <https://www.bugzilla.org/>.
- [10] ISO 27 005 Information technology — Security techniques — Information security risk management.
- [11] ISO 31000 Risk management. URL: <https://www.iso.org/iso-31000-risk-management.html>.
- [12] ISO/IEC 15504 Information technology – Process assessment.
- [13] ISO/IEC 33001:2015 Information technology – Process assessment – Concepts and terminology.
- [14] IT Operations Analytics Change Analytics Configuration Management and Change Management Software | Evolven. URL: <https://www.evolven.com/>.
- [15] Joomla! The CMS Trusted By Millions for their Websites. URL: <https://www.joomla.org/>.
- [16] Main Page - OneCMDB. URL: http://onecmdb.org/wiki/index.php?title=Main_Page.
- [17] Nmap: the Network Mapper - Free Security Scanner. URL: <https://nmap.org/>.
- [18] Secunia Advisory SA51202. URL: <https://secunia.com/advisories/51202/>.
- [19] SmartDraw. URL: <http://www.smartdraw.com/>.
- [20] The Trac Project. URL: <https://trac.edgewall.org/>.
- [21] *IEC 60812 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*. IEC, Ženeva, 2 edition, 2006.
- [22] MindGenius Mind Mapping Software - Special Offer with eLearning courses, August 2012. URL: <http://continuingprofessionaldevelopment.org/mindgenius-mind-mapping-software-special-offer-with-elearning-courses/>.
- [23] Drupal - Open Source CMS, September 2016. URL: <https://www.drupal.org/>.

- [24] FreeMind, 2017. URL: http://freemind.sourceforge.net/wiki/index.php/Main_Page.
- [25] Responsibility assignment matrix, September 2017. Page Version ID: 802846049. URL: https://en.wikipedia.org/w/index.php?title=Responsibility_assignment_matrix&oldid=802846049.
- [26] ITIL Wiki - IT Process Wiki, 2018. URL: https://wiki.en.it-processmaps.com/index.php/Main_Page.
- [27] ČSN EN IEC 31010 ED.2 Management rizik - Techniky posuzování rizik, 2020.
- [28] Home - Freeplane Documentation, 2026. URL: <https://docs.freeplane.org/>.
- [29] Evren Ashdown, Uri Eryurek, Valliappa Gilad, Anita Lakshmanan, and Jessi Kibunguchy-Grant. *Data Governance: The Definitive Guide*. O'Reilly Media, 2021.
- [30] Associated Press. Yahoo punishes CEO Marissa Mayer over hacks that cost firm \$350 million. URL: <http://www.telegraph.co.uk/technology/2017/03/02/yahoo-punishes-ceo-marissa-mayer-hacks-cost-firm-350-million/>.
- [31] Atlassian. JIRA Software - Issue & Project Tracking for Software Teams. URL: <https://www.atlassian.com/software/jira>.
- [32] AXELOS. ITIL. URL: <https://www.axelos.com/best-practice-solutions/itil>.
- [33] AXIS Security Consultants and XiSEC Consultants Ltd. RA2 art of risk V 1.1 :: IT.CS. URL: <http://itcs2.webnode.cz/products/ra2-art-of-risk-v-1-1/>.
- [34] BSI. *Threats Catalogue – Elementary Threats*. BSI, Bonn, 2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.html.
- [35] Nicholas G. Carr. IT Doesn't Matter. *Harvard Business Review*, May 2003. URL: <https://hbr.org/2003/05/it-doesnt-matter>.
- [36] Combodo. ITop: ITIS open source ITIL software. URL: <https://www.combodo.com/itop>.
- [37] Louis Anthony Cox. What's wrong with risk matrices? *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 28(2):497–512, April 2008. doi:10.1111/j.1539-6924.2008.01030.x.
- [38] Kosutic Dejan. Free List of Information security threats and vulnerabilities. URL: <https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/>.
- [39] Flexera Software. Corporate Software Inspector. URL: <https://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/corporate-software-inspector/>.
- [40] Free RW-Soft. Personální audit, SW a HW audit | AW Caesar evidence počítačů, SW a licenci. URL: <http://www.awcaesar.cz/aw-caesar-8>.
- [41] FreeRW Soft. Evidence počítačů, SW, licenci, ITSM, ITIL, SAM. URL: <http://www.awcaesar.cz/>.
- [42] M. Garsox. COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing - An overview, 2013. URL: http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf.
- [43] Gary Hinson. Analog Risk Assessment method, ARA. URL: <http://blog.noticebored.com/2013/08/analog-risk-assessment-method-ara.html>.
- [44] IDG. 2011 State of the CIO Survey.
- [45] IDG. "State of the CIO 2008" Data Shows CIO Salaries, Influence Rising.

- [46] ISACA. COBIT 5 Mapping Exercise for Establishing Enterprise IT Strategy. URL: <http://www.isaca.org/COBIT/focus/Pages/cobit-5-mapping-exercise-for-establishing-enterprise-it-strategy.aspx>.
- [47] ISO27k Implementation Forum. ISMS Implementation and Certification Process v3. URL: http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3.pdf.
- [48] Robert S. Kaplan and David P. Norton. The Balanced Scorecard - Measures That Drive Performance. *Harvard Business Review*, (1):71–79, 1992.
- [49] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang. *NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology, Gaithersburg, 2006. doi:10.6028/NIST.SP.800-86.
- [50] G. L. Kovacich. *Průvodce bezpečnostního pracovníka informačních systémů*. UNIS Publishing, Brno, 2000.
- [51] Fabian Lange. Išikawův fishbone diagram příčin a následků, December 2010. URL: https://commons.wikimedia.org/wiki/File:Ishikawa_Fishbone_Diagram_cz.svg.
- [52] Metacomet. Paretův graf, March 2006. URL: <https://commons.wikimedia.org/wiki/File:Pareto.PNG>.
- [53] Microsoft. Microsoft Baseline Security Analyzer 2.3 (for IT Professionals). URL: <https://www.microsoft.com/en-us/download/details.aspx?id=7558>.
- [54] Microsoft. Přehled služby Microsoft Intune. URL: <https://www.microsoft.com/cs-cz/cloud-platform/microsoft-intune>.
- [55] Kevin Mitnick and Wiliam L. Simon. *Umění klamu*. HELION, Praha, 2003.
- [56] Kevin D. Mitnick and William L. Simon. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley, Indianapolis, IN, 60282nd edition edition, December 2005.
- [57] MKLab. StarUML 2. URL: <http://staruml.io/>.
- [58] Moodle. Moodle project dashboard. URL: <http://tracker.moodle.org/browse/MDL>.
- [59] J. Nenadál. *Měření v systémech managementu jakosti*. Management Press, Praha, 2 edition, 2004.
- [60] J. Nenadál, D. NOSKIEVIČOVÁ, R. PETŘÍKOVÁ, J. PLURA, and J. TOŠENOVSKÝ. *Moderní management jakosti*. Management Press, Praha, 2008.
- [61] NIST. *NIST SP 800-30 Guide for Conducting Risk Assessments*. NIST, Washington, 2012. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- [62] OMG. UML 2.5. URL: <http://www.omg.org/spec/UML/2.5/>.
- [63] Qualys. Vulnerability Management. URL: <https://www.qualys.com/suite/vulnerability-management/>.
- [64] Rapid 7. Nexpose - Your on-prem vulnerability scanner. URL: <https://www.rapid7.com/products/nexpose/>.
- [65] SANS Institute. Cybersecurity Policies and Standards, 2026. URL: <https://www.sans.org/information-security-policy>.
- [66] Joseph Schmuller. *Myslíme v jazyku UML: knihovna programátora*. Grada, Praha, 2001. Google-Books-ID: TUZTywAACAAJ.
- [67] Tony Thirlwell and John Blunden. *Mastering Risk Management*. O'Reilly Media, 2022.

- [68] Philip Thomas, Reidar B. Bratvold, and J. Eric Bickel. The Risk of Using Risk Matrices. *SPE Economics & Management*, 6(02):56–66, March 2014. doi:10.2118/166269-PA.
- [69] Martyn Williams. PlayStation Network hack will cost Sony \$170m. URL: <http://www.computerworld.com/article/2508315/computer-hardware/playstation-network-hack-will-cost-sony--170m.html>.
- [70] Česko. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). *Sbírka zákonů ČR*, 2000(36), 2000.
- [71] ČSN. Čsn en 61025 analýza stromu poruchových stavů (fta).
- [72] ČSN. Čsn en 6205 techniky analýzy spolehlivosti - analýza stromu událostí (eta).
- [73] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 1: Obecné principy.
- [74] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 3: Hmotné škody na stavbách a ohrožení života.
- [75] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 4: Elektrické a elektronické systémy ve stavbách.
- [76] ČSN. Čsn en 62305-2 ed. 2 ochrana před bleskem - Část 2: Řízení rizika.
- [77] Pavel Šenovský. *Bezpečnostní informatika II*. VŠB-TU Ostrava, Ostrava, 5 edition, 2012. URL: <http://prometheus.vsb.cz>.
- [78] Pavel Šenovský. *Modelování rozhodovacích procesů*. VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 4 edition, 2015. URL: http://home1.vsb.cz/~sen76/CMS/data/uploads/skripta/modelovyni_4vydani_upravene.pdf.
- [79] Pavel Šenovský. *Počítačové sítě a ochrana dat*. VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2 edition, 2023. URL: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/pc_ochr_dat_2vyd.pdf.
- [80] Pavel Šenovský. *Bezpečnostní informatika 1*. VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 11 edition, 2025. URL: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/bi1_11vyd.pdf.
- [81] Pavel Šenovský. *Bezpečnostní informatika 3*. VŠB-TU Ostrava, Ostrava, 6 edition, 2026. URL: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/bi3_6ed.pdf.
- [82] Pavel Šenovský. *Umělá inteligence v bezpečnosti*. VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 3 edition, 2026. URL: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/ai_3vyd.pdf.
- [83] Pavel Šenovský. *Šablony systému řízení bezpečnosti informací*. VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2026. URL: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/%C5%A0ablony_syst%C3%A9mu_%C5%99%C3%ADzen%C3%AD_bezpe%C4%8Dnosti_informac%C3%AD.pdf.

Seznam zkratk

- AD** Active Directory. 66, 67, 144
- ARA** Analog Risk Assessment Method. 87, 88, 144
- AUP** Acceptable Use Policy. 51, 144
- B2B** Business to Business. 39, 144
- BI** Bezpečnostní inženýrství. 9, 144
- BIA** Business Impact Analysis. 41, 144
- BPL** Bezpečnostní plánování. 9, 144
- BRA** Binary Risk Analysis. 85, 88, 144
- BSC** Balance Score Cards. 114, 120, 144
- BYOD** Bring Your Own Device. 50, 52, 144
- CASE** Computer Aided System Engineering. 66, 144
- CBA** Cost-Benefit Analysis. 83, 144
- CCTA** Central Computer and Telecommunication Agency. 122, 144
- CEO** Chief Executive Officer. 18, 19, 144
- CERT** Computer Emergency Response Team. 18, 144
- CFO** Chief Financial Officer. 18, 19, 144
- CIO** Chief Information Officer. 5, 18–20, 32, 134, 144
- CISO** Chief Information Security Officer. 18–20, 32, 45, 134, 144
- CIT** Centrum informačních technologií. 32, 144
- CMDB** Configuration Management Database. 67–70, 73, 74, 144
- CMS** Content Management System. 30, 48, 144
- COBIT** Control Objectives for Information and Related Technologies. 111, 144
- COO** Chief Operation Officer. 18, 19, 144
- CSIRT** Computer Security Incident Response Team. 18, 144
- CSO** Chief Security Officer. 18–20, 32, 34, 134, 144
- CTO** Chief Technological Officer. 18, 34, 144
- DMS** Document Management System. 30, 144

- EAL** Evaluation Assurance Level. 14, 144
- EPS** elektrická požární signalizace. 17, 144
- ERP** Enterprise Resource Planning. 64, 144
- ETA** Event Tree Analysis. 57, 60, 144
- FMEA** Failure Mode and Effect Analysis. 91–93, 144
- FTA** Fault Tree Analysis. 57, 60, 144
- GEIT** Governance of Enterprise IT. 113, 144
- GRC** Governance, Risk and Compliance. 19, 144
- HIM** hmotný investiční majetek. 64, 144
- HRA** Human Reliability Analysis. 57, 144
- IA** information assurance. 18, 144
- ICS** Industrial Control System. 111, 144
- IDM** identity management. 18, 48, 67, 72, 144
- IDS** Intruder Detection System. 17, 19, 125, 144
- IFB** Inženýrství fyzické bezpečnosti. 9, 144
- IoT** Internet of Things. 50, 52, 144
- IP** Intellectual Property. 58, 144
- IPS** Intruder Prevention System. 17, 19, 125, 144
- ISACA** Information Systems Audit and Control Association. 111, 144
- ISMS** Information Security Management System. 5, 9, 11, 12, 15–17, 40–45, 48, 68, 82, 84, 124, 144
- ISOC** Information Security Operations Center. 18, 19, 144
- ISP** Internet Service Provider. 14, 144
- IT** Informační technologie. 144
- ITIL** IT Infrastructure Library. 12, 121, 144
- ITSM** IT Service Management. 74, 144
- LDAP** Lightweight Directory Access Protocol. 67, 144
- LRC** Linear Responsibility Chart. 116, 144
- MCA** Multi-Criteria Analysis. 83, 144
- MDA** Model Driven Approach. 64, 144
- MTBF** Mean Time Between Failures. 56, 144
- NBU** Národní bezpečnostní úřad. 46, 144
- NDA** Non-Disclosure Agreement. 52, 144
- NIM** nehmotný investiční majetek. 64, 144

- OMG** Object Management Group. 64, 144
- PCS** poskytovatel certifikačních služeb. 14, 144
- PDCA** Plan Do Check Act. 40, 43, 144
- PSN** PlayStation Network. 82, 144
- RACI** Responsible Accountable Consulted Informed. 49, 144
- RAKOS** Rada pro koordinaci a strategii ICT. 5, 32, 33, 144
- RRIT** Rada pro rozvoj informačních technologií. 5, 32, 33, 144
- RTP** Risk Treatment Plan. 15, 40, 42, 56, 57, 144
- SCM** Supply Chain Management. 144
- SIEM** Security Information and Event Management. 144
- SLA** Service Level Agreement. 51, 52, 123, 144
- SOA** Statement of Applicability. 15, 40, 42, 46, 144
- SŘBI** Systém řízení bezpečnosti informací. 15, 144
- TBOM** Technická bezpečnost osob a majetku. 144
- TDD** Test Driven Development. 144
- UAC** User Access Control. 26, 144
- UML** Unified Modeling Language. 64, 66, 144
- USD** Unified States Dollar. 144
- UTM** Unified Threat Management. 144
- VLE** Virtual Learning Environment. 30, 144

Rejstřík

aktivum

- podpůrné, 15, 64
- primární, 15, 64

analýza rizik

- Attack Tree, 57
- CARVER, 89
- diagram příčin a následků, 90
- ETA, 57
- FMEA, 91
- FTA, 57
- Ishikawův diagram, 90
- myšlenková mapa, 90
- Paretův graf, 91

analýza rizika

- ARA, 87
- BRA, 85

apetit k riziku, 42

architekt KB, 45

audit

- externí, 35
- interní, 34

auditor, 45

Balance Score Cards, 114

bezpečnostní dokumentace

- metodika, 23
- podpůrné, 23
- politika, 23
- postup, 23
- pracovní instrukce, 23
- procedura, 23
- směrnice, 23
- záznamy, 23

bezpečnostní incident, 127

bezpečnostní politika, 47

bezpečností incident, 82

BIA, 41

BSC, 114

bug hunting program, 55

CBA, 83

CERT, 18

ChatGPT, 53

CMDB, 69

COBIT, 111

COBIT 2019, 112

Common criteria, 14

cost-benefit analýza, 83

CSIRT, 18

data governance, 52

dokumentace

- monolitická, 24

dokumentované informace

- uchovávané, 23
- udržované, 23

doména COBIT, 115

ERP, 64

exploit, 55

faktor

- kontextový, 113
- strategický, 113
- taktický, 113

forenzní proces, 130

forenzní techniky, 129

garant

- aktiva, 84

garant aktiva, 68

governance, 114

hrozba, 54

identifikace rizik, 54, 83

IDM, 18

incident, 125, 127

incident handler, 130

informační aktivum, 15, 64

inventarizace informačních aktiv, 42

ISACA, 111

ISMS, 15, 40

ISMS rozsah, 41

ISO 15504, 118

ISO 27000, 37

ISO 27002, 44

ISO 27005, 83

ISOC centrum, 18

ISP, 14

IT profesionál, 130

ITIL, 121

kaskáda cílů, 113

klíčové bezpečnostní role, 45

koncept bezpečnosti organizace, 13

kontext bezpečnosti, 15

- kontrola, 46
- kódovací agent, 53
- licence, 74
- majetek
 - HIM, 64
 - NIM, 64
- management, 114
 - CIO, 19
 - CISO, 18
 - COO, 19
 - CSO, 19
- management aktiv, 67
- management změn, 73
- management zranitelností, 76
- matice rizik, 58, 93
- MCA, 83
- mise, 21
- model dospělosti, 118, 125
- multikriteriální analýza, 83
- návrh služeb, 123
- obnova, 128
- oddělení
 - bezpečnost IT, 17
 - technická bezpečnost, 17
- organizace
 - oddělení IT, 16
- organizační struktura, 16
- PDCA, 43
- plán na vypořádání se s rizikem, 56
- Plán zvládání rizik, 42
- plánování
 - dlouhodobé, 20
 - krátkodobé, 20
 - střednědobé, 20
- plány, 15
 - havarijní, 15
 - kontinuity, 15
 - obnovy, 15
- policy first, 46
- politika
 - AI, 53
 - BYOD, 52
 - cloudové služby, 51
 - IoT, 52
 - malware, 51
 - sociálních médií, 50
 - zpracování dat, 52
- politika ISMS, 44
- Politika systému ISMS, 42
- postranní kanál, 57
- pravděpodobnost, 82
- princip
 - adresná zodpovědnost, 29
 - aktuálnost, 31
 - integrity, 30
 - znalost, 29
 - úměrnost, 31
- princip úměrnosti, 131
- Prohlášení o aplikovatelnosti, 42, 46
- projekt, 22
- průběžné zlepšování služeb, 125
- přechod služeb, 124
- přístup
 - liberální, 27
 - paranoidní, 28
 - promiskuitní, 27
 - racionální, 28
- RACI, 49, 116
- role, 48
- rozsah ISMS, 44
- RTP, 42, 56
- shromáždění důkazů, 128
- SLA, 123
- služba, 122
- smyčka, 53
- SOA, 42
- sociální inženýrství, 16
- správa licencí, 73
- správce software, 74
- stakeholder, 113
- strategie služeb, 122
- systém reakce na incident, 127
- Systémy řízení bezpečnosti informací, 15
- SRBI, 15
- událost, 125
- UML, 66
 - actor, 65
 - asociace, 65
 - diagram aktivit, 66
 - komponenta, 66
 - případy užití, 66
 - třídní diagram, 66
 - uzel, 66
- vize, 21
- vlastník, 68
 - rizika, 84
- vnitropodniková kultura, 15, 16
- vyšetřovatel, 130
- Výbor kybernetické bezpečnosti, 32
- world model, 53
- zero day vulnerability, 55
- zranitelnost, 54
- zranitelnost nultého dne, 55
- závazek vedení, 41
- řízená dokumentace, 41

řízení změn, 20

škody

 nepřímé, 40

 přímé, 40