VŠB - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

doc. Ing. Pavel Šenovský, Ph.D.

Bezpečnost informačních systémů

skripta
1. vydání

Ostrava, 2017

Bezpečnost informačních systémů
1. vydání
tento text neprošel jazykovou úpravou

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obsah

Seznam obrázků

Seznam tabulek

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 Technická bezpečnost osob a majetku (TBOM).

Tato skripta se zaměřují především na oblast systémů řízení informační bezpečnosti (ISMS). Z tohoto pohledu tato skripta logicky navazují na předměty *Bezpečnostní informatika II* a *Počítačové sítě a ochrana dat*. Pokud jste tyto předměty 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 skripta 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 TBOM 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, naštěstí 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 zasluhovaly, 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 skripta 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 skript.

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 zpříjemnění 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.

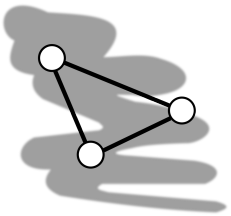
Vysvětlení, definice, poznámka
U této ikony najdete vysvětlující text, poznámku k probíranému tématu, která problém uvede do širších souvislostí, popřípadě důležitou definice.

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.

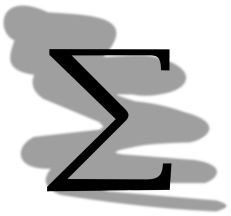
Příklad
Příklady obsahují praktické demonstrace diskutovaného problému.

Na konec skript naleznete 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.



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



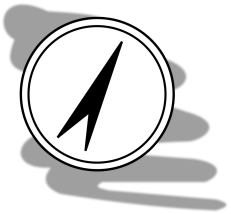
Shrnutí
Obsahuje základní myšlenky kapitoly, kterým by měl být věnována zvláštní pozornost během studia.

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

doc. Ing. Pavel Šenovský, Ph.D.

Kapitola 1

Systémy řízení informační bezpečnosti



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

Po přečtení této kapitoly budete
Znát

- základní pojmy z oblasti procesní bezpečnosti IT
- souvislost mezi bezpečností a kulturou organizace

Umět

- rozčlenit bezpečnostní politiky do kategorií

Čas nutný ke studiu
Pro prostudování této kapitoly budete potřebovat přibližně 4 hod.

1.1 Bezpečnostní dokumentace

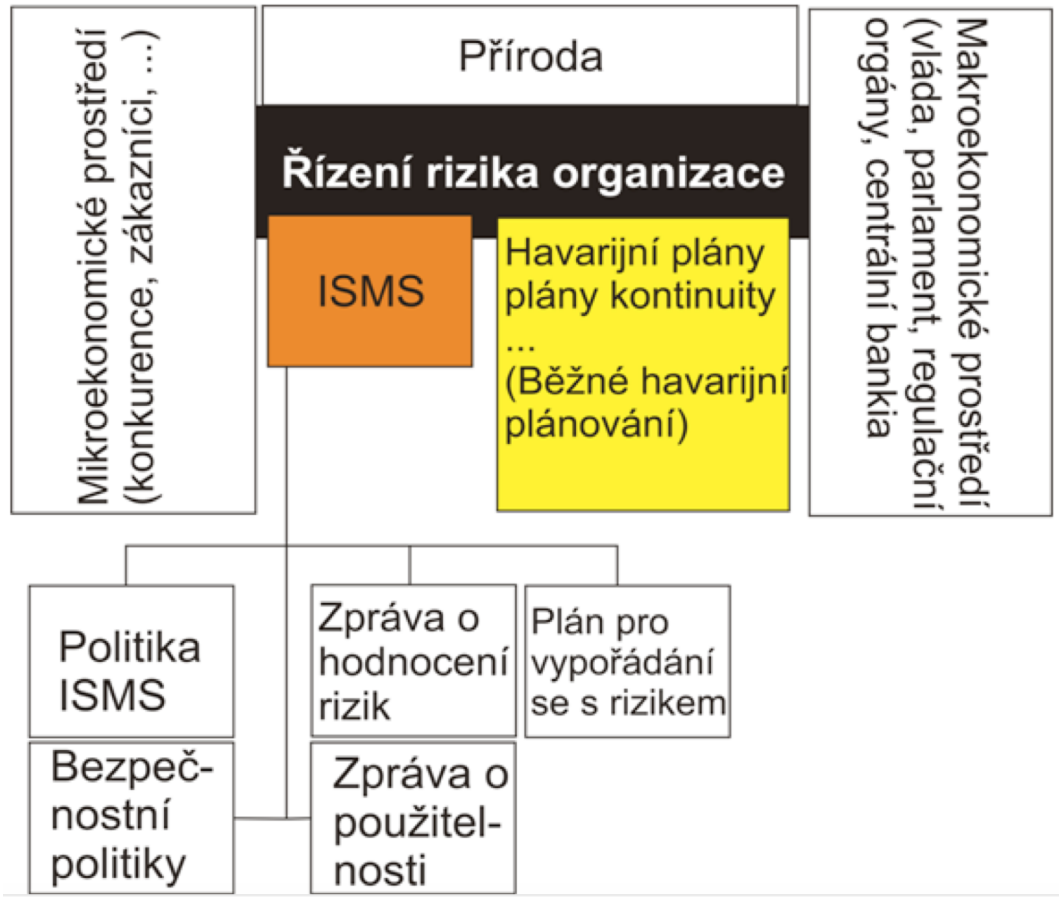
Nepochybně se shodneme na tom, že bezpečnostní aspekty práce s IT organizace je potřeba řídit. Je přitom lhostejné, v jakém oboru organizace působí, jestli se jedná o výrobní nebo nevýrobní podnik, nebo třeba orgán státní správy. V případě, že bezpečnostním hrozbám čelíme pouze realizací náhodně vybraných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

Jediným řešením je proto zavedení celého komplexu postupů, opatření, které jsou pevně zakotveny v bezpečnostní dokumentaci organizace a v ideálním případě jsou navázány na další oblasti mající návaznost na bezpečnost.

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.

Organizace svojí místní lokalizací (např. polohou poboček) je vystavena lokálním hrozbám přírodního (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 nelze realizovat v krátkém časovém horizontu, pokud se s touto možností předem nepočítalo).



Obrázek 1.1: Celková koncepce bezpečnosti organizace

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. 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, plánky 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. Jedná se o ucelený filozofický přístup pro řízení bezpečnosti veškerých citlivých in formací bez ohledu na to kde a v jaké formě se nacházejí. Z tohoto důvodu předmětem zájmu jsou jednak IT aktiva, jednak informace uchovávané v listinné podobě a další.

Aktivem IT přitom rozumíme veškeré prostředky výpočetní techniky, které pro danou organizaci mají cenu (přinášejí jí užitek). Mezi IT aktiva tak budou spadat jednak informační systémy (IS) v jejich nejširší podobě, jednak to mohou být třeba aktivní síťové prvky.

Podrobnější informace o informačních systémech můžete nalézt ve skriptech Bezpečnostní informatika II [68]. Základní informace o aktivních síťových prvcích a jejich funkcích můžete nalézt ve skriptech Počítače a ochrana dat [70].

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

1. politiku ISMS
2. zpráva o hodnocení rizik
3. plán pro vypořádání se s rizikem
4. bezpečnostní politiky
5. zpráva o použitelnosti

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. 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 IT aktivum, uveďte alespoň tři příklady IT aktiva.
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 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 obratným sociálním inženýrem, aby donutil své objeti ke spolupráci.

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, které mají alespoň do určité míry vyřešenou centralizaci svých IT služeb.

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 ošetřovaní 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 proškolování 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. proškolování 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 historické nutnosti (vznikla potřeba něco vyřešit) a často je způsobena lidským faktorem: stávající útvar pod daným vedoucím není schopen nebo ochoten čelit novým výzvám, kterým je vystaven a z nějakého důvodu tohoto vedoucího není možné vyměnit – problém se tedy vyřeší jinak a vznikne odchylka, která pro danou organizaci v daném časovém okamžiku dává smysl. Tato odchylka, ale v organizaci zůstává trvale a s postupem času se přidávají další větší, či menší odchylky.

Ve finále lze říci, že žádné dvě společnosti nejsou stejné. Obecná zkušenost z provozu ISMS tak může být přenositelná mezi různými organizacemi, zároveň ale musí být přizpůsobena 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 informační bezpečnosti a jejím systematickém řešení hovoříme až v několika posledních letech. Do té doby se všeobecně předpokládalo, že k řešení IT bezpečnosti postačuje pořízení, instalace a údržba antivirového software a běžná údržba IT aktiv.

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 informační bezpečnosti, 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 fyzickou 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 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 na stejné úrovni jako ředitel (Chief Executive Officer (CEO)), finanční ředitel (Chief Financial Officer (CFO)) a další ředitelé). CISO by měl mít přístup do nejvyšších pater řízení organizace tak, aby měl možnost pracovat napříč organizací, což odpovídá povaze organizace bezpečnosti, která taktéž musí být dodržována napříč celou organizací. Mezi povinnosti CISO patří:

- 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 informační bezpečnosti
- 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 reálu 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 skripta Bezpečnostní informatika 2 [68]).

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 správu 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 uživatelích do provozovaných systémů organizace, v potřebném rozsahu.

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. Shromažďují 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).

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 [38]. 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 [39].

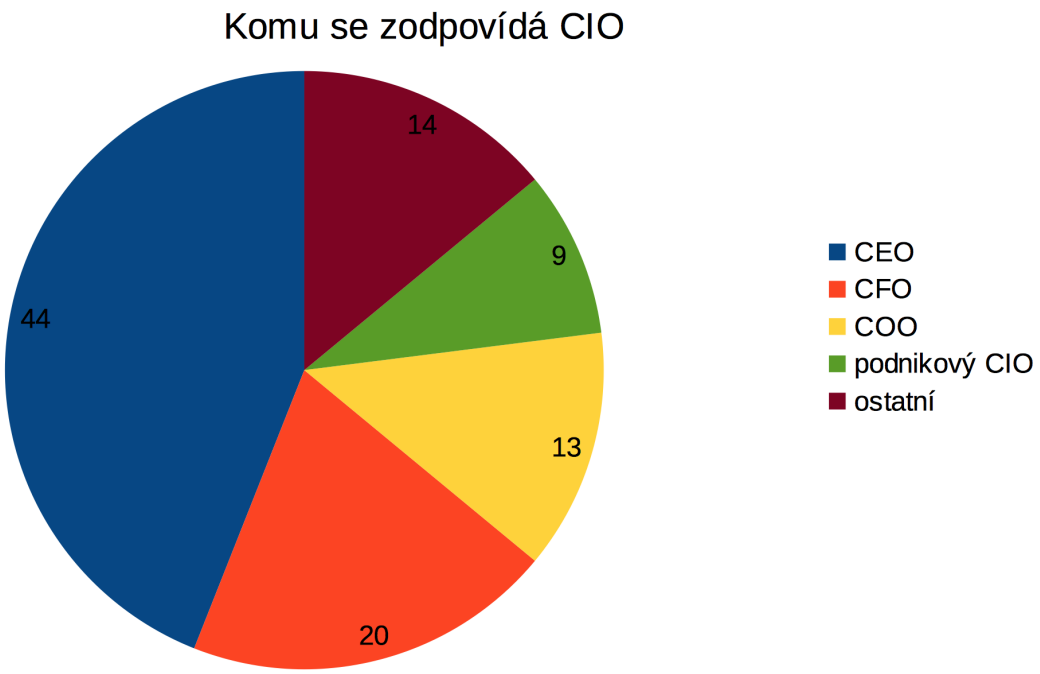
Zdaleka největší podíl přímé podřízenosti připadá na CEO (44 %) a teprve daleko za ním je podřízenost pod CFO (20 %).

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 bezpečnost IT (spojení s funkcí CISO). Na druhou stranu funkce CSO a CIO se prakticky nepřekrývají a proto ke slučování funkcí CIO a CSO 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 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,



Obrázek 1.3: Komu se zodpovídá CIO (data: průzkum [38])

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.

Kontrolní otázky

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 měli vůbec 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 (pro dlouhodobější plány) a umožňuje organizaci efektivně mobilizovat zdroje pro zajištění běžných funkcí organizace.

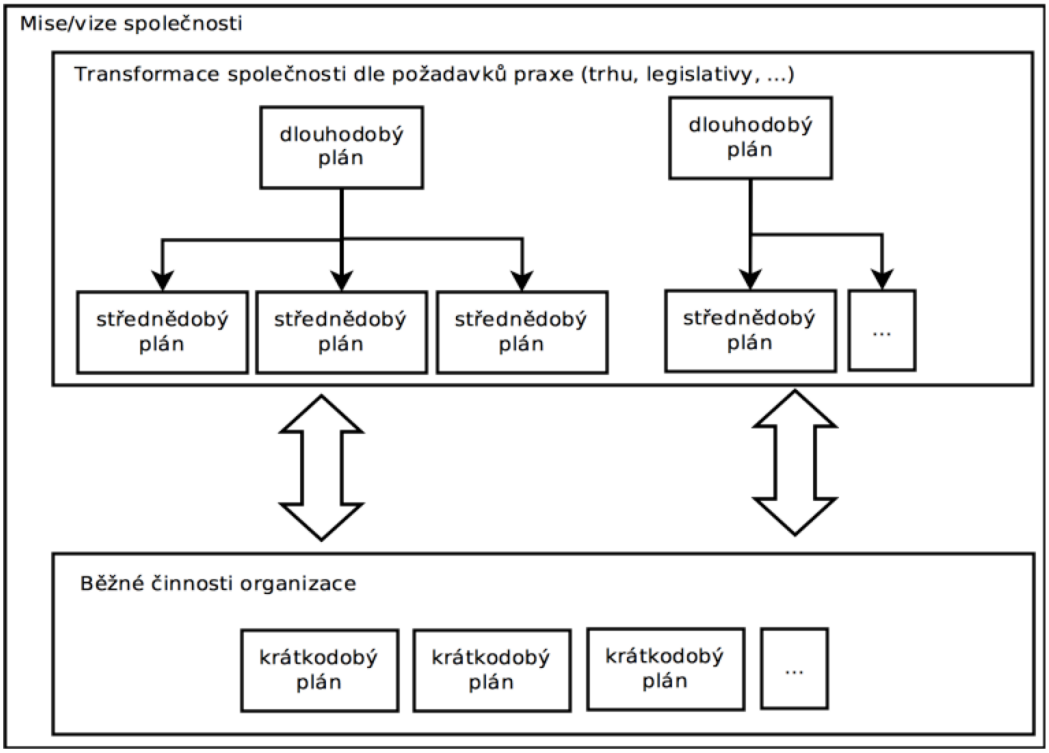
Dlouhodobé plány tedy stanovují dlouhodobé cíle a také způsoby jejich dosažení. Výsledkem realizace dlouhodobých plánů jsou tak mohou být rozsáhlé změny v organizačních strukturách, nasazení nových technologií nebo systémů, fúze s jinou společností apod. Dlouhodobé plány proto mají své

dopady i do oblasti bezpečnosti, protože tyto zásadní změny je potřeba zabezpečit tak, aby s jejich realizací nebyla spojena nepřiměřená rizika.

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 sepsán 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.*

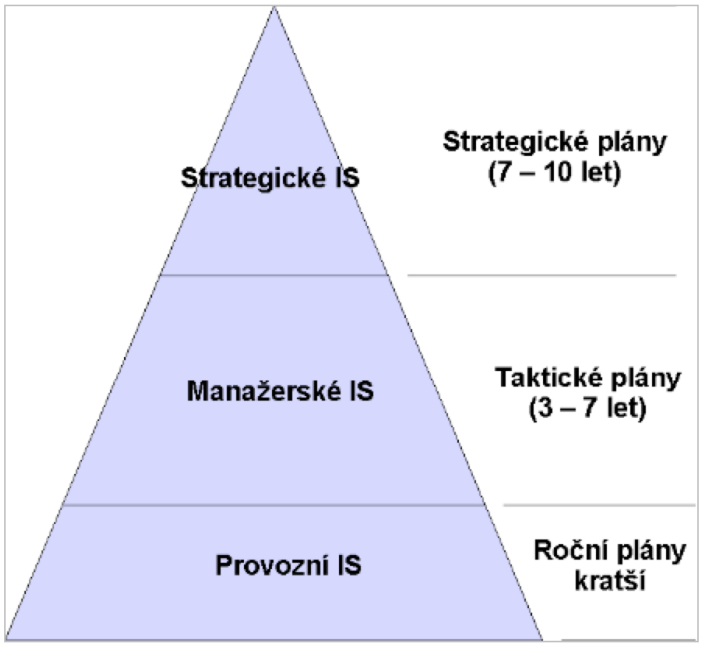
Z hlediska časového, tedy na jak dlouhý časový horizont je zaměřeno dlouhodobé, střednědobé a krátkodobé plánování, neexistuje jednoznačná odpověď. Plánovací horizont si jednotlivé organizace určují samy pro sebe na základě poznatků o fungování prostředí, ve kterém musí organizace působit.

Obecně platí, že plánovací horizont je delší v oborech, kde jsou inovace spojovány s nutnosti 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 [68])

Kontrolní otázky

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* [69] 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.

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 výji-

mečné, 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.

Jako příklady projektů IT bychom mohli uvést např. následující:

- pořízení nového IS
- sloučení datových základen informačních při fúzi společností
- zavádění nové majoritní verze informačního systému, programu nebo operačního systému, apod.

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.

Pojmenování, ale také forma této dokumentace je přitom závislá čistě na vnitropodnikové kultuře. Vnitropodniková kultura ovlivňuje zejména:

- pojmenování jednotlivých dokumentů
- jejich organizaci (např. v kolika dokumentech bude problém řešen)
- ve stanovení 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. 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 často formální bezpečnostní dokumentace IT vůbec nezpracovává.

Druhým extrémem je systém, kdy každé IT aktivum má svůj bezpečnostní dokument. Ani k tomuto systému se většinou nepřikláníme. V zájmu zvýšení efektivity se spíše snažíme identifikovat podobná IT aktiva v majetku organizace a tato 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 (její údržba stojí menší finanční prostředky). Pozitivní efekt lze vysledovat také v nákladech na provoz zařízení samotných.

1.3.3 Formálnost vs schvalovací proces

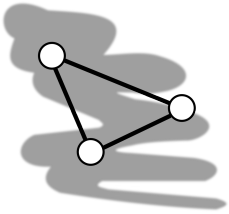
Konečně se dostáváme k *formálnosti dokumentace*. Přístup k tvorbě dokumentace může být výrazně rozdílný právě v této oblasti. Obvykle se s bezpečnostní dokumentací začíná v čistě neformální rovině. Bezpečnostní opatření v takovém případě nejsou psaná nebo jsou psána neformálním jazykem jako určitá doporučení,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

Kontrolní otázky

1. Co je to projekt?
2. Jak se liší provozní a projektová bezpečnostní dokumentace?
3. Co rozumíme monolitickou dokumentací?
4. Vysvětlete výhody a nevýhody koncentrace dokumentace?

Seznamování s dokumentací pak probíhá také neformálně, vetšinou 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 jsou 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 řízené dokumentace a oblast řízení bezpečnosti 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. 1.6.

Bezpečnostní dokumentace nejen IT by tedy neměla být mrtvým cárem papíru, ale měl by odrážet aktuální obraz práce s riziky v oblasti IT v daném časovém okamžiku. Bezpečnost je z tohoto pohledu pouze jedním z nástrojů, které dané organizace používá pro dosažení svých cílů. Bezpečnost tedy obvykle sama o sobě není cílem dané organizace.

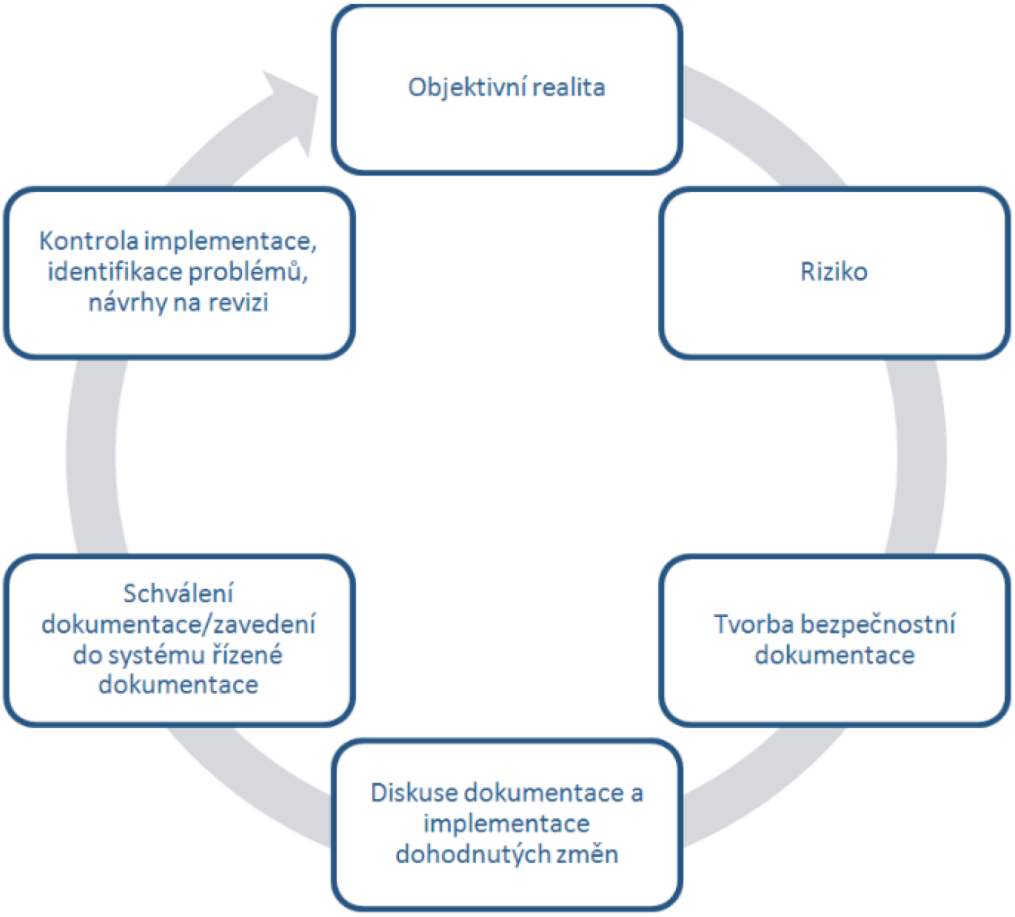
Připomeňme si základní cíl organizace je definován v misi organizace a tam obvykle nejsou formulace typu: firma ABC má ambice využívat nejzabezpečenější informační systém. Zabezpečení je pouze funkcí, která umožnit naplnění cíle, za kterým daný informační systém nasazujeme.

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 nepřímo úměrné výši zabezpečení.

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

V praxi toto můžeme ilustrovat třeba pro operační systém Windows 7 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.



Obrázek 1.6: Proces tvorby, schvalování a revize bezpečnostní dokumentace

Kontrolní otázky

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.

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.

Z hlediska restriktivnosti rozlišujeme čtyři stupně[1]:

- 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.

[1] V předmětech Bezpečnostní informatika 2 [68] a Počítačové sítě a ochrana dat [70] 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 šířeji, a proto spíše používám pojmy jako bezpečnostní dokumentace nebo přístup (např. liberální přístup).

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.

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) od subjektů systému (uživatelé). Jinými slovy toto znamená, že vytváříme databázi uživatelů a jejich rolí.

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 zabezpečí? 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 popsatelná 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. Odstraněná funkčnost 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 případě obzvláště citlivých IT aktiv. V ostatních případech je preferován především racionální přístup.

Volba přístupu k zabezpečení

Organizace obvykle provozují celou řadu IT aktiv pracujícími 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. 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?

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.

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 (vymahatelná) 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 dostát. 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 levná. 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 odseděl 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 různé 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.

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.

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

V literatuře (např. [43]) lze najít ještě řadu dalších principů, které se doporučuje dodržovat, ale vzhledem k omezenému prostoru se tady jimi zabývat nebudu.

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.

Čas nutný ke studiu

1. Vyjmenujte alespoň tři principy, kterými se řídí tvorba bezpečnostní dokumentace.
2. Vysvětlete 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 oproštěný 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.

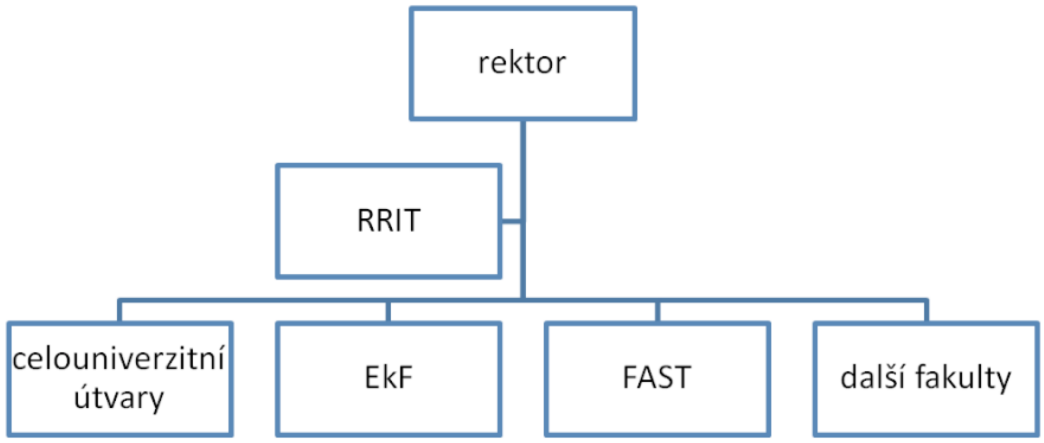
CISO, ale vše nezvládne sám. Jelikož jeho vzdělání je obvykle specificky zaměřené na oblast bezpečnosti, popřípadě IT nemusí (a také obvykle není) CISO odborníkem v oboru, ve kterém organizace působí. Z tohoto důvodu není CISO sám (a se svými podřízenými) schopen sestavit bezpečnostní dokumentaci tak, 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. Z názvů, které se nabízejí s ohledem na vykonávané funkce bychom mohli vybrat: Rada pro IT, Poradní orgán IT, Platforma pro rozvoj IT, Bezpečnostní výbor IT, apod. Se jmény můžeme být samozřejmě také kreativnější, např. VŠB – TU Ostrava svého času zřídila k tomuto účelu (a některým dalším účelům) orgán RRIT , aby ji později nahradila skupinou RAKOS. Pro účely těchto skript budeme označovat takovou platformu jako *Rada pro IT*.

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. 1.7.

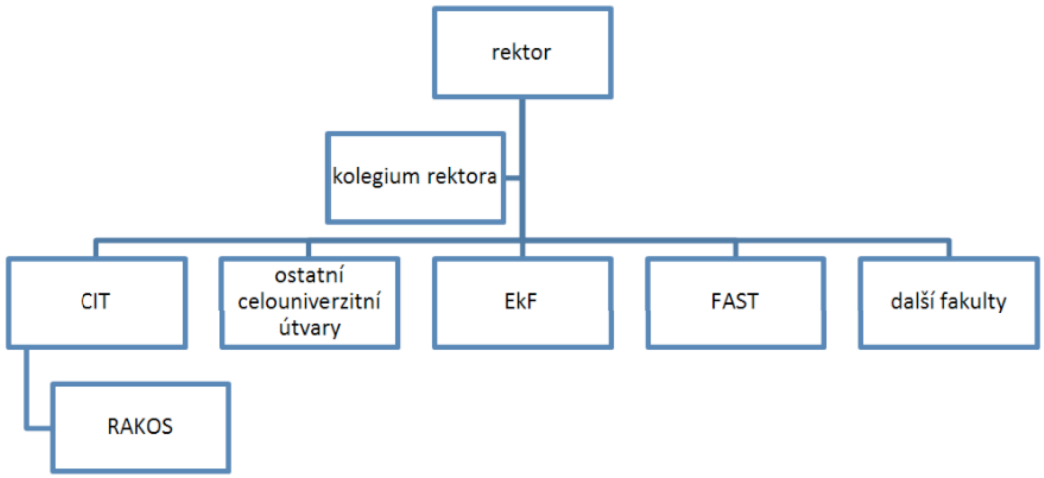


pozn: Ekonomická fakulta (EkF)
Stavební fakulta (FAST)

Obrázek 1.7: Organizační začlenění RRIT

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. 1.8.



Obrázek 1.8: Organizační začlenění RAKOS

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.

K činnostem rady IT může patřit např.:

- 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

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].

[a] V tomto předmětu předpokládáme potřebu vést vnitropodnikovou dokumentaci (tedy nutnost formálně řídit bezpečnost IT).

- tvorba strategie rozvoje IT
- a další.

Aby Rada mohla fungovat, musí být 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 auditoři potřebují čas pro seznámení se s bezpečnostní situací organizace

- je finančně náročnější – audit je dodáván jako služba externí firmou a je proto patřičně zpoplatněn.
- auditoři 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 auditoři 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. Takové nástroje 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 měla schválit, popř. vzít na vědomí Rada pro IT. S výsledky auditů by se mělo dále pracovat zejména pokud byly nalezeny neshody mezi nastavením jednotlivých procesů a jejich skutečnou implementací. Tedy výsledky auditu by měly posloužit jako jeden z podkladů pro provedení revize bezpečnostní dokumentace, popřípadě dalších vnitropodnikových norem.

Kontrolní otázky

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 srovnáním s externím nemůže provést?
4. Jako jsou úkoly CISO?
5. Jaké jsou úkoly rady IT?
6. Jaké jsou úkoly administrátora IT aktiva?

Kapitola 2

ISO 27000

Průvodce studiem
V této kapitole se podívané 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

Čas nutný ke studiu
Pro prostudování této kapitoly budete potřebovat přibližně 2 hod.

ISO 27000 je kodex norem, který je zaměřen na systémové řízení informační bezpečnosti. 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 29.3.2017). 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 27015 Information technology - Security techniques - Information security management guidelines for financial services
- 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 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 protiopatření, 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 27035:2011 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 Busines (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 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002

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 bezpečnosti 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 - 3 roky. Většina revizí se ale omezuje na drobnější opravy a změny - tedy základní filozofie norem zůstává nezměněna.

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).

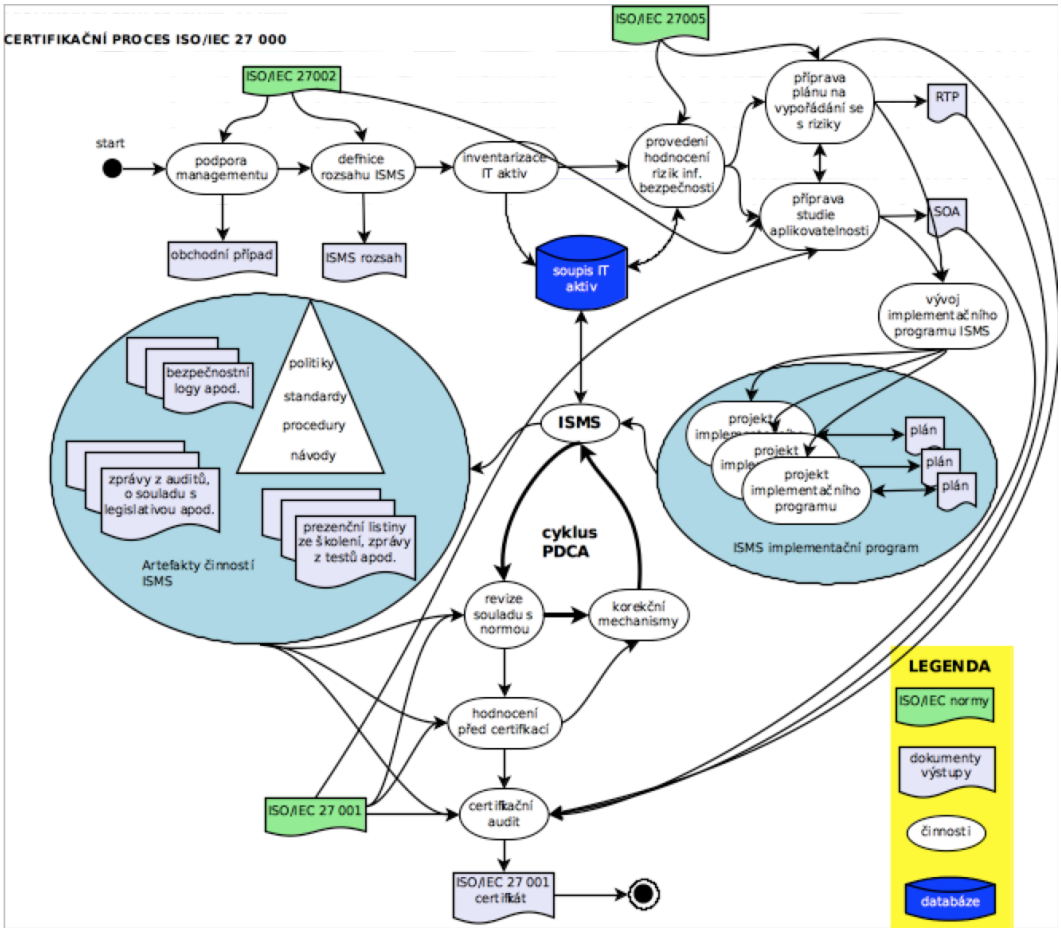
Filozoficky je koncept ISO 27000 založen na byrokratickém způsobu řízení, tedy svým způsobem se jedná o „papírovou válku“ podobně jako v případě systémů řízení jakosti dle ISO 9 000 (viz předmět Řízení jakosti I nebo literatura [52, 53]) a jako takový je v některých případech problém zajistit promítnutí se nastavení procesů do praktického způsobu, jakým jsou procesy vykonávány - tedy zajištění, aby řízení informační bezpečnosti (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 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.

Selhání při řízení informační bezpečnosti ale může vést k uniku citlivých informací, nebo dokonce přímého narušení poskytované služby. Následky tak mohou být velmi silné s prakticky okamžitým

nástupem. Tlak na dobře funkční systém řízení informační bezpečnosti je proto větší.

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



Obrázek 2.1: Certifikační proces ISMS (adaptováno z [41])

Na obr. 2.1 znamená:

- Plan Do Check Act (PDCA) - Naplánuj, proveď, zkontroluj, oprav
- Study of Applicability (SOA) - studie aplikovatelnosti
- Risk Treatment Plan (RTP) - plán na vypořádání se s riziky

Všimněte si, že celý proces přípravy organizace na zavedení systému ISMS a jeho následná certifikace podléhá několika 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

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).

Rozhodnutí o zavedení ISMS je rozhodnutím manažerským, které má své dopady na fungování celé organizace. Každé manažerské rozhodnutí přitom musí být odůvodněno ekonomicky. Se zavedením každého systému řízení jsou totiž spojeny poměrně rozsáhlé transformační náklady (provedení analýz, vytvoření potřebné dokumentace, prvotní proškolení uživatelů a interních auditorů, náklady na certifikaci apod.) a také jsou s ním spojeny určité náklady na provoz systému (provádění periodických auditů, revizí bezpečnostní dokumentace apod.).

Přínosy zavedení je vyčíslit náročnější, totiž jak moc je ekonomicky výhodné udržení informací vedených v dané organizaci v bezpečí. Intuitivně se nabízí odpověď, že je to velmi výhodné, ale co

to přesně znamená pokud to porovnáme s explicitně vyčíslenými prostředky nutnými na zavedení a udržení systému ISMS?

Pro tyto účely se zpracovává případová studie. Z praktických důvodu (částečně naznačených výše) se při zpracování takové stude spíše zaměřujeme na vyčíslováni škod, které by mohly (s určitou pravděpodobností) nastat, pokud bychom systém ISMS ve zvoleném rozsahu neimplementovali. Do nákladů můžeme zařadit třeba pokuty za únik osobních údajů, poškození dobrého jména, kompenzace koncovým zákazníků a další.

Některé typy škod souvisí s předmětem podnikání a nejsou tak obecně použitelné - např. vyčíslení rizika ztráty licence na poskytování telekomunikačních služeb. Existuje také celá řada dalších scénářů, o kterých lze v souvislosti s narušením informační bezpečnosti uvažovat – zneužití infrastruktury pro provádění dalších útoků, narušení poskytování IT služeb a v důsledku toho neschopnost organizace vykonávat své běžné činnosti, apod.

Rozhodnutí o zavedení systému ISMS je rozhodnutím velmi závažným, proto o něm musí existovat zápis nebo je možné toto zajistit pomocí obecného vnitropodnikového předpisu, kterým se daná organizace přihlásí k řízení informační bezpečnosti pomocí ISMS.

ISMS jako byrokratický systém funguje obvykle v systému řízené dokumentace. Tedy zavedení ISMS předpokládá existenci formalizovaného systému oběhu dokumentů. Tento systém, ve smyslu zavedení, není přímo součástí norem řady 27000 – organizace ho tedy zavádí nezávisle na systému ISMS.

Většina firem, které usilují o certifikaci na normu ISO/IEC 27001 již má implementován systém řízení kvality dle ISO 9000, který taktéž vyžaduje systém řízené dokumentace a proto by v souvislosti s oběhem dokumentů neměly vzniknout problémy.

Jako první krok při zavádění systému ISMS je *definice rozsahu ISMS*. Rozsah definujeme pomocí dvou základních dokumentů:

1. Rozsah ISMS
2. Politika 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.

Náplni obou dokumentů se proto budeme zabývat podrobněji, pro tuto chvíli nám bude stačit, že rozsah bude obsahovat definici toho, co daná organizace řadí do ISMS. Politika ISMS již definuje základy organizace ISMS v daném podniku.

Dalším krokem certifikačního procesu je inventarizace IT 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 IT aktiv měla obsahovat.

Inventarizace aktiv by měla být kontinuálním procesem. Důvodem je to, že neustále dochází k obměně výpočetní techniky (hardware), ale také software. 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.*

Inventarizaci aktiv potřebujeme v ISMS z toho důvodu, abychom mohli provést rizikové analýzy jednotlivých aktiv, popř. jejich skupin a rozhodnout se, jakým způsobem budeme riziko řešit. Na rizikové analýzy se zaměřuje ISO/IEC 27005.

Do této oblasti spadá rozhodnutí o používaných metodách rizikové analýzy a provedení samotných rizikových analýz pro vybraná IT aktiva nebo jejich skupiny. Samotná filozofie nasazení je podrobněji rozebrána v *podkapitole věnované ISO 27005.*

Na základě zjištěných údajů v rizikových analýzách (a z dalších zdrojů uvnitř organizace) zpracováváme Plán pro vypořádání se s rizikem (RTP) a také Studii aplikovatelnosti (SOA).

Plán pro vypořádání s rizikem slouží pro rozhodnutí o řešení rizik – tedy která rizika vůbec hodláme v daném prostředí řešit a obecně jakým způsobem. SOA se vytváří na základě analýz rizik a také RTP a slouží k volbě kontrolních mechanizmů pro řízení rizik. Takových mechanismů, které je možno použít, je totiž velké množství, ale ne všechny je možné reálně využít v prostředí dané organizace.

RTP i SOA jsou podrobněji rozebrané v kapitole ISO 27005.

Znalost rozsahu ISMS, rizik, která hodláme řešit a vhodnou volbou kontrolních kriterií jsou základními stavebními kameny k tomu, abychom mohli začít se samotnou implementací ISMS. Zavádění ISMS se neděje úplně 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

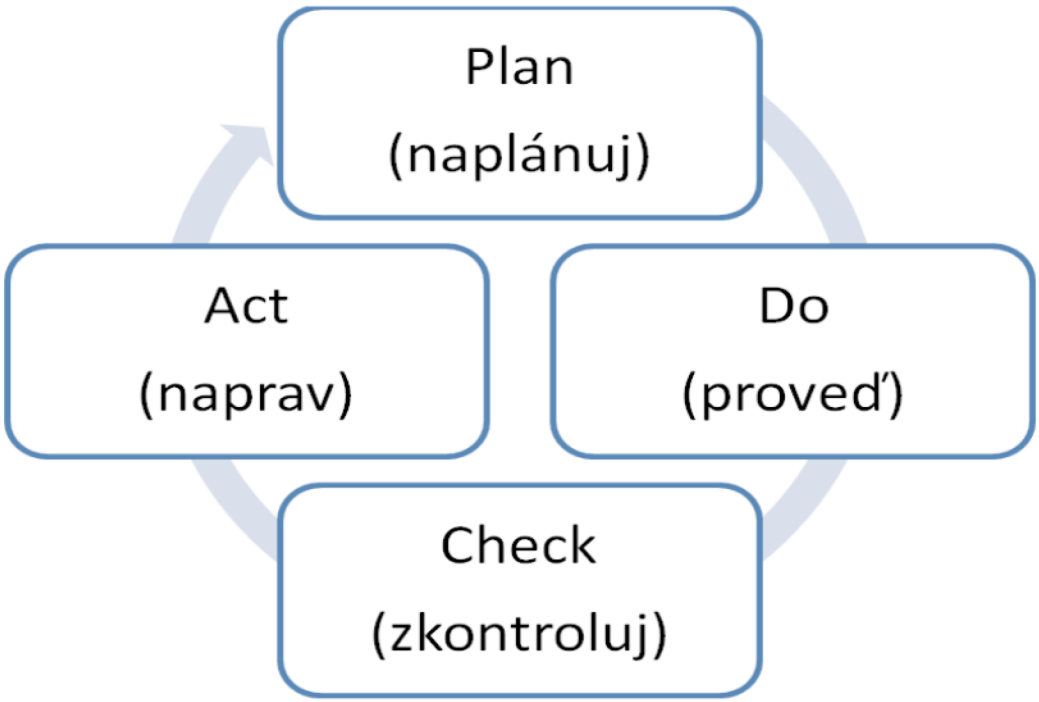
Bezpečnostním politikám se budeme podrobněji věnovat v následující podkapitole, co ale další dokumenty, které mají být výsledkem implementačního procesu? Opatření definovaná bezpečnostními politikami musíme podle něčeho kontrolovat. Za tímto účelem se navrhuje proces auditu. Tento proces nám říká, jakým 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 IT 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 zlepšovat kontrolu nad řízeným procesem. Kromě tohoto účelu však PDCA našel uplatnění v řadě dalších

oblastí, jako je řízení kvality nebo také řízení informační bezpečnosti.

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

1. Co je to ISMS?
2. Co je účelem stanovení rozsahu a politiky ISMS?
3. Vysvětlete princip PDCA.

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 ochrana IT používaných organizací, nebo chápeme ISMS šířeji a budeme se snažit o zavedení integrované ochrany včetně informací třeba v papírové podobě, archivy apod.? Takové rozhodnutí je velmi závažné protože informace v různých podobách jsou vystaveny různým rizikům a proto také náročnost implementace a údržby 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 jí 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.

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
   - 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, běžné uživatele.
4. Návaznosti na další procesy systému ISMS
   - Řízení IT aktiv
   - Řízení rizik
   - 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.

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 závislost na zvoleném způsobu řešení. Do této kapitoly patří také definice role Rady IT.

V případě rady, bychom ale také mohli definovat její jmenování, pravomoci a způsob práce, pokud nemá Rada vlastní statut, tedy samostatný dokument, který tyto věci definuje. Pokud existuje statut rady můžeme se v Politice ISMS omezit na prosté začlenění této Rady do širší organizace informační bezpečnost 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 rolemi 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, že řeší bezpečnostní incidenty.

Z pohledu práv a povinností těchto generických rolí můžeme např. specifikovat, že uživatel má právo na to, aby IT aktivum pracovalo tak jak má a uživatel tak mohl vykonávat své pracovní povinnosti. Mohou zde být také obecná omezení že IT 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 řízení konfigurací 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.

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.

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)!

Studie aplikovatelnosti (SOA) se vytváří na základě jednotlivých provedených analýz rizika aktiv IT a také na základě rozhodnutí o vypořádání se s riziky. K čemu vlastně SOA slouží pokud už máme identifikována rizika, zhodnocenu jejich závažnost a jsme také rozhodnuti o tom, co s nimi hodláme dělat? Naši motivací pro pořízení SOA je identifikace dalších kontrolních mechanismů, které není možné z ostatních rizikově orientovaných dokumentů získat.

Může se jednat o další požadavky vyplývající z platné legislativy, požadavků kontraktorů dané organizace např. v souvislosti se zapojením do rozsáhlejších odběratelsko-dodavatelských řetězců (Supply Chain Management (SCM)).

Důležitou úlohou SOA je také říci, zda identifikované kontrolní mechanismy jsou anebo nejsou implementovány v dané organizaci a popřípadě popsat také způsob jakým jsou implementovány. Informace o způsobu implementace jsou obvykle v tomto dokumentu velmi krátké a to z toho důvodu, že je jich velmi mnoho. SOA se místo popisu implementace může také odkazovat na další dokumenty, ve kterých je implementace popsána podrobněji.

SOA je tedy centrálním repozitářem zvolených kontrolních mechanismů, ze kterého lze vyjít během revize celého systému ISMS. Z tohoto důvodu je také tento dokument jedním z prvních, které auditoři kontrolují během 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.

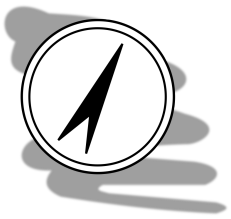
Ve srovnání s Politikou ISMS je tedy hlavní rozdíl v zaměření na konkrétní aktivum nebo skupinu aktiv. Lze také říci, že bezpečnostní politika aktiva implementuje Politiku ISMS pro potřeby řízení informační bezpečnosti tohoto aktiva.

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 řad 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, analýza rizik daného aktiva (pokud byla zpracována), případně další dokumenty mající vazbu k danému aktivu (může se jednat např. o dokumentaci procesu, podle ISO 9000, kde dané aktivum hraje významnou roli apod.).

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 předmětu, 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 připravující 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 předpokládaný čas revize odlišný, než ten, který určila Politika ISMS.

Kontrolní otázky

1. Co je to SOA a k čemu slouží?
2. Vysvětlete 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?

2.3 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], které se zaměřují na systémy řízení rizik obecně.

ISO 27005 ani ISO 31000 nepožadují použití určité přesně definované metody analýzy rizik. ISO 31000 ale může pomoci při výběru vhodné analytické metody tak, aby splňovala potřeby organizace. Volba metody samotné je tedy přímo na dané společnosti.

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.

IT 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.

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. brainmapping 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.

Bohužel ne všechny zranitelnosti jsou známy, popř. jsou známy všem zainteresovaným skupinám. Z tohoto pohledu zranitelnosti můžeme rozlišovat na známé a neznámé. Známé a neznáme 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.

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 plynou 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 zužitkovat při odhadu rizika.

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

Co se týče metod pro vizualizaci, tak metody brainmappingu 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 FreeMind [24] 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.

Podstata zranitelnosti může být *fyzická* - v takovém případě je zranitelnost způsobena např. nevhodným fyzickým umístněním 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 zranitelností může, ale také nemusí souviset s fyzickým umístněním aktiva – to platí u povodní, kde na základě předchozích zkušeností však můžeme odhadnout pravděpodobnost této mimořádné události a přizpůsobit naše rozhodování o umístnění aktiva.

Události jako je úder blesku apod. však ovlivnitelné nejsou[1].

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 servisy) 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 – čim 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 vyhnout[2]. Většina chyb sice nebude zneužitelná → nevede tedy ke vzniku zranitelností, některé však zneužitelné jsou. Pokud je SW vyvíjen ve vlastní režii, pak 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

[1] Žádné 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 [63–66].

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

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 Mittnick: Umění klamu [48] (vyšlo v češtině) a The Art of Intrusion [49], 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.

Fáze identifikace rizik je popsána výše v souvislosti s dalšími činnostmi, které organizace vykonává (inventarizace IT 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 době známy a obě jsou použitelné pro analýzu rizik IT aktiv.

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 portfoliu 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 použité 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 IT aktiv*.

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

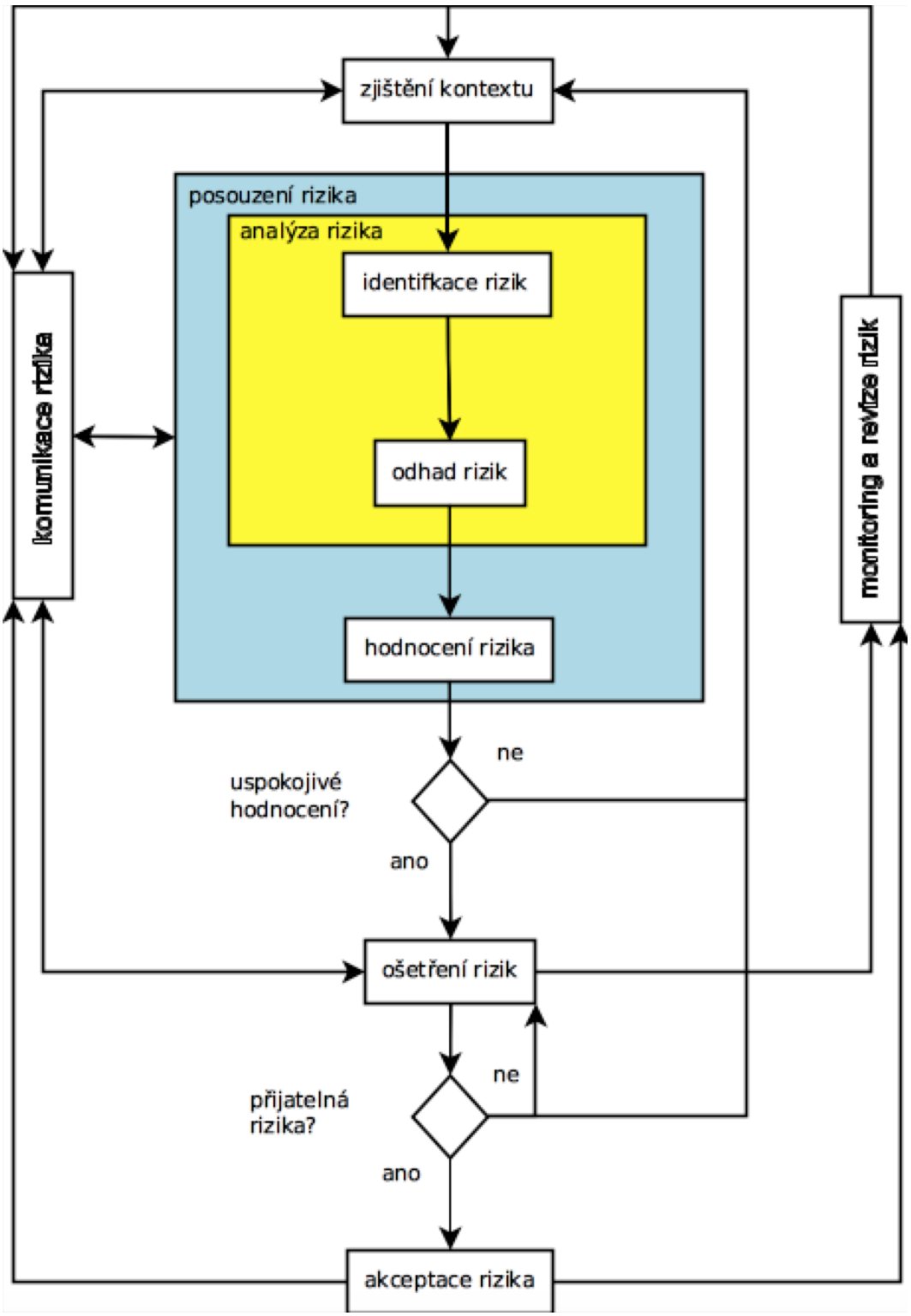
Pro základní rozlišení z hlediska přijatelnosti nám může posloužit matice rizik, viz obr. 2.4.

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 připíšeme.

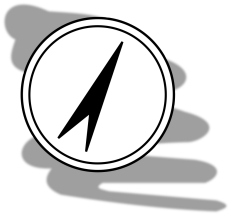
Standardizace je obzvláště potřebná u závažnosti, jelikož se jedná o tzv. kategoriální proměnnou s neostrou definicí. O závažnosti můžeme říci, že je například malá, střední nebo velká, můžeme ale vymyslet naprosto odlišnou stupnici (bez následků, ohrožení chodu systému, ohrožení chodu organizace, ohrožení 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 mát dostatek finančních prostředků k jejich zakoupení a proto se musí smířit s tím, že rizika spojená s Intelectual Property (IP) vlastnictvím nemá pokryta tak, jak by si představovala.



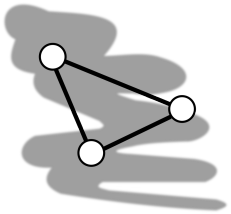
Obrázek 2.3: Proces posuzování informačního rizika (převzato z ISO 27005 [10]



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 „ajťáci“. 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

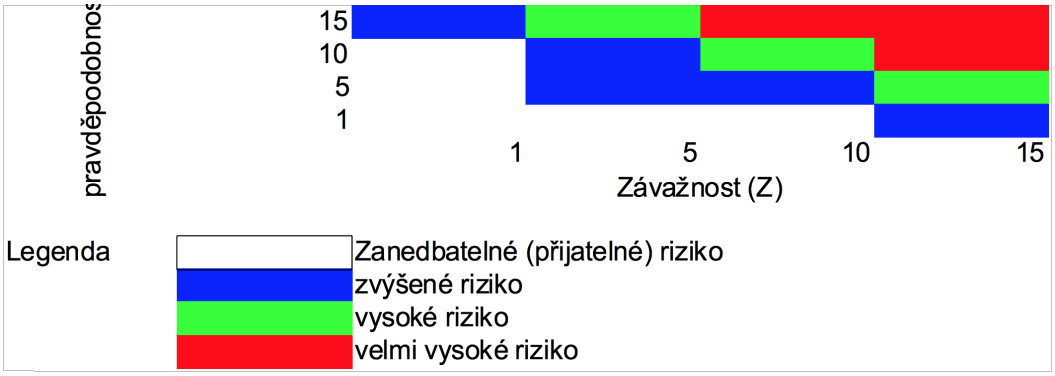
Při volbě metod bereme v úvahu také fakt, že často existuje celá řada variant metody. Abychom zajistili opakovatelnost musíme metodu nějak zakotvit. V případě metod FTA a ETA je to jednoduché, obě metody jsou normalizované. V případě FTA je to ČSN 61025 [61], v případě ETA je to ČSN 62502 [62].

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

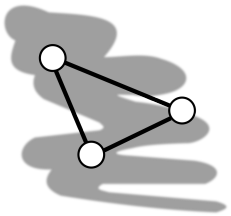
Analýza rizika – semestrální projekt

Jeden ze semestrálních projektů je na zpracování analýzy rizik IT 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



RA2 – The Art of Risk [28]

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.

Kontrolní otázky

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

Systém řízení konfigurací

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

Po přečtení této kapitoly budete
Znát

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

Čas nutný ke studiu
Pro prostudování této kapitoly budete potřebovat přibližně 2 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 následujících řádků.

3.1 Inventarizace IT aktiv

Inventarizací aktiv rozumíme proces, kterým pořizujeme soupis IT aktiv. Inventarizace může probíhat 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 IT 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 40 000,- 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 Rosource Planning (ERP) v ceně 150 000,- sloužící pro plánování zdrojů podniku.

Z hlediska účetnictví drobný majetek s pořizovací cenou pod 40 000,- není předmětem zájmu. 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 obsahuje kritická data nutná pro fungování organizace, ale jelikož se jedná o open source program, jeho pořizovací hodnota je 0,- Kč a tedy očividně nespadá do skupiny NIM majetku, kam by jinak software přináležel. Situace, že by se takový systém neinventarizoval pro účely řízení informační bezpečnosti tak není přípustná.

Další otázkou je, co je přesně IT aktivum? Tímto pojmem jsme se extenzivně zabývali v předchozích dvou kapitolách. Možná jste si všimli, že z kontextu vyplývalo, že aktivum IT mělo v některých případech charakter spíše hardware zatímco v jiných případech mělo charakter software. Takže je aktivum software nebo hardware? Odpověď zní ano, což lze číst buďto, podle Vašeho toho, jak situaci vnímáte, nebo obojí.

Situace ale může být ještě komplikovanější – 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 klastry? 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 [55] z června 2015.

Jazyk UML byl původně určen především pro programátory, protože jim umožňoval získat trošku 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).

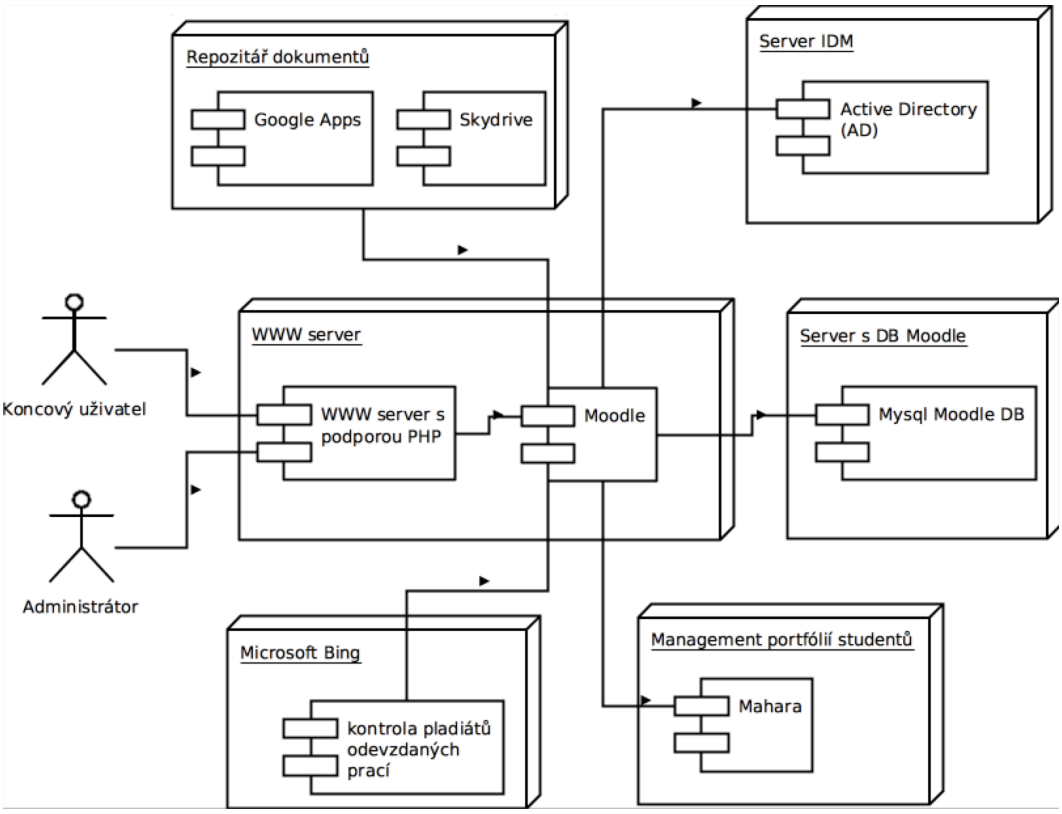
Nás pro účely konfigurací bude zajímat pouze jeden z mnoha diagramů, které jazyk UML poskytuje a to konkrétně diagram nasazení (deployment diagram). Tento diagram popisuje jakým způsobem jsou rozmístěny jednotlivé komponenty systému na HW.

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

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.



Obrázek 3.1: Deployment diagram Moodle

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 klastr, 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. Databázový backend systému je veden na samostatném databázovém serveru – v tomto případě na serveru MySQL.

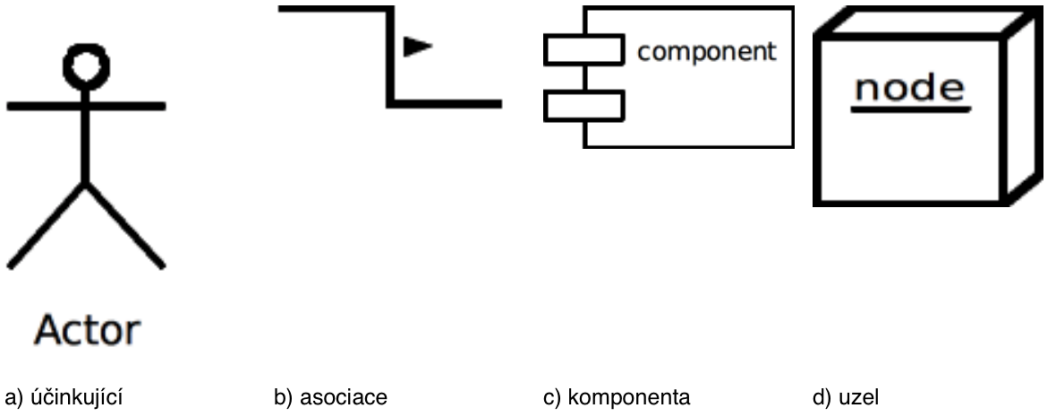
Identitu uživatelů Moodle ověřuje vůči externí databázi uživatelských účtů, v tomto případě realizovanou pomocí Active Directory (AD). Kromě toho kontroluje Moodle semestrální projekty na plagiáty pomocí vyhledávače Bing, umožňuje připojování externích repositářů údajů (Google Apps, MS OneDrive (původně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

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 [50], 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 Profesional[1].

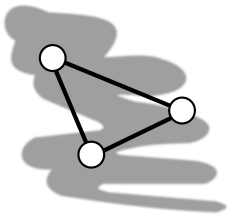
Použít lze také některé webové aplikace, jako je např. Draw.io [5]. Výhodou webových aplikací bývá jejich nezávislost na operačním systému a také možnost integrace s cloudovými službami jako např. Google Drive [8], DropBox [6] a další.

Podrobnější informace o jazyku UML můžete získat buďto z knih jako je např. *Myslíme v jazyku UML* [58] (nebo kterékoliv jiné knize zabývající se UML), použít můžete ale také skripta z předmětu Expertní systémy [67], které obsahují také kapitolu věnovanou jazyku UML (a nemusíte za ně platit).

[1] Standard verze nepodporuje jazyk UML



Obrázek 3.2: Konstruktory deployment diagramu jazyka UML



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.
- činností (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).

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 „síťaři“, 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 IT aktivy, jaké zdroje informací o IT aktivech máme vlastně k dispozici?

1. evidence běžného majetku (klasická inventarizace majetku)
2. evidence licencí software
3. procesní dokumentace (např. v systému ISO 9000)
4. nástroje pro „mapování“ sítě
5. 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 zasadě 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, 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 scaning)
- 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 informační bezpečnosti. 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 uživatelích 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 uživatelích, 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 konfigurací*, 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

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 konfigurací

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 IT aktiva se jedná (tedy SW, HW, ale také lidé kteří s nimi pracují). Právě získání této kontroly je cílem managementu konfigurací.

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

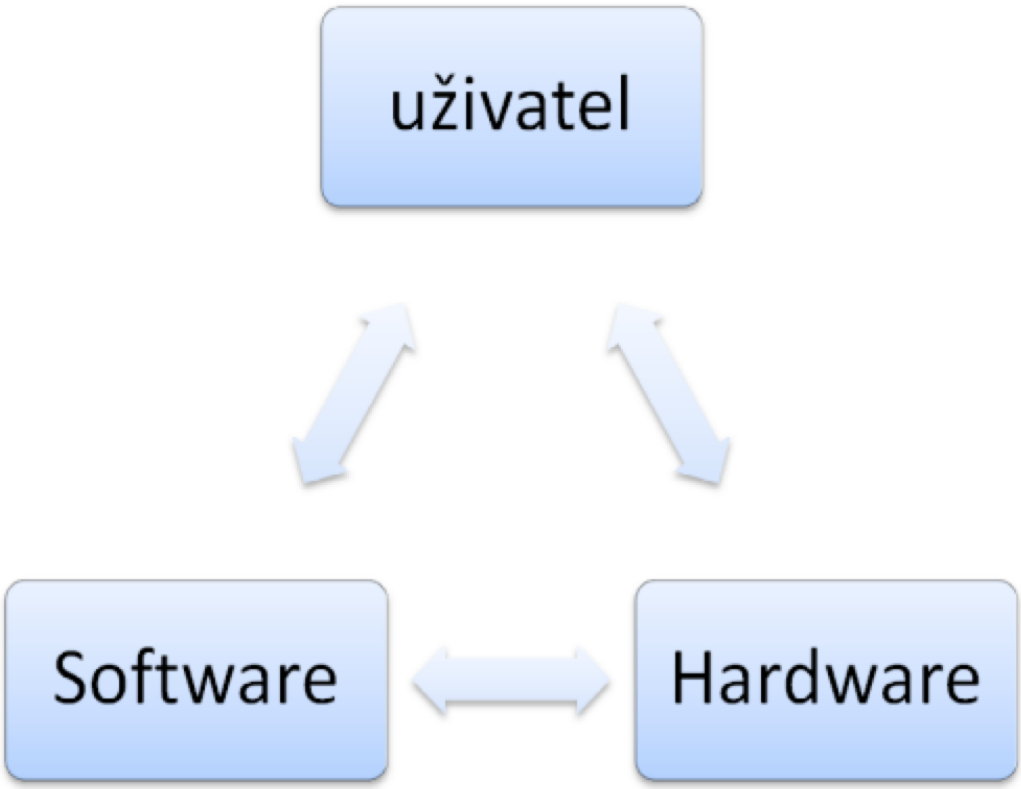
Management konfigurací proto obsahuje (nebo může obsahovat) následující komponenty:

1. inventarizace aktiv,
2. pořizování a správa databáze CMDB,
3. správa požadavků,
4. správa licencí,
5. evidence poruch IT 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 zobrazenu na obr. [?]. 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

3.2.1 Pořizování a správa databáze CMDB

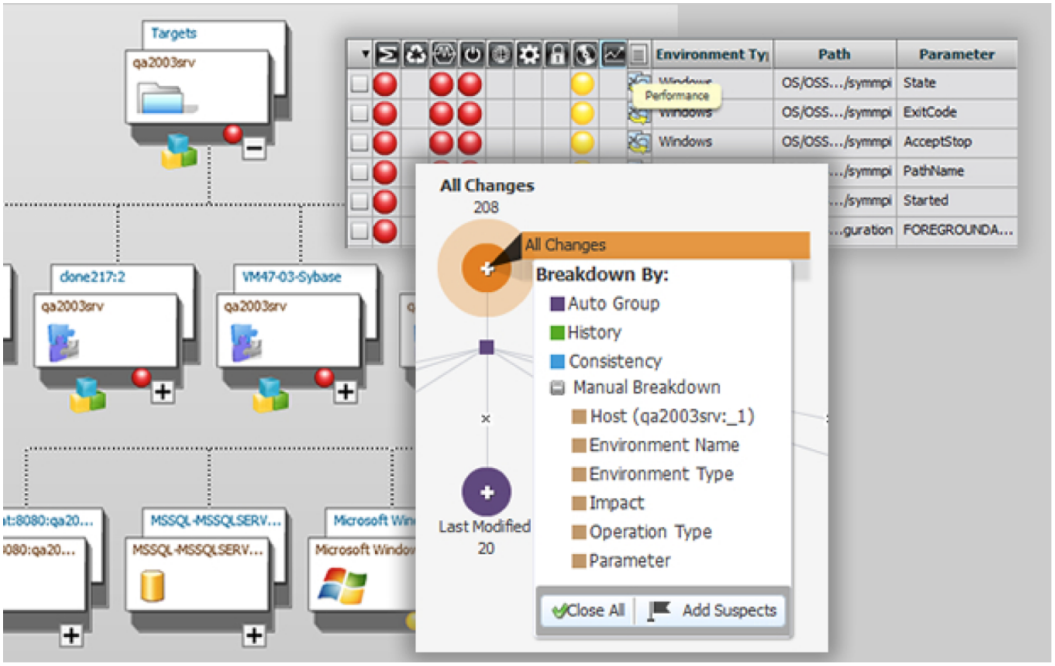
Rozhodnutí o pořízení specializovaného software pro databázi CMDB je očividně velmi závažné. Vzhledem k velmi různorodým informacím, které do CMDB budou vkládány se obvykle očekává investice do datových pump, které údaje převedou z jejich původního umístnění do databáze CMDB.

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 zbytí.

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

Evolven 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 Evolven, 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 [31]. 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 Evolven ale v sobě nemá automatický detekční modul, který by části CMDB automatizovaně naplnil.



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

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 proprietálních 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.

3.2.2 Správa požadavků

Správou požadavků rozumíme v souvislosti s managementem konfigurací evidenci všech požadavků souvisejících s aktivem. Požadavky se mohou týkat žádostí 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 informační bezpečnosti.

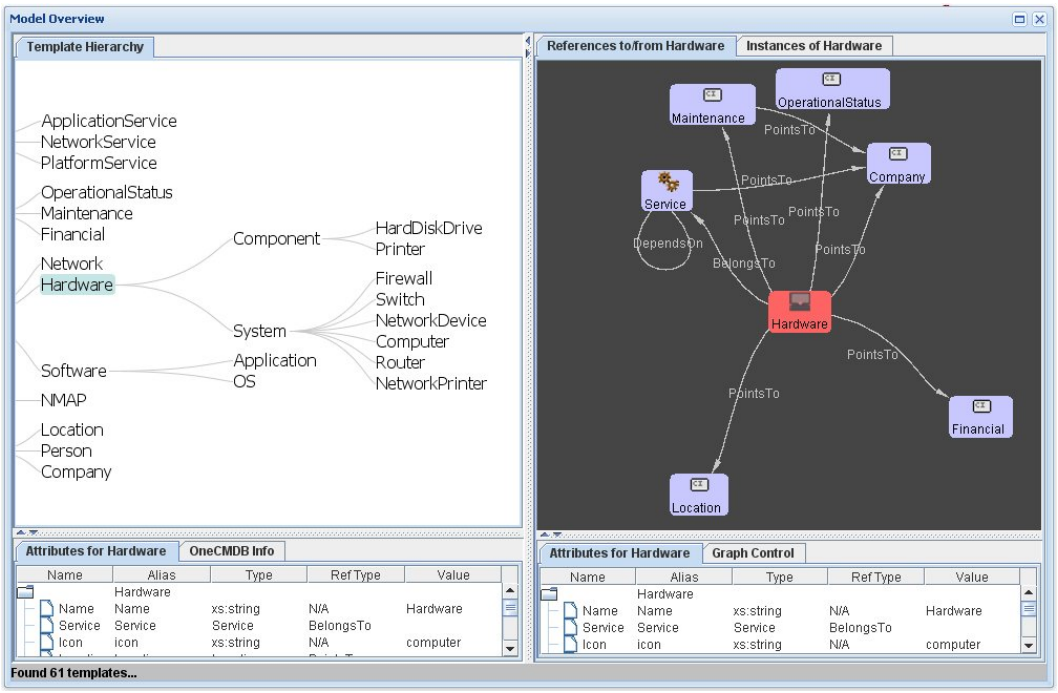
Správa požadavků se děje obvykle pomocí specializovaného software. Tento software se může lišit podle toho, jaké požadavky jsou jím sledovány. Např. požadavky směřované na vývoj software mohou být evidovány pomocí jiného software než požadavky na řešení problému s provozem aktiv.

Můžeme si to demonstrovat na specializovaných SW nástrojích pro evidenci požadavků na vývoj jako je Trac [20], Jira [27] 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.



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

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
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.

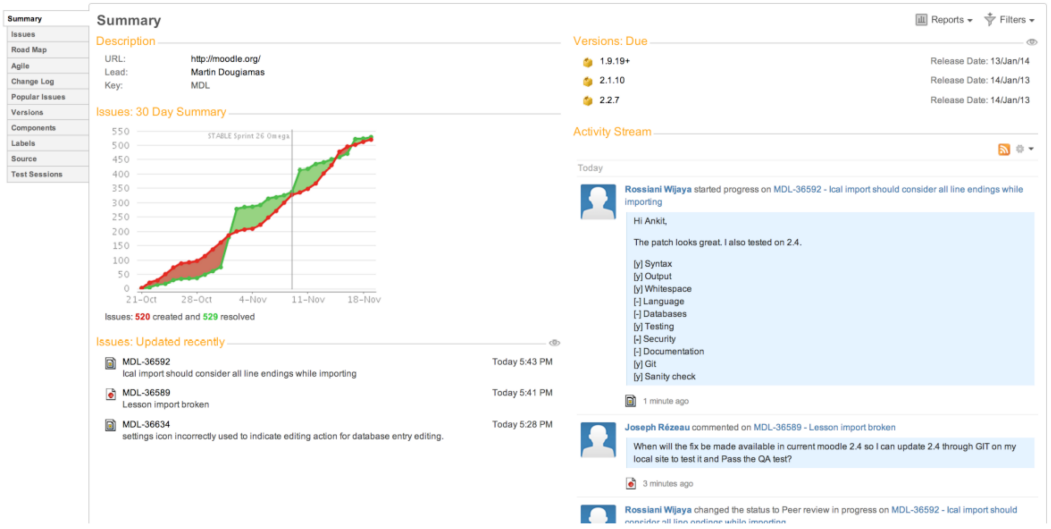
Pojmenování řad by mělo být pokud možno intuitivní, aby bylo na první pohled možné identifikovat účel řady.

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 buisiness 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



Obrázek 3.6: Jira GUI pro projekt Moodle (převzato z [51])

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 (http://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, Arctel, Docházka, Odběr stravy + stravenky, Dovolenky)
- 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

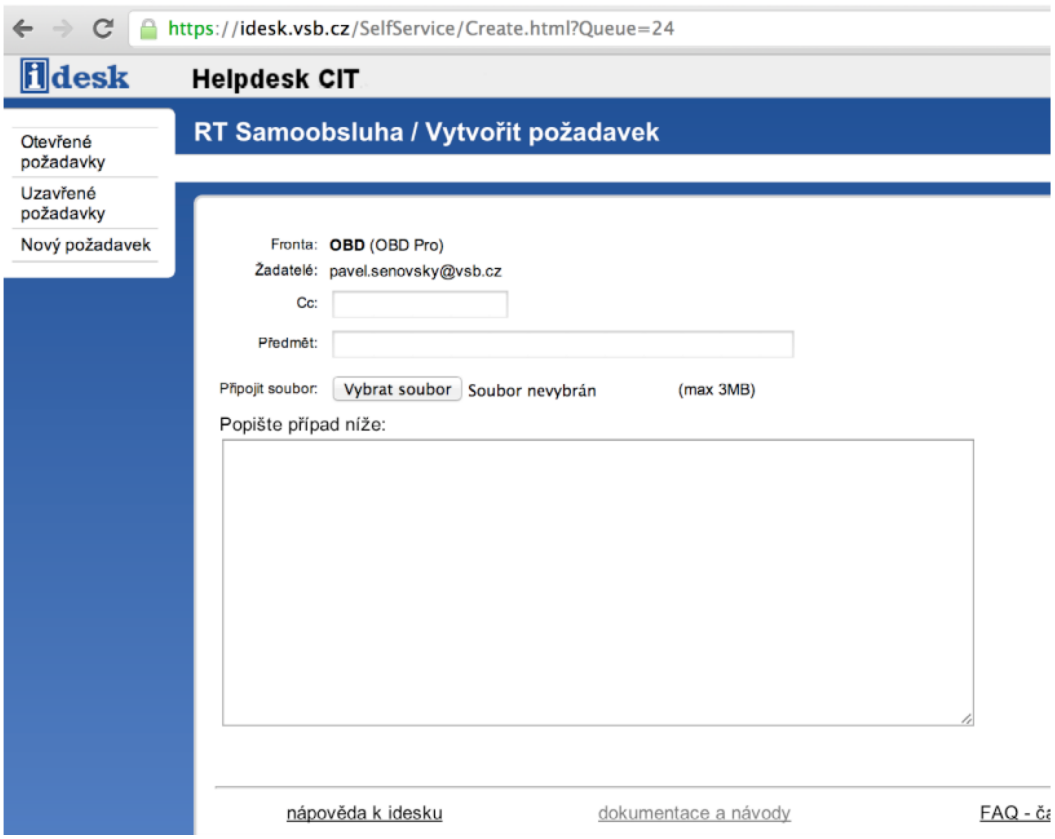
- Osobní počítače a příslušenství (Problémy s počítačem, tiskárnou, skenerem apod)
- Počítačová síť - registrace PC (Registrace PC do počítačové sítě. Neslouží pro registraci PC na kolejích)
- Počítačová síť a připojení (Problémy a požadavky související s provozem počítačové sítě (Internet, VPN, WiFi, ...))
- 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 řad 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 umístnění aktiv).

Bez těchto rozhodnutí a definicí 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.

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

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?

3.3 Správa licencí

Účelem správy licencí je primárně zajistit naplnění požadavků autorského zákona (zákon 121/2000 Sb. [60]), 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 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 desetitisíci provozovanými počítači již 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 přináležející
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 licencuje rovnou pro celou organizaci (site licence). Tímto způsobem jsou tak pokryty operační systémy, 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.

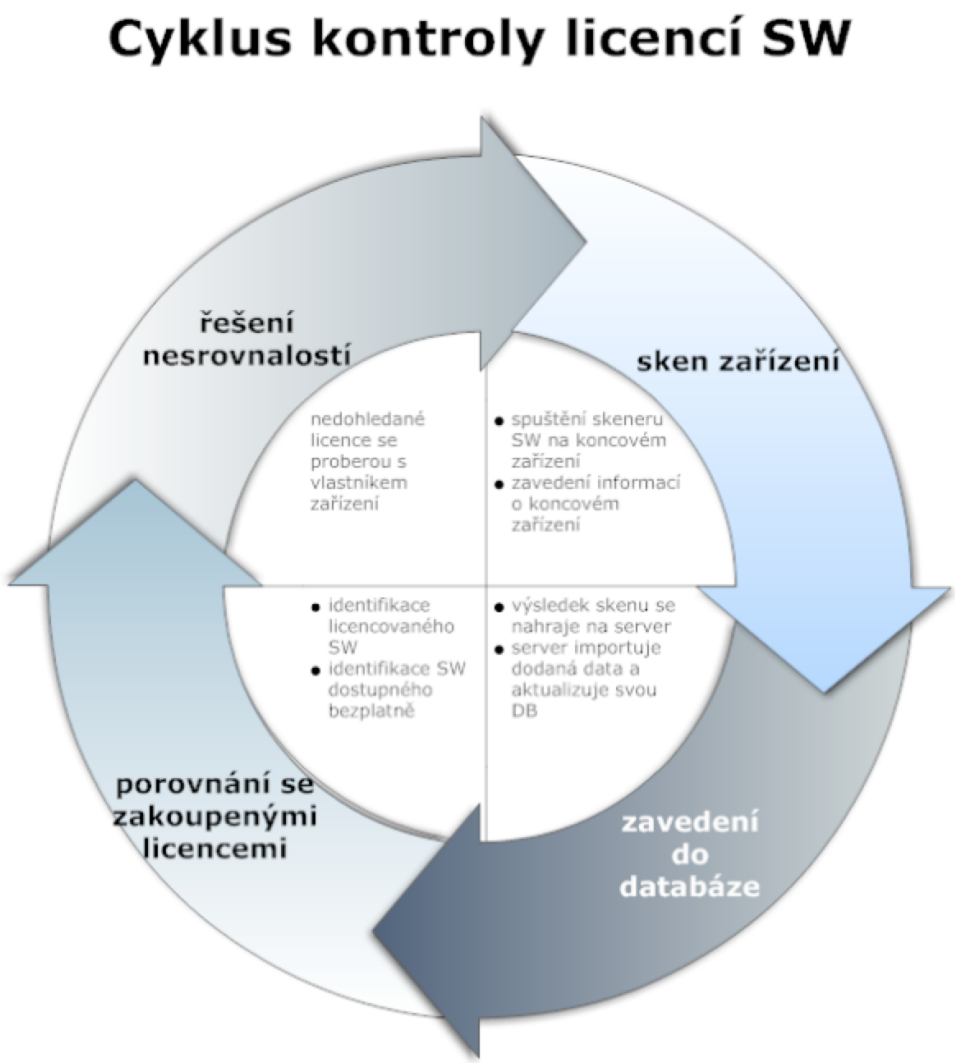
Vzhledem k tomu, že sken software provádí analýzu na úrovní souborů není spojení mezi licencí a soubory úplně přímočaré - jeden softwarový produkt může obsahovat klidně stovky nebo tisíce knihoven a spustitelných souborů. Software pro správu licencí pak obsahuje databázi známých souborů, které umožňují 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.

Pokud je identifikován nelicencovaný software, je nutné buďto dokoupit licenci nebo daný SW odinstalovat. 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



Obrázek 3.8: Cyklus kontroly licencí SW

to koncový uživatel nebo pracovník IT? Tomu je potřeba přizpůsobit proces kontroly, tedy především její fáze řešení nesrovnalostí.

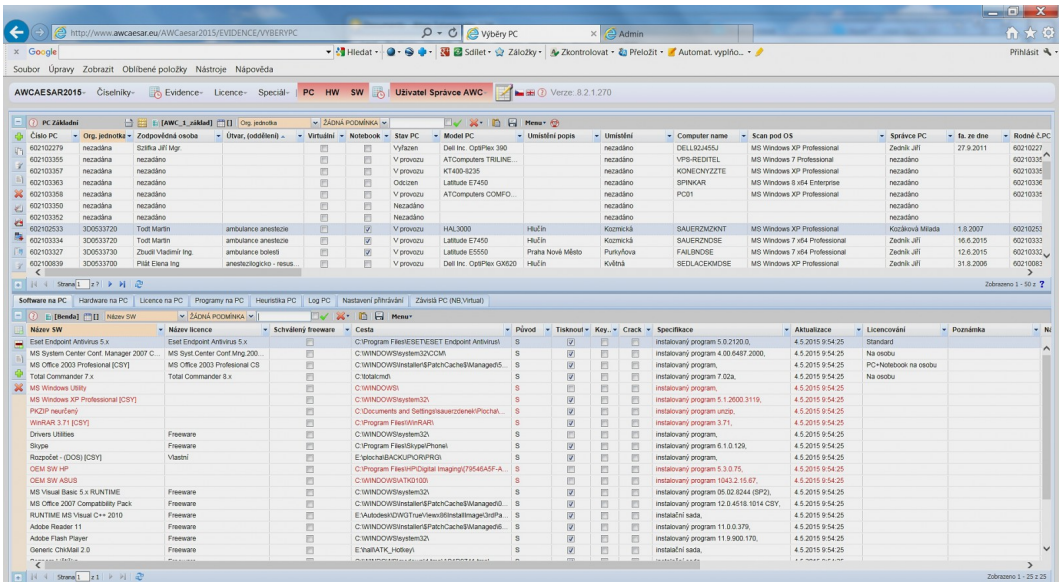
Dále je potřeba připomenout, že obor IT se výrazně vyvíjí a to s sebou nese inovace v oblasti SW, tedy fakt, že se neustále objevují nové verze SW, které uživatelé (nebo jejich nadřízení) požadují. Správa licencí proto není jednorázovou záležitosti. Vzhledem ale k tomu, že vyhodnocení není úplně triviální, 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 [35]. Demonstrační snímky obrazovky tohoto produktu naleznete na obr. 3.9 a 3.10.

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 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 [57] nebo Qualys Guard Vulnerability Management [56] a další.



Obrázek 3.9: GUI AW Caesar (převzato z [34])

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.

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).

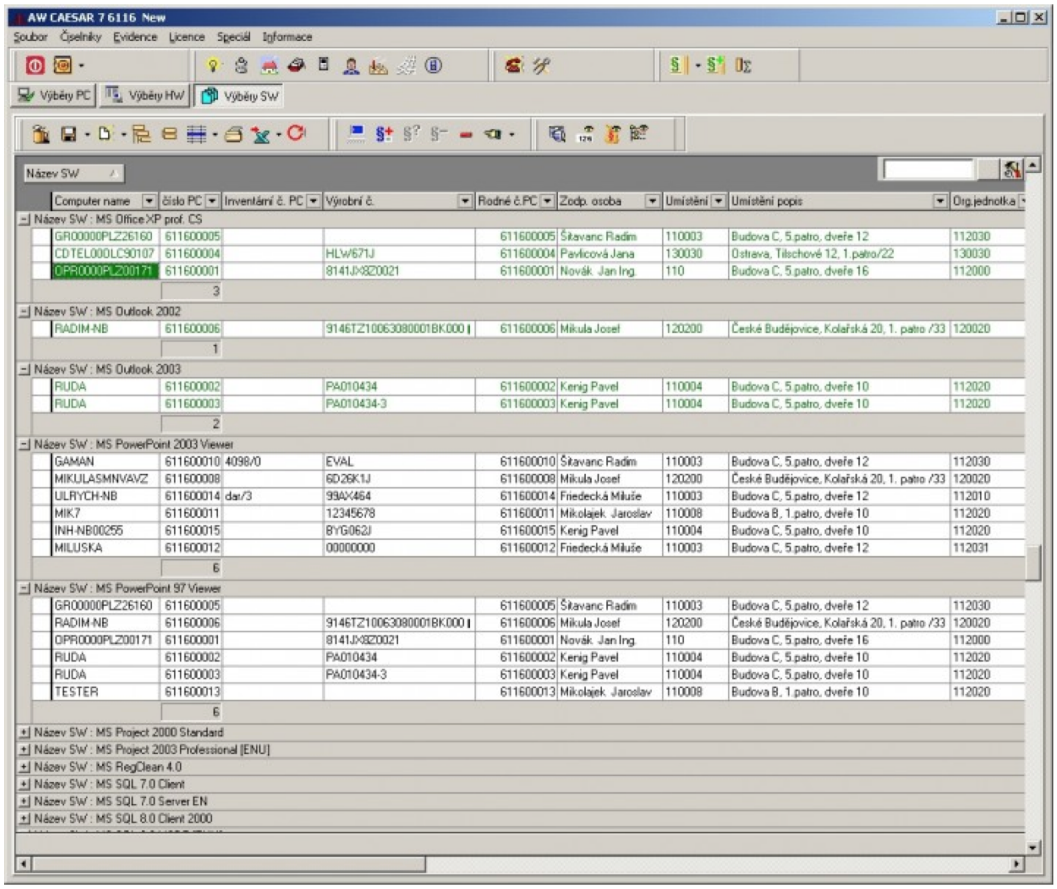
Výhodou skenování po síti je to, že není vyžadována instalace nástrojů do koncových zařízení, nevýhodou pak omezené portfolio informací o zařízení, které jsme schopni tímto způsobem získat - identifikovány jsou pouze ty prostředky (popř. jejich verze), které komunikují po síti a to bez zásahu uživatele. Neodhaleny 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 [46] 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



Obrázek 3.10: GUI AW Caesar - Analýza SW (převzato z [34])

Kontrolní otázky

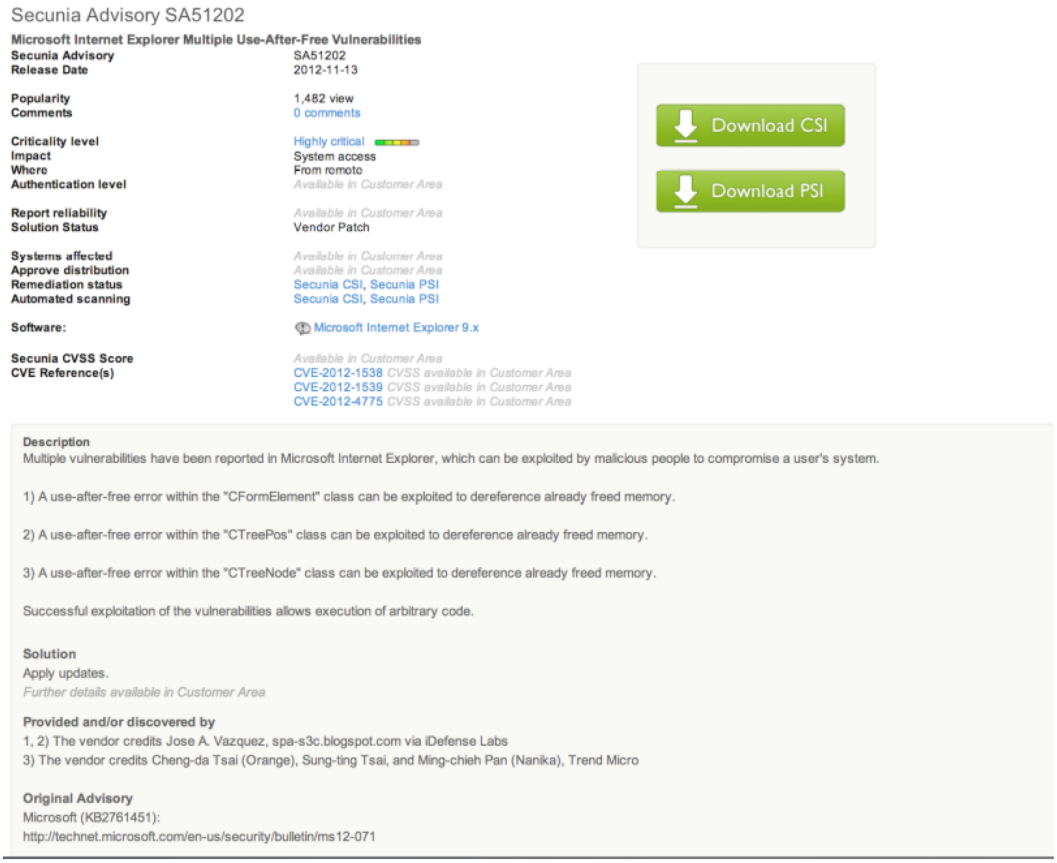
1. Co je účelem managementu licencí?
2. Definujte povinnosti správce SW.
3. Jak probíhá SW audit?
4. Jak řešíme nesrovnalosti v auditu SW?

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 [47], 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 [33] splečnosti 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



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

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.

Kontrolní otázky

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.

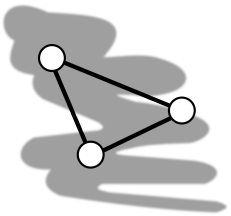
Kapitola 4

Metody a postupy při řízení rizik IT

Průvodce studiem
V této kapitole se podíváme na některé metody a postupy, které je možno použít pro analýzu rizik IT.

Po přečtení této kapitoly budete
Znát

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



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 a rizika, kterým jsou jednotlivá zájmová aktiva vystavena,
- výši škod, které vzniknou v důsledku realizace hrozby pro organizaci,

- opatření, kterými se rizika odstraní nebo alespoň minimalizují, pokud úplné odstranění není možné.

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 IT).

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 systému řízení konfigurací, který slouží jako podklad tyto kroky, celou předchozí kapitolu :-).

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 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) z roku 2011 [59], který způsobil únik informace o 77 mil. účtů uživatelů PSN a měsíční nedostupnost této služby. Celkové náklady společnost Sony vyčíslila 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 [26]. Informace o úniku přišla pro Yahoo v ten nejméně vhodný okamžik, protože právě v této době finišovala 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) [69]. 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, uvvlastníky 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 [29] 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 [32], 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 [32]:

- ponecháno 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 v vlastnictvím aktiva.

Vlastník 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. Zainteresovaností 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 řídících 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).

$$R = f(P, N) \tag{4.1}$$

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

$$R = P \cdot N \tag{4.2}$$

$$R = P + N \tag{4.3}$$

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 semikvantitavní 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.

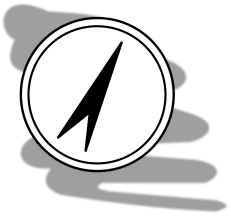
Alternativně lze požít model rizika, který hodnotu aktiva bere v úvahu. Mějme tedy stejný příklad, ale s odlišným modelem rizika. Použijeme opět semikvantitativní hodnocení na pětistupňové škále (0 - 4).

- 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 ochraně aktiva známé 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.

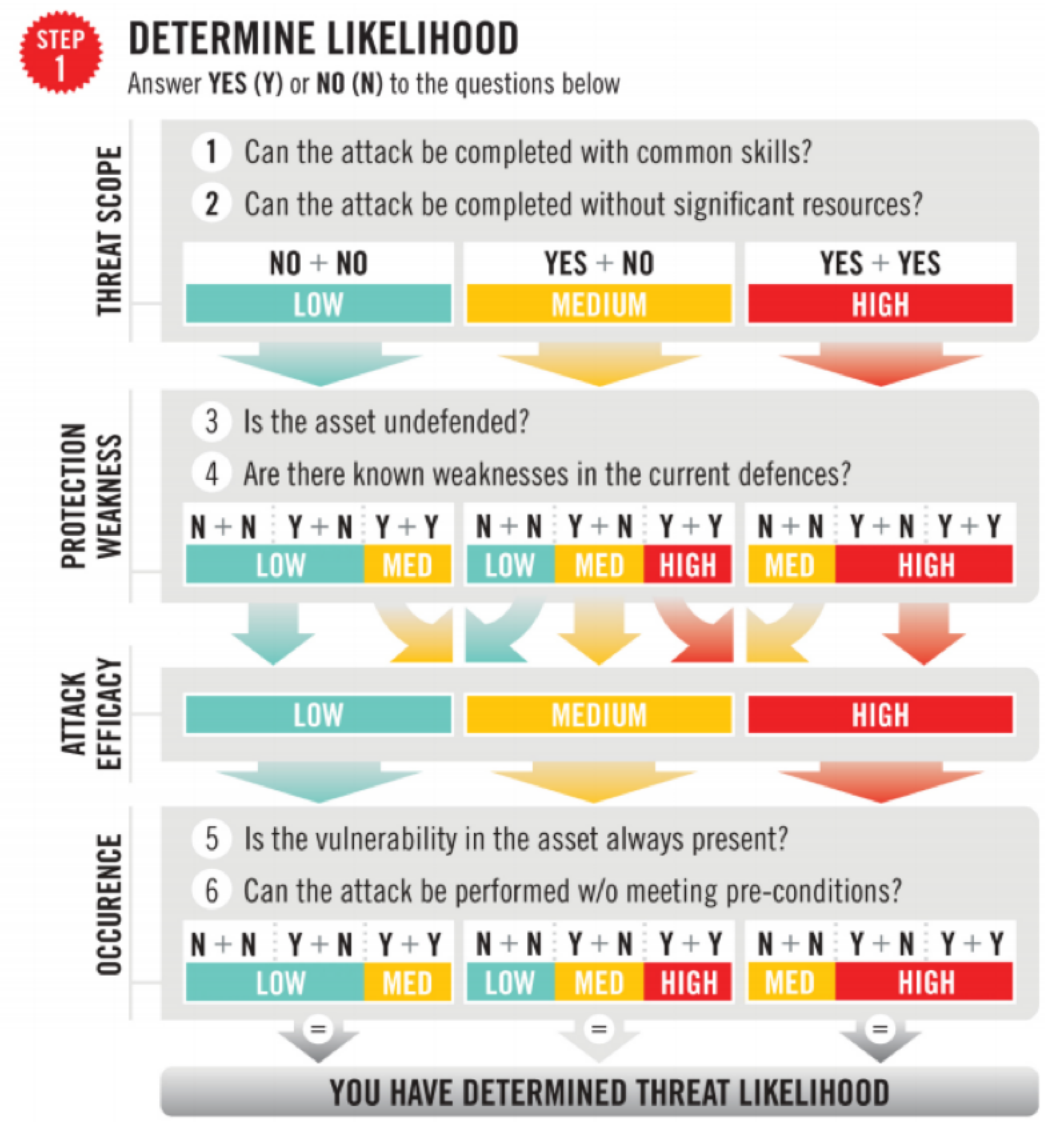
Formálně je BRA semi-kvalitativní metodou analýzy rizika, která pracuje s třístupňovou škálou (nízká, střední, vysoká ... pravděpodobnost).

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].



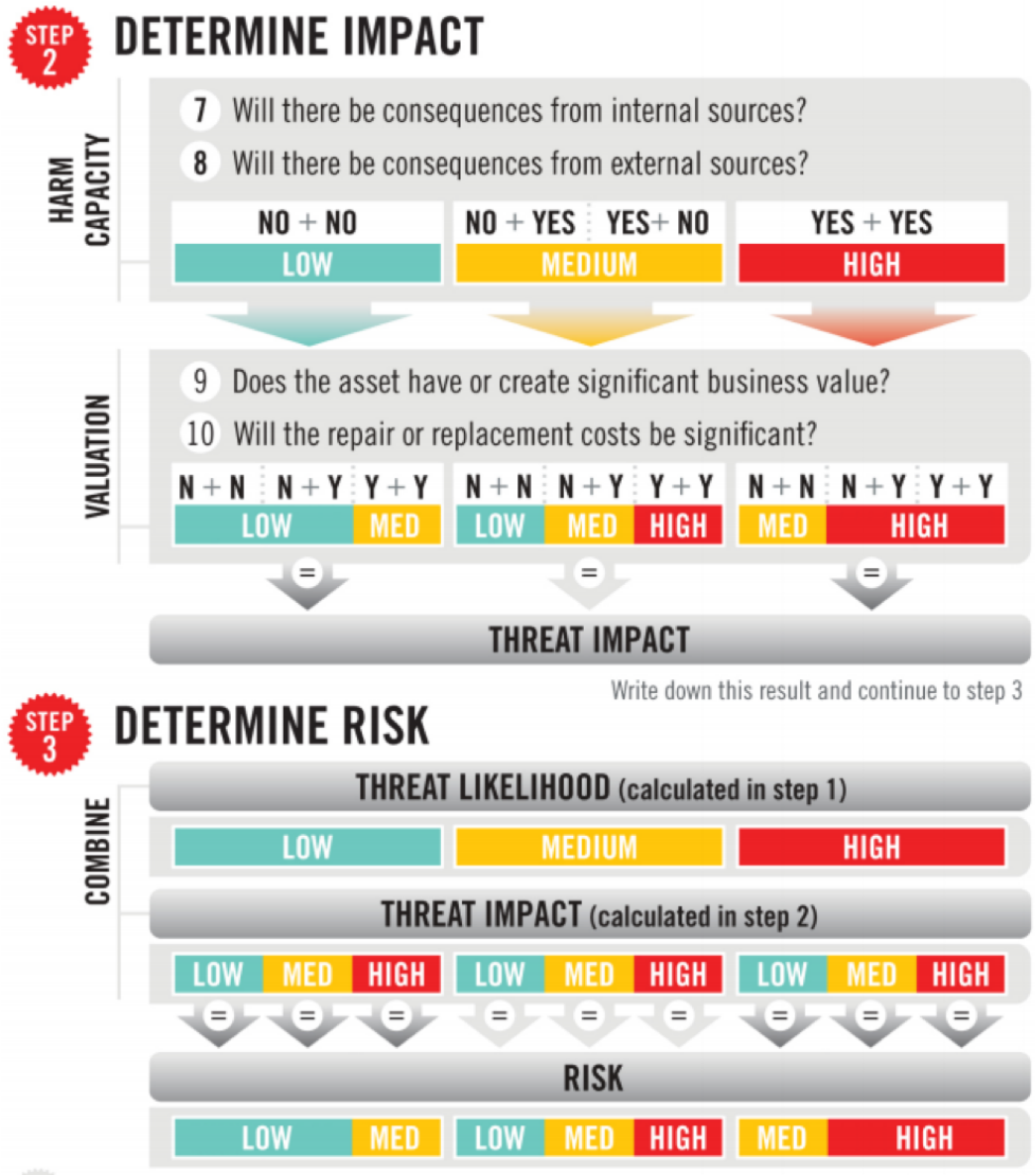
Obrázek 4.1: BRA - hodnocení pravděpodobnosti (převzato z [2])

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



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

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.

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 důležitých vlastností systémů, které k rozhodnutím v oblasti rizik mohou přispívat.

Obrázek 4.3: ARA - pravděpodobnost vs dopady (převzato z [37])

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 charekterizována 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
- 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

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 [54])

- 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 [54] k 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

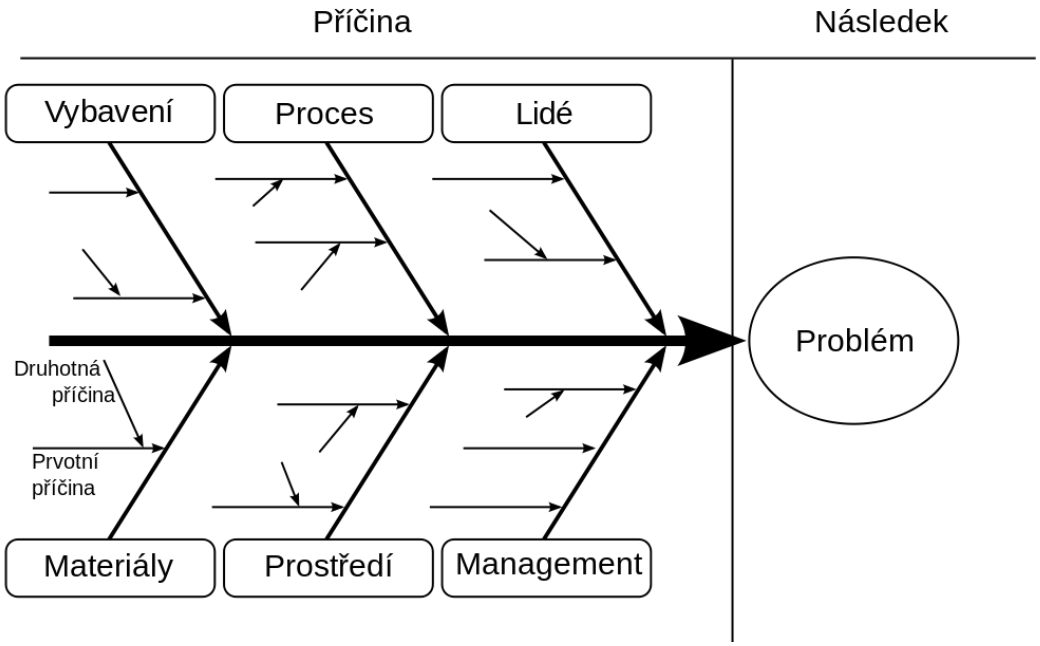
s největším dopadem pro aktivní útok. Metoda proto v oblasti IT je dobře schopna pokrýt hrozby obsahující aktivní element útočníka, který chce napáchat co možná největší škody. Na druhou stranu ale nepokrývá naturogenní hrozby (např. úder blesku), nebo antropogenní hrozby jako jsou běžná selhání hardware apod.

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

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.



Obrázek 4.5: Ishikawův diagram (převzato z [44])

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.

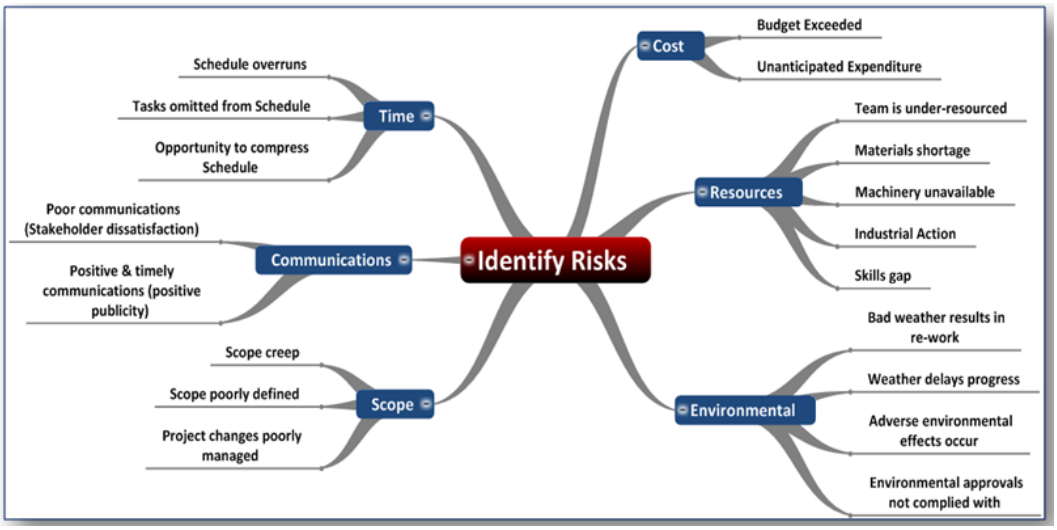
Obě metody mají společnou jednu věc - jsou primárně určeny pro poznání rizika. Samy o sobě nemají potenciál ho ale celé popsat. Z tohoto důvodu se tyto metody používají na začátku analýzy rizik, pro účely jejich identifikace (identifikace rizika a jeho vlastností) a následně jsou doplňovány dalšími metodami, které jsou schopny riziko v nějaké formě kvantifikovat a umožnit tak účelový výběr rizik k jejich řešení.

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.

$$RPN = P \cdot N \cdot H \tag{4.4}$$



Obrázek 4.6: Myšlenková mapa (převzato z [22])

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. Lecos 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 odpovědno za 80 % následků. Původní poměr byl odvozen pozorováním výrobní linky a zkoumáním příčin výroby zmetků.

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 %.

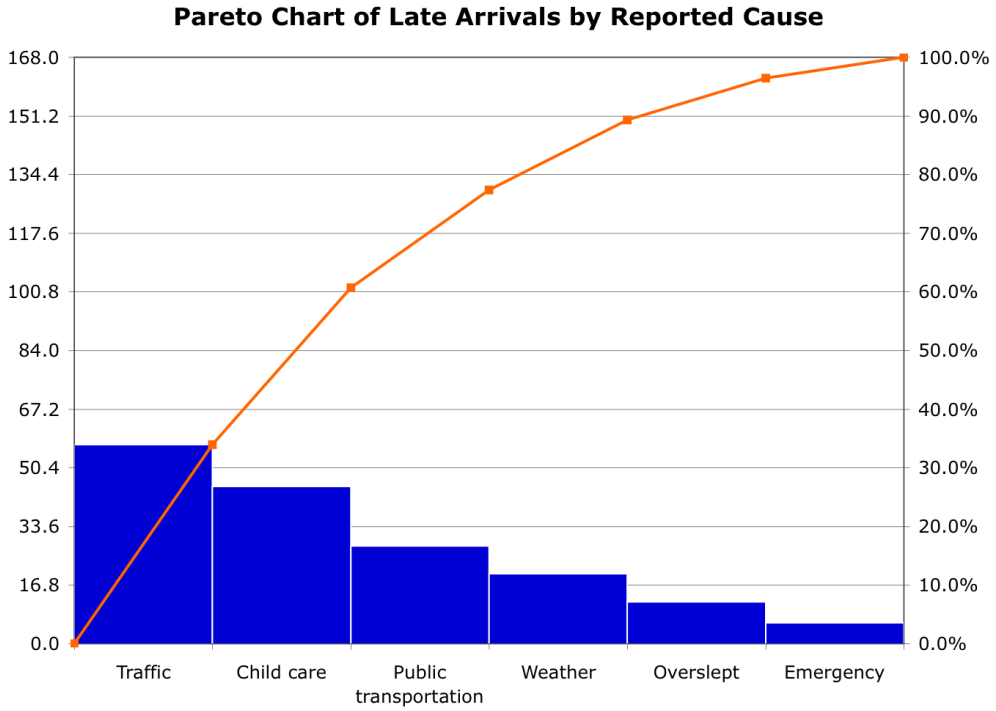
Tím, že příčiny jsou řazeny sestupně podle hodnoty následku platí, že rizika při postupu zleva doprava představují stále menší podíl na následcích. Určením zájmové procentní hodnoty tak můžeme oddělit podstatné od nepodstatného.

Paretův princi 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.



Obrázek 4.7: Paretův graf (převzato z [45])

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, pravděpodobností 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.

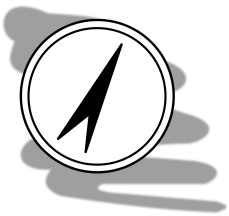
Uvažovat lze i opačný příklad, kdy RPN signalizovaný rozdíl bude menší než skutečný. Stačí abychom pravděpodobnosti stanovili následovně: $P_1 = 61\% ... P_1 = 4$ a $P_2 = 100\% ... P_2 = 5$. Ačkoliv se hodnoty RPN nezměnily, hodnoty pravděpodobností jsou signifikantně odlišné.

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.

Kapitola 5

Případové studie bezpečnostní dokumentace ISMS



Průvodce studiem
V této kapitole načtrneme několik příkladů různých typů dokumentů, které hrají úlohu v systému ISMS.

Čas nutný ke studiu
Na prostudování kapitoly budete potřebovat přibližně půl hodiny na dokument. Doporučujeme se studovat příklady před započetím prací na patřičném semestrálním projektu. Dokumenty, které na semestrální projekt nezpracováváte je pak vhodné nastudovat v rámci přípravy na zkoušku.

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.*

Glosář
...

Komentář *Do glosáře, seznamu zkratek, 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
je nejvyšším výkonným orgánem společnosti. V oblasti IT bezpečnosti:
- schvaluje bezpečnostní dokumentaci
- předkládá jednateli 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
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 oblastí 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
Zodpovídá za oblast provozu systémů IT ve společnosti, zejména pak za procesy:
- pořizování, 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.

Rada IT
Rada IT je poradním orgánem Ředitele informační bezpečnosti, zřízená předpisem XYZ Statut [odkaz]. Hlavním úkolem je diskuzní platforma o problémech a výzvách, kterým společnost čelí v oblasti informační bezpečnosti.

Složení rady je následující:

- ředitel informační bezpečnosti (předsedá radě)
- ředitel IT
- zástupci významných skupin uživatelů

přičemž zástupce významných skupin uživatelů navrhují do rady vedoucí pracovníci jednotlivých oddělení. Ředitel informační bezpečnosti má právo jmenovat do rady další dva členy dle vlastního uvážení (navíc k navrhovaným zástupcům významných skupin), kteří disponují odbornými znalostmi, které by mohly být přínosné pro fungování rady nebo zastupují skupinu uživatelů, která nebyla návrhy dostatečně zastoupena.

Ředitel informační bezpečnosti má právo pozvat dle vlastního uvážení na jednání rady hosty, kteří mohou přispět informacemi k probíranému tématu, hosté však nejsou považováni za členy rady, nemají tak hlasovací práva ani právo k přístupu k důvěrným informacím nutných pro práci rady.

O předložených návrzích rada rozhoduje ve sboru.

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 rolemi 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.

Administrátor

Administrátorem je osoba pověřená správou (administrací) aktiva. Administrátor je určen pro každé aktivum obvykle během pořizovací fáze životního cyklu aktiva, nejčastěji vlastníkem aktiva, který administrátora také zavede do systému evidence aktiv.

Administrátor aktiva 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 administrátor 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 zdělen a vysvětlen.

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.

Přesné povinnosti a postupy administrátora 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. Auditoři jsou jmenování 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 Rady IT.

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. nevyužité 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 uživatele[1].

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 administrátora 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 administrátora 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.

Evidence aktiv

Pro zajištění požadované úrovně informační bezpečnosti je nutno získat kontrolu nad všemi zájmovými aktivy IT. Jedná se především o:

- hardware,
- software a
- lidské zdroje.

[1] Za 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.

Veškerá aktiva musí být evidována od pořízení až po vyřazení z provozu (hardware a software), resp. od přijetí do pracovního poměru do ukončení pracovního poměru (lidské zdroje).

Evidence 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 začlenění do systému ISMS. Vše ostatní je řešeno ve specializovaném předpisu, který je v textu pouze odkazován.*

Management rizika

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 rizika (proces SPR-15-123457)
- vypořádání se s rizikem (proces SPR-15-123458)

Procesy managementu rizik spravuje *Ředitel informační bezpečnosti.*

Identifikace rizik probíhá najednou pro celou společnost a všechna její zájmová aktiva. Identifikaci provádí odbor informační bezpečnosti. Identifikovaná rizika slouží jako podklad pro evaluaci rizika.

Evaluaci rizika a následně vypořádání se s rizikem provádí vlastníci aktiv, obvykle prostřednictvím administrátorů nebo jiných pověřených osob, pod supervizí ředitele informační bezpečnosti.

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 administrátor aktiva, který při obnově spolupracuje s vlastníkem aktiva, uživateli aktiva a případně také dalšími osobami (např. specialisty na obnovu dat apod.) dle charakteru bezpečnostního incidentu.

O průběhu a řešení incidentu musí administrátor zpracovat zprávu, kterou předá Manageru informační bezpečnosti a také vlastníkovi aktiva. V případě obzvláště závažných bezpečnostních incidentů musí byt informována Rada IT, 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.

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 IT aktivech společnosti a způsobu jejich shromažďování.

Účelem shromažďování informací o aktivech je především:

- 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

IT aktivy pro účely se rozumí 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)

Každý druh aktiva má vlastní způsob označování (evidence) a je s ním spojen jiný rozsah evidovaných údajů.

Evidence údajů

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 vlastník aktiva (v případě převodu aktiva provádí záznam původní vlastník 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 princi 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, pak 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 svázán s tímto předpisem a nemá smysl to nějak zastírat.

PC, servery a notebooky[2]

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 přidělenu 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 evidovaný 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 služeb sítě, i těch, které jsou v soukromém 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*

[2] týká 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)

(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

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

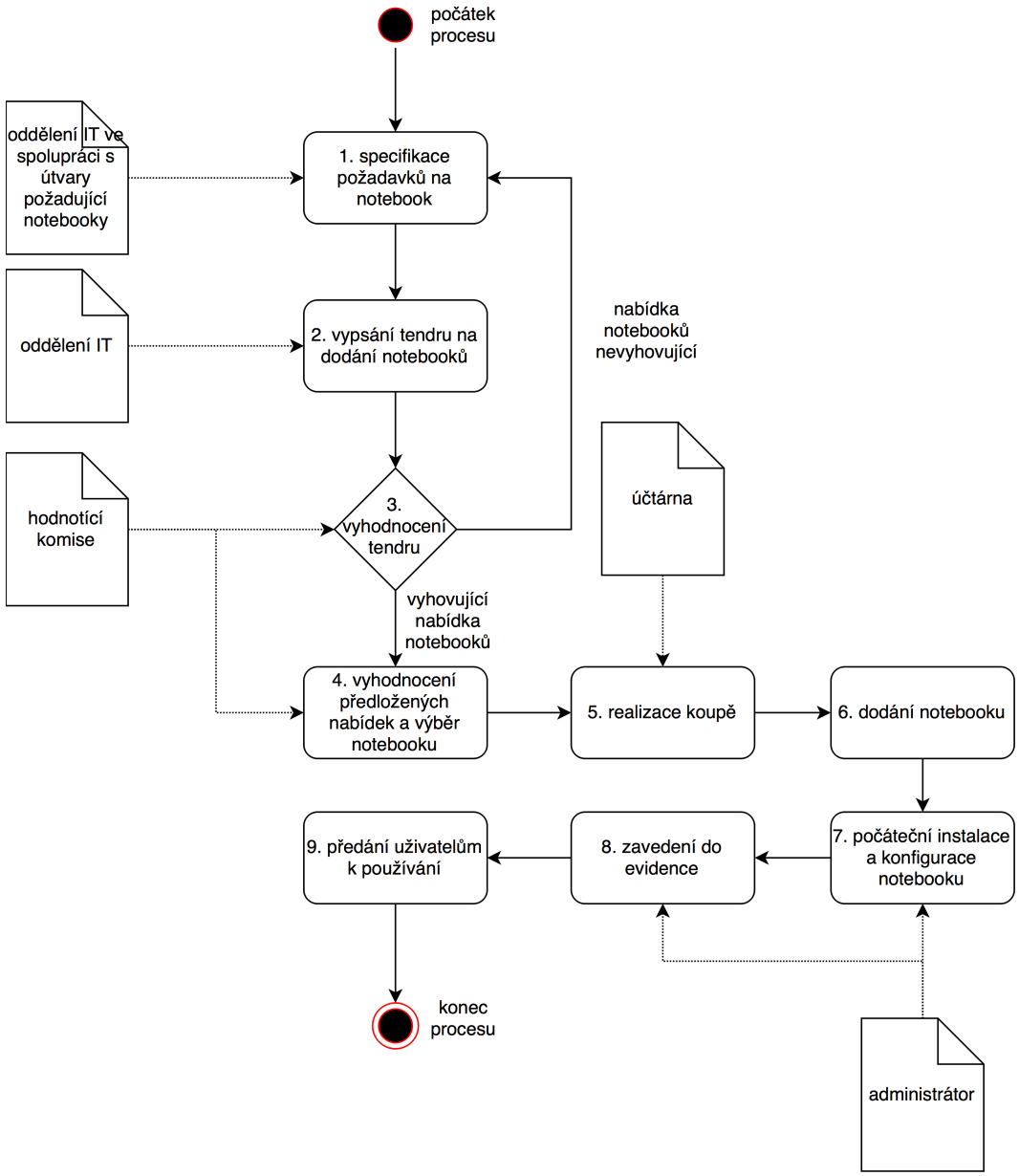
Notebooky pořizované pro nasazení ve společnosti musí splňovat následující požadavky na konfiguraci:

- čtečka otisků prstů
- 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. Čtečka otisků prstů 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.*

Požadavky na software
V případě, že notebook má být provozován na platformě MS Windows je nutné aby se jednalo o verzi podporující šifrování disku.

Proces počátečního pořízení a konfigurace notebooku
Proces pořízení a počáteční konfigurace je znázorněn na obr. 5.1.



Obrázek 5.1: Proces pořízení a počáteční konfigurace notebooku

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 požadavků, které na ně budou kladeny.

Specifikaci požadavků kompletuje oddělení IT ve spolupráci se zástupci oddělení, které vznesly požadavek na nákup.

2. vypsání 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 misí být obesláni minimálně 3 dodavatelé výpočetní techniky.

Ředitel IT může provést zveřejnění znění zakázky na specializovaných portálech 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 zátěžový 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 specifících 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 (více 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 byt 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 specifících spojených s používáním změněného zařízení.

6. Informování o bezpečnostním incidentu

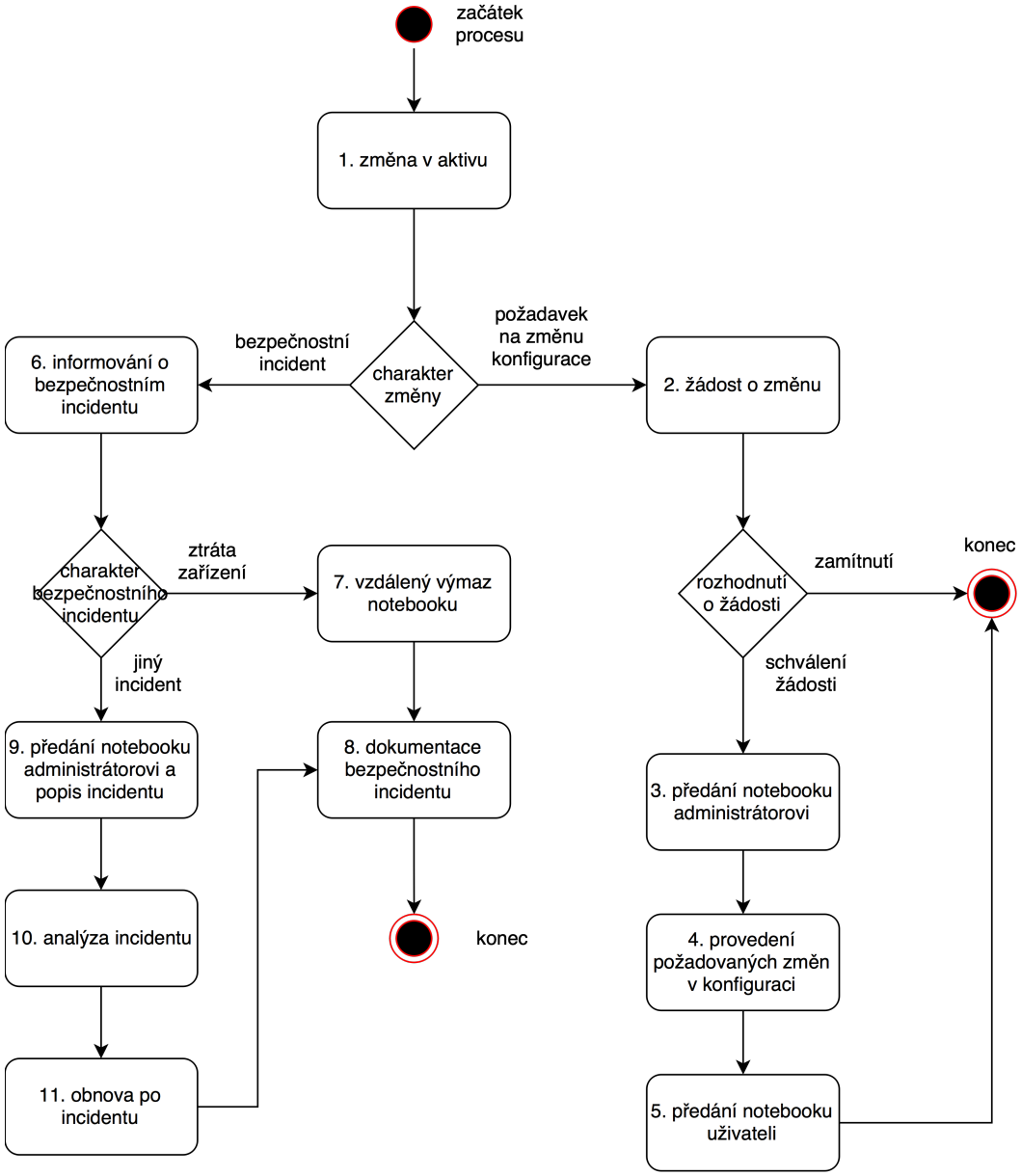
Uživatel informuje administrátora o zaznamenaném bezpečnostním incidentu co možná nejdříve po jeho zjištění. Dle charakteru bezpečnostního incidentu se postupuje dále buďto krokem 7. v případě, že došlo ke ztrátě notebooku (ať už se jednalo skutečně ztrátu nebo krádež zařízení), nebo krokem 9. v případě 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



Obrázek 5.2: Proces realizace změn konfigurace notebooku a bezpečnostní incident

na to, zda mohly dojít k narušení důvěrnosti uchovávaných údajů. Podle závažnosti incidentu se následně volí další postup dle ustanovení *Politiky ISMS*.

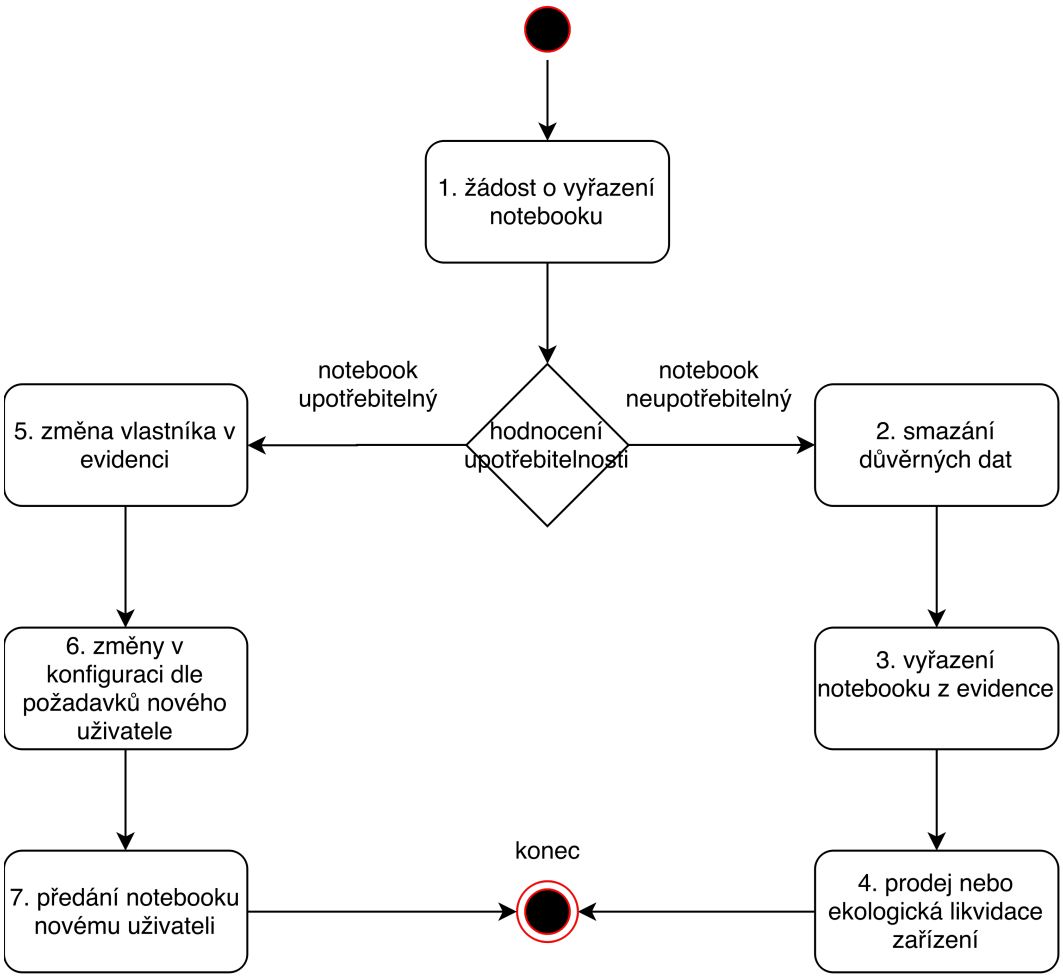
9. Předání notebooku administrátorovi a popis incidentu
Uživatel předá notebook administrátorovi a popíše znaky bezpečnostního incidentu tak, jak je zaznamenal.

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 přeinstalování 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.



Obrázek 5.3: Proces vyřazení notebooku z evidence

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.

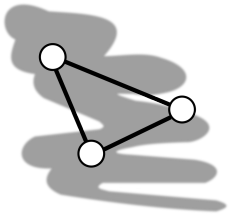
Pokud oslovený pracovník souhlasí, provede administrátor změnu v databázi CMDB (notebook přepíše na osloveného pracovníka).

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 admnistrátor registruje v databázi CMDB jako nainstalovaný na daném notebooku.

7. Předání notebooku novému uživateli
Připravený notebook předá administrátor novému uživateli. Administrátor uživatele poučí o specifících 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 jeden krát ročně. Za provedení revize tohoto předpisu zodpovídá ředitel informační bezpečnosti.



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 [70], 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.

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

Čas nutný ke studiu
Pro prostudování této kapitoly budete potřebovat přibližně 2 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 řídících systému (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 nedávné) se předpokládalo, že investice do IT firmám automaticky přinášejí konkurenční výhodu a tedy, že se automaticky vyplatí.

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* [30], ve kterém popisuje relativně malé přínosy pokračujících investic a také různé aspekty provozu IT systémů, vytvářejících náklady včetně např. spotřeby elektřiny apod.

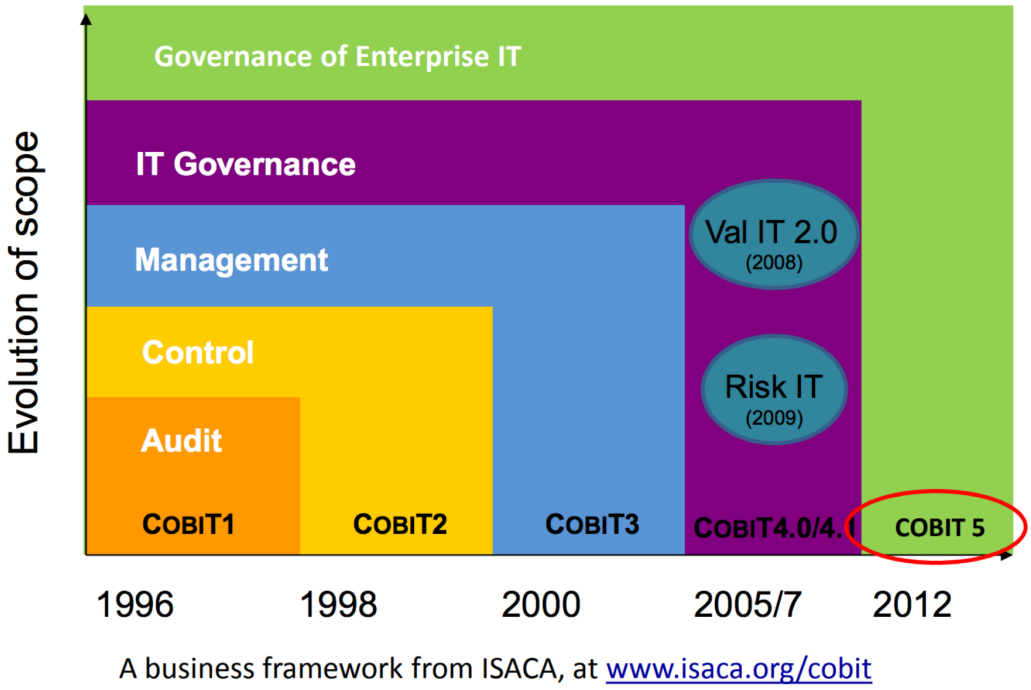
Finanční audit je tedy pouze malou částí problému. ISACA na situaci reagovala rozšířením rámce (1998) v COBIT 2 doplněním cílů pro další oblasti a v roce 2000 pak v COBIT 3 přidala i průvodce pro management.

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.

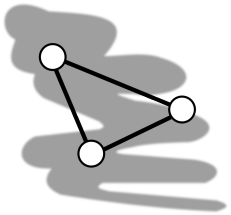
Verze 5 (poslední verze standardu z roku 2012) pak obsah těchto norem integruje do rámce COBIT. Z norem COBIT se tak stává ucelený rámec pro řízení prakticky všech aspektů IT.

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 (převzato z Garsoux [36])



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 dosahováno 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 ve verzi 5 je založeno 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 stakehledry 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. Zájmy stakeholderů tak mohou být 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. enabler goals

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. Enablers jsou faktory, které umožňují dosažení cílů (enable to achieve).

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

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.

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.

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 [42] 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 odebírá 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 počin. 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. řízená 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.

Mapování se provádí také na jednotlivé procesy COBIT. Organizaci procesů COBIT ale probereme v samostatné podkapitole.

			Enterprise Goal			
			Stakeholder Value of Business investments	Customer - oriented service culture	Optimisation of business process functionality	Skilled and motivated peole
			1	6	11	16
IT -Related Goal			Financial	Customer	Internal	Learning and Growth
Financial	1	Alignment of IT and business strategy	P	P	P	S
Customer	7	Delivery of IT services in line with business requirements	P	P	P	S
Internal	9	IT agility	S	S	P	S
Learning and Growth	16	Competent and motivated business and IT personnel	S	S		P

Obrázek 6.2: Mapování BSC IT cílů na podnikové cíle (převzato z Garsoux [36])

6.3.2 Domény a procesy COBIT

Jádro COBIT je realizováno okolo procesů zajišťujících IT služby v organizaci. Procesy jsou organizovány do čtyř domém:

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, hodnoť a posuzuj (monitor, evaluate and assess)

V výše uvedeným doménám, které jsou přiřazovány k managementu pak COBIT používá ještě doménu EDM - hodnoť, řiď 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.

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.

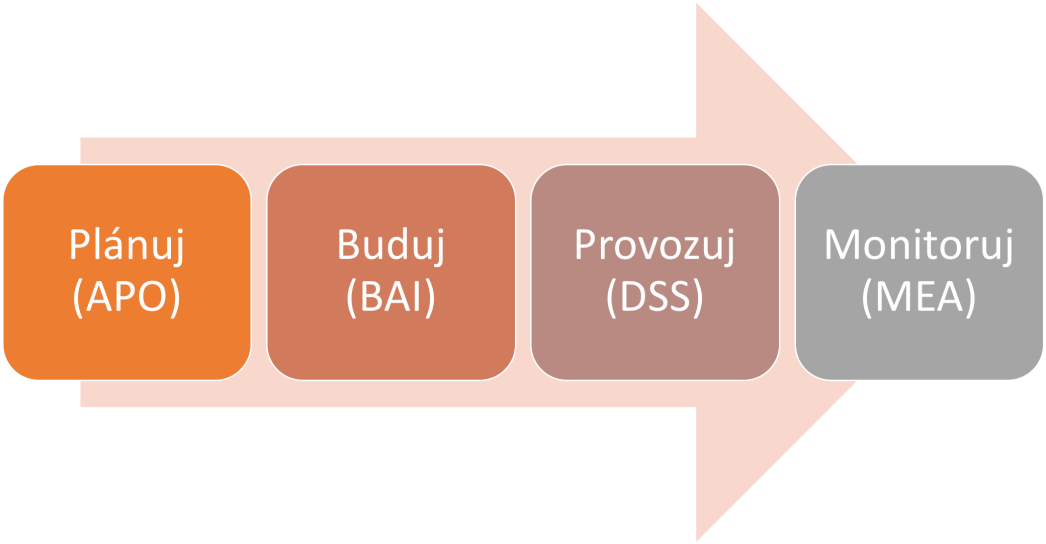
Aby nad výše uvedeným postupem bylo možné získat kontrolu pracuje COBIT s 37 procesy, které zařazuje do jednotlivých domén. Procesy nejsou rozděleny rovnoměrně (EDM - 5 procesů, APO - 13 procesů, BAI - 10 procesů, DSS - 6 procesů a MEA - 3 procesy).

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 doporučovanou 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.



Obrázek 6.3: Návaznost domén COBIT

Obrázek 6.4: Hodnocení domény COBIT (adaptováno z [40])

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:

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 zvyšují, opatření samotné pak ale přináší stále menší užitek (na cestě vzhůru zvládnutím procesu).

Z tohoto důvodu je při zlepšování potřeba soustřeďovat se na „slabá místa“, popř. tam kde existuje největší rozdíl mezi plánovaným a skutečným stavem.

- R (responsible) - odpovědný osoba/osoby, které na úkolu/procesu pracují
- A (accountable) - osoba/osoby, které jsou zodpovědné za úkol/proces jako celek
- 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 považování 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 dvojí - 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.

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					

V COBIT se RACI matice používá primárně pro deskripci procesů.

6.3.4 Model dospělosti

Zajímavou možností, kterou lze využít pro posuzování mezer v systému řízení IT je nasazení tzv. modelu dospělosti (maturity model).

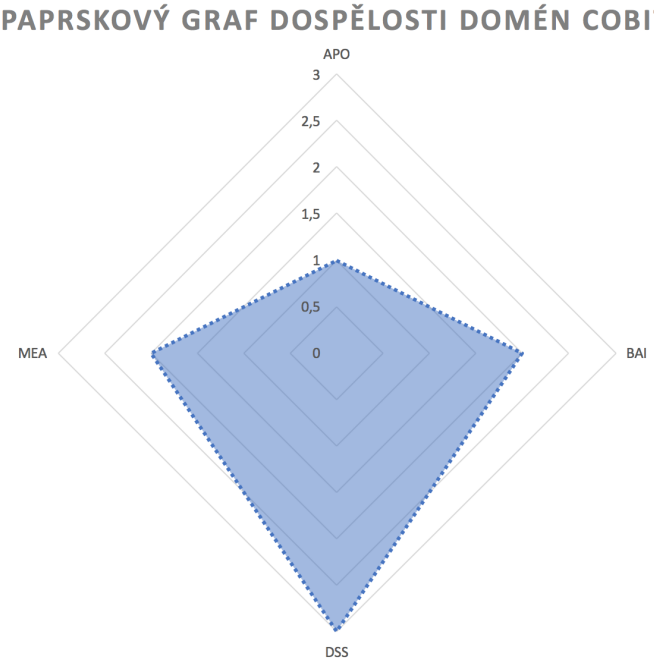
Modelem dospělosti rozumíme hodnocení vyspělosti řízených procesů. Tento model byl poprvé nasazen v COBIT 4 a v COBIT 5 pak doznal značných změn. Vzhledem k tomu, že oba přístupy mají širší aplikaci, budou v této kapitole popsány oba.

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.

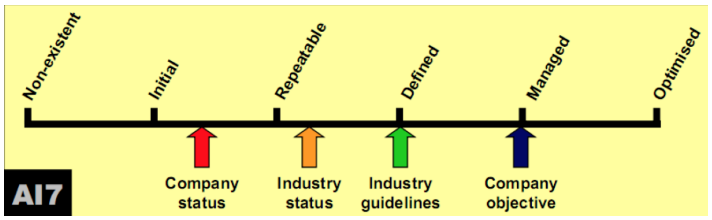
Existuje více možností, jak provést hodnocení. Hodnocení lze provést třeba na úrovni domén COBIT. Vizualizace management domén APO - 1, BAI - 2, DSS - 3, MEA - 2 by mohla vypadat podobně jako na obr. 6.5.



Obrázek 6.5: Vizualizace modelu dospělosti paprskovým grafem

Paprskový graf umožňuje velmi jednoduše identifikovat domény, ve kterých organizace procesů zaostává a kde tedy investice do získání kontroly má největší smysl. Paprskové 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.



Obrázek 6.6: Porovnání stavu vyspělosti procesu s konkurencí, doporučeními a cíli společnosti.

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.

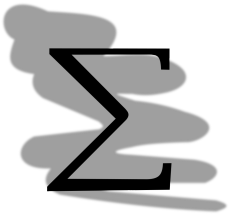
Podobně jako v předchozím případě jsou procesy zařazovány do jedné z šesti úrovní. Tyto úrovně se ale v obou případech neshodují.

- 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
- 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

1. Vysvětlete rozdíl mezi management a governance.
2. Vysvětlete 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?

Literatura

[1] 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

[2] Binary Risk Analysis.

[3] Common Criteria.

[4] Dia draws your structured diagrams: Free Windows, Mac OS X and Linux version of the popular open source program.

[5] Draw.io.

[6] Dropbox.

[7] F01 - Analýza nákladů a přínosů. In *Sourcebook II: Metody a techniky*, pages 388–397. MVČR, Praha.

[8] Google Drive.

[9] Home :: Bugzilla :: bugzilla.org.

[10] ISO 27 005 Information technology — Security techniques — Information security risk management.

[11] ISO 31000 Risk management.

[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.

[15] Joomla! The CMS Trusted By Millions for their Websites.

[16] Main Page - OneCMDB.

[17] Nmap: the Network Mapper - Free Security Scanner.

[18] Secunia Advisory SA51202.

[19] SmartDraw.

[20] The Trac Project.

[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.

[23] Drupal - Open Source CMS, September 2016.

[24] FreeMind, 2017.

[25] Responsibility assignment matrix, September 2017. Page Version ID: 802846049.

[26] Associated Press. Yahoo punishes CEO Marissa Mayer over hacks that cost firm $350 million.

[27] Atlassian. JIRA Software - Issue & Project Tracking for Software Teams.

[28] AXIS Security Consultants and XiSEC Consultants Ltd. RA2 art of risk V 1.1 :: IT.CS.

[29] BSI. *Threats Catalogue – Elementary Threats.* BSI, Bonn, 2011.

[30] Nicholas G. Carr. IT Doesn't Matter. *Harvard Business Review*, May 2003.

[31] Combodo. ITop: ITIS open source ITIL software.

[32] Kosutic Dejan. Free List of Information security threats and vulnerabilities.

[33] Flexera Software. Corporate Software Inspector.

[34] Free RW-Soft. Personální audit, SW a HW audit | AW Caesar evidence počítačů, SW a licencí.

[35] FreeRW Soft. Evidence počítačů, SW, licencí, ITSM, ITIL, SAM.

[36] M. Garsoux. COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing - An overview, 2013.

[37] Gary Hinson. Analog Risk Assessment method, ARA.

[38] IDG. 2011 State of the CIO Survey.

[39] IDG. "State of the CIO 2008"Data Shows CIO Salaries, Influence Rising.

[40] ISACA. COBIT 5 Mapping Exercise for Establishing Enterprise IT Strategy.

[41] ISO27k Implementation Forum. ISMS Implementation and Certification Process v3.

[42] Robert S. Kaplan and David P. Norton. The Balanced Scorecard - Measures That Drive Performance. *Harvard Business Review*, (1):71–79, 1992.

[43] G. L. Kovacich. *Průvodce bezpečnostního pracovníka informačních systémů.* UNIS Publishing, Brno, 2000.

[44] Fabian Lange. Išikawův fishbone diagram příčin a následků, December 2010.

[45] Metacomet. Paretův graf, March 2006.

[46] Microsoft. Microsoft Baseline Security Analyzer 2.3 (for IT Professionals).

[47] Microsoft. Přehled služby Microsoft Intune.

[48] Kevin Mitnick and Wiliam L. Simon. *Umění klamu.* HELION, Praha, 2003.

[49] 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.

[50] MKLab. StarUML 2.

[51] Moodle. Moodle project dasboard.

[52] J. Nenadál. *Měření v systémech managementu jakosti.* Management Press, Praha, 2 edition, 2004.

[53] J. Nenadál, D. NOSKIEVIČOVÁ, R. PETŘÍKOVÁ, J. PLURA, and J. TOŠENOVSKÝ. *Moderní management jakosti.* Management Press, Praha, 2008.

[54] NIST. *NIST SP 800-30 Guide for Conducting Risk Assessments.* NIST, Washington, 2012.

[55] OMG. UML 2.5.

[56] Qualys. Vulnerability Management.

[57] Rapid 7. Nexpose - Your on-prem vulnerability scanner.

[58] Joseph Schmuller. *Myslíme v jazyku UML: knihovna programátora.* Grada, Praha, 2001. Google-Books-ID: TUZTywAACAAJ.

[59] Martyn Williams. PlayStation Network hack will cost Sony $170m.

[60] 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.

[61] ČSN. Čsn en 61025 analýza stromu poruchových stavů (fta).

[62] ČSN. Čsn en 6205 techniky analýzy spolehlivosti - analýza stromu událostí (eta).

[63] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 1: Obecné principy.

[64] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 3: Hmotné škody na stavbách a ohrožení života.

[65] ČSN. Čsn en 62305-1 ed. 2 ochrana před bleskem - Část 4: Elektrické a elektronické systémy ve stavbách.

[66] ČSN. Čsn en 62305-2 ed. 2 ochrana před bleskem - Část 2: Řízení rizika.

[67] Pavel Šenovský. *Expertní systémy.* VŠB-TU Ostrava, Ostrava, 2007.

[68] Pavel Šenovský. *Bezpečnostní informatika II.* VŠB-TU Ostrava, Ostrava, 5 edition, 2012.

[69] Pavel Šenovský. *Modelování rozhodovacích procesů.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 4 edition, 2015.

[70] Pavel Šenovský. *Počítačové sítě a ochrana dat.* VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2015.

Seznam zkratek

AD Active Directory. 51, 53, 105

ARA Analog Risk Assessment Method. 70, 72, 105

B2B Business to Busines. 34, 105

BI Bezpečnostní inženýrství. 9, 105

BPL Bezpečnostní plánování. 9, 105

BRA Binary Risk Analysis. 69, 72, 105

BSC Balance Score Cards. 96, 101, 105

CASE Computer Aided System Engineering. 51, 105

CBA Cost-Benefit Analysis. 66, 105

CEO Chief Executive Officer. 17, 18, 105

CERT Computer Emergency Response Team. 17, 18, 105

CFO Chief Financial Officer. 17, 18, 105

CIO Chief Information Officer. 5, 17–19, 29, 30, 105

CISO Chief Information Security Officer. 17–19, 29, 40, 105

CIT Centrum informačních technologií. 30, 105

CMDB Configuration Management Database. 53–55, 59, 105

CMS Content Management System. 27, 42, 105

COBIT Control Objectives for Information and Related Technologies. 93, 105

COO Chief Operation Officer. 17–19, 105

CSIRT Computer Security Incident Response Team. 17, 18, 105

CSO Chief Security Officer. 17–19, 29, 105

DMS Document Management System. 27, 105

EAL Evaluation Assurance Level. 14, 105

EPS elektrická požární signalizace. 17, 105

ERP Enterprise Rosource Planning. 50, 105

ETA Event Tree Analysis. 46, 48, 105

FMEA Failure Mode and Effect Analysis. 74, 76, 105

FTA Fault Tree Analysis. 46, 48, 105

GEIT Governance of Enterprise IT. 95, 105

GRC Governance, Risk and Compliance. 18, 105

HIM hmotný investiční majetek. 50, 105

HRA Human Reliability Analysis. 46, 105

IA information assurance. 17, 105

ICS Industrial Control System. 93, 105

IDM identity management. 17, 18, 42, 43, 53, 58, 105

IDS Intruder Detection System. 17, 18, 105

IP Intelectual Property. 46, 105

IPS Intruder Prevention System. 17, 18, 105

ISACA Information Systems Audit and Control Association. 93, 105

ISMS Information Security Management System. 5, 9, 15, 16, 35–42, 53, 66, 67, 105

ISOC Information Security Operations Center. 17, 18, 105

ISP Internet Service Provider. 14, 105

IT Informační technologie. 105

ITSM IT Service Management. 59, 105

LDAP Lightweight Directory Access Protocol. 53, 105

LRC Linear Responsibility Chart. 98, 105

MCA Multi-Criteria Analysis. 67, 105

MDA Model Driven Approach. 50, 105

MTBF Mean Time Between Failures. 45, 105

NBU Národní bezpečnostní úřad. 41, 105

NIM nehmotný investiční majetek. 50, 105

OMG Object Management Group. 50, 105

PCS poskytovatel certifikačních služeb. 14, 105

PDCA Plan Do Check Act. 36, 38, 39, 105

PSN PlayStation Network. 66, 105

RAKOS Rada pro koordinaci a strategii ICT. 5, 29, 30, 105

RRIT Rada pro rozvoj informačních technologií. 5, 29, 30, 105

RTP Risk Treatment Plan. 36, 37, 45, 46, 105

SCM Supply Chain Management. 41, 105

SIEM Security Information and Event Management. 105

SOA Study of Applicability. 36, 37, 41, 105

TBOM Technická bezpečnost osob a majetku. 9, 105

TDD Test Driven Development. 105

UAC User Access Control. 23, 105

UML Unified Modeling Language. 50–52, 105

USD Unified States Dollar. 105

UTM Unified Threat Management. 105

VLE Virtual Learning Environment. 28, 105

Rejstřík