Nástroje pro provádění analýzy rizik a možnosti jejich využití v souladu s legislativou EU.

Risk analysis tools and their use in accordance with European Union's legislation.

Bc. Tomáš Račák

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš RAČÁK**
Osobní číslo:	**A09487**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Nástroje pro provádění analýzy rizik a možnosti jejich využití v souladu s legislativou EU.**

Zásady pro vypracování:

1. **Poveďte literární rešerši na zvolené téma.**
2. **Vypracujte přehled vhodných softwarových nástrojů pro analýzu rizik.**
3. **Formou projektu navrhněte a realizujte analýzu informačně bezpečnostních rizik.**
4. **Proveďte diskusi nad zvoleným řešením.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČERMÁK, Miroslav. Řízení informačních rizik v praxi . 1. Brno : Tribun EU, 2009. 134 s. ISBN 978-80-7399-731-1.**
2. **DOUCEK, Petr ; NOVÁK, Luděk; SVATÁ, Vlasta. Řízení bezpečnosti informací . Praha : Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.**
3. **KAFKA, Tomáš. Průvodce pro interní audit a risk management . Praha : C.H. Beck, 2009. 167 s. ISBN 978-80-7400-121-5.**
4. **Kolektiv autorů. Příručka manažera I – Informační bezpečnost. Praha : TATE International s.r.o., 2001. 124 s. ISBN 80-902858-4-8.**
5. **Kolektiv autorů. Příručka manažera IX – Business Continuity Management. Bratislava : TATE International Slovakia s.r.o., 2008. 276 s. ISBN 978-80-969747-2-6.**
6. **Kolektiv autorů. Příručka manažera X – Outsourcing. Praha : TATE International s.r.o., 2008. 268 s. ISBN 978-80-86813-16-5.**
7. **SMEJKAL, Vladimír; RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. Praha : Grada Publishing a.s., 2006. 296 s. ISBN 80-247-1667-4.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá nástroji použitelnými k analyzování rizik a dalšími možnostmi jejich využití v souladu s legislativou Evropské unie. Literární rešerše okrajově nastiňuje téma analyzování a řízení rizik s ohledem na evropskou legislativu touto problematikou se zabývající. Praktická část práce se pak zabývá vybranými softwarovými nástroji vhodnými k provádění analýzy. V závěru práce je uvedena pilotní studie a analýza rizik ve vybrané firmě zabývající se výrobou kovového nábytku.

Klíčová slova:

Riziko, řízení rizik, metodika analýzy rizik, kvantitativní metoda, kvalitativní metoda, RANIT, CRAMM, @RISK, RiskIT, COBIT, RiskPAC, RiskWatch, aktivum, hrozba, zranitelnost, dopad, opatření, komponenta.

ABSTRACT

This paper deals with risk analysis tools and their usage in context of European Union. Theoretical part focuses on risk analyzing and risk management in framework of European legislation. Practical part contains comparison of several software products applicable for risk analyzing. In the end work is presented case study focused on risks associated with data assets in unnamed company, which is producing metal garden furniture.

Keywords: Risk, risk management, methodology of risk analysis, quantitative and qualitative methods, RANIT, CRAMM, @RISK, RiskIT, COBIT, RiskPAC, RiskWatch, assets, threats, vulnerability, impacts, measures, components.

Tímto bych chtěl poděkovat své rodině a přítelkyni za podporu během studia a psaní této práce, bez nichž bych to určitě nezvládnul.

Mé poděkování také patří doc. Mgr. Roman u Jaškovi, Ph.D za odborné vedení a rady při zpracování této práce.

„Učenci a vědci! Nebojte se létat! Žádný učený z nebe nespadne!“

Vlasta Burian

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Ochrana dat a informací je dnes již neoddělitelnou součástí celkové bezpečnosti informačního systému a informačních technologií v jednotlivých organizacích. IB se stává stále diskutovanější oblastí, i proto je pro mne toto téma velmi atraktivní. Roste obecný zájem o aplikaci informační bezpečnosti ve firmách zabývajících se celou škálou služeb. Ať už je k tomu vede již nastalý problém, únik informací, nenávratná a nenahraditelná ztráta dat, díky které firma málem ukončila svou činnost, či zájem ochránit svá data a obchodní tajemství ve stále sílícím konkurenčním prostředí.

Aby bylo možné správně implementovat zabezpečení IS a IT, je nutné se seznámit s hlavními základy ať už bezpečnosti IT či IS. Pojem bezpečnosti informačního systému bývá u většiny lidí chápán různě, nejčastěji mají společnosti za to, že sem spadá pouze bezpečnosti informací uchovávaných v podnikovém ERP systému.

Je nutné sem ovšem zařadit mimo jiné i komunikační bezpečnost, ochranu před přírodními katastrofami, fyzickou i personální bezpečnost atd.

Často se stává, že bývá tato bezpečnost zaměřena pouze na části IS, jež jsou provozovány za pomocí výpočetní techniky. K čemu nám, ale je dokonale zabezpečený výpočetní systém, když se volně po firmě pohybují citlivé listiny. Které mohou být snadno vyneseny z organizace.

Informace jsou jedním ze základních a klíčových zdrojů každé organizace. Útočníci při snaze narušit tuto podnikovou bezpečnost přicházejí stále s lepšími a sofistikovanějšími útoky, které mohou být velmi nebezpečné.

S rostoucí tendencí chránit takováto data se objevují seznamy hrozeb, zranitelností a v konečném důsledku dochází ke stále více útokům na tyto informace, ať už je to z vnějšího nebo vnitřního prostředí.

I. TEORETICKÁ ČÁST

1 STRUČNÝ ÚVOD DO ANALÝZY RIZIK

Tato kapitola shrnuje základy analýzy rizik, definuje základní pojmy a ve stručnosti charakterizuje jednotlivé fáze celého procesu analyzování rizik.

Aby měla analýza rizik smysluplný výstup je nejprve nutné přesně a jasně definovat cíle bezpečnostní politiky a stanovit způsob, jakým bude tohoto cíle dosaženo. Výstupem analýzy rizik je pak detailní rozbor hrozeb, kterým je společnost vystavena. A jaké mohou mít tyto hrozby důsledky. Výsledkem celého snažení je pak eliminace potenciální přímých i nepřímých ztrát, dále stanovit jak velká je hrozba zneužití určité zranitelnosti a jaký to bude mít dopad na firmu.

1.1 Základní pojmy používané v analýze rizik

Při analýze rizik se nejčastěji používají následující pojmy [1]:

- **aktiva (asset)** - veškerý hmotný i nehmotný majetek, kterému společnost připisuje nějakou hodnotu a který chce odpovídajícím způsobem chránit,
- **hrozba (threat)** – událost způsobující narušení integrity, důvěryhodnosti a dostupnosti aktiva,
- **zranitelnost (vulnerability)** – aktivum nebo slabina na úrovni logické, fyzické nebo administrativní bezpečnosti, často bývá zneužita hrozbou,
- **riziko** - pravděpodobnost zneužití zranitelnosti hrozby, která způsobí přerušení integrity, důvěrnosti a dostupnosti,
- **opatření (countermeasure)** – snižuje zranitelnost systému na úrovni fyzické, logické nebo administrativní bezpečnosti a zároveň chrání před danou hrozbou.

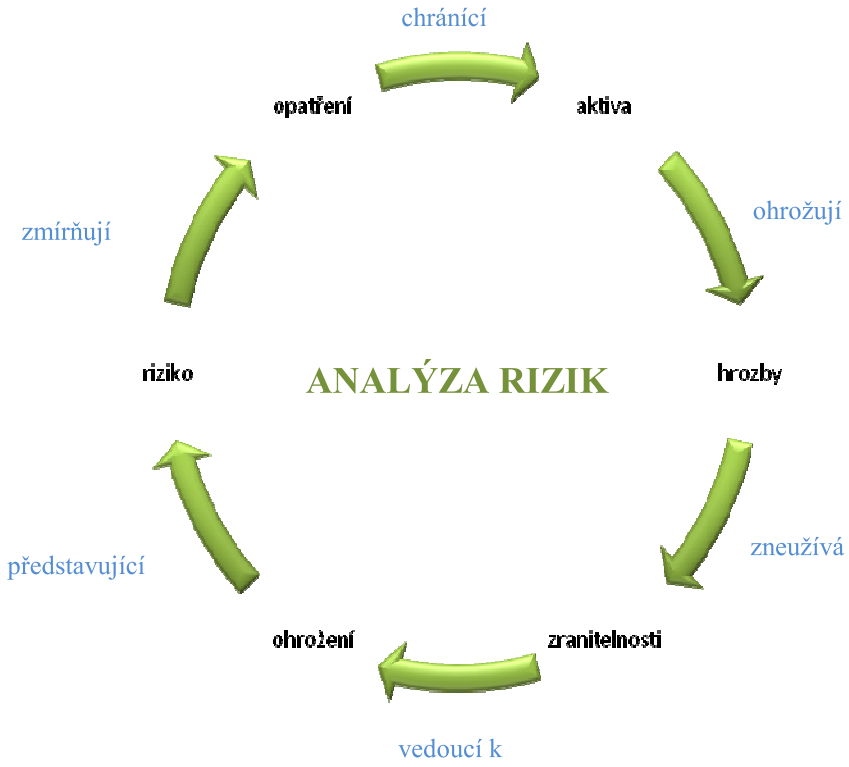
Je potřeba rozlišovat a vzájemně nezaměňovat pojmy *riziko* a *hrozba*. Hrozba totiž může být zdrojem jednoho i více rizik, ale sama o sobě riziko nepředstavuje. Ta pouze zneužívá zranitelnosti, která pak vede k ohrožení, tedy riziku. [1]

Také se můžeme potkat s dalšími pojmy, které ovšem už nejsou tak časté jako předchozí, ale přesto stojí za to se o nich zmínit[1]:

- **ohrožení (exposure)** – říká nám, že existuje určitá zranitelnost, kterou může hrozba zneužít,

- **narušení (breach)** – stav, kdy dojde k překonání bezpečnostních opatření v důsledku narušení integrity, důvěrnosti nebo dostupnosti aktiva.

Vzájemné vazby mezi těmito pojmy nejlépe vystihuje *Obrázek 1*.



Obrázek 1 Fáze analýzy rizik [1]

2 JAK SE ŘEŠÍ INFORMAČNÍ BEZPEČNOST

Následující schéma (*Obrázek 2*) ukazuje posloupnost šestice na sebe navazujících procesních kroků vycházejících z mezinárodního bezpečnostního standardu ISO 13335. Ve schématu postupujeme postupně o shora dolů. Za určitých okolností se vracíme opět zpět k předchozímu kroku. Obecně platí, že proces bezpečnosti musíme kontinuálně opakovat.[10]

Obrázek 2 Schéma posloupnosti řešení bezpečnosti [10]

2.1 Cíle a strategie řešení bezpečnosti IS

Hlavním úkolem je určit si přesně a jednoznačně cíl a jakou cestou se k dosažení cíle vydáme. Obecně můžeme říct, že je potřeba chránit všechny druhy informací, které souvisejí s existencí společnosti. V některých případech je však nutné omezit se pouze na některé skutečnosti, tak abychom urychlili řešení aktuálních problémů spojených s informační bezpečností společnosti.

Pro většinu společností vyhovuje tato definice: „*Základním cílem je eliminovat případné přímé a nepřímé ztráty způsobené zneužitím, poškozením, zničením nebo nedostupnosti*

informací, vytvořením uceleného, nákladově optimalizovaného a efektivně fungujícího systému řízení bezpečnosti informací“. [10]

Cílem projektu je dále:

- prozkoumat a následně zhodnotit stávající úroveň informační bezpečnosti,
- definovat úroveň a principy řízení informační bezpečnosti,
- správně navrhnout postup pro dosažení cílů společnosti a požadovanou úroveň zabezpečení,
- nastavit prostředí tak, aby bylo možné informační bezpečnost udržovat a neustále prohlubovat.

Také je nutné stanovit:

- v jakých hranicích se budeme informační bezpečností zabývat,
- jaké typy informací (dat) do našeho řešení zahrneme,
- jaké části náš informační systém obsahuje,
- jakých organizačních složek společnosti se bude týkat,
- případně, zda budou do procesu zařazeny i dceřiné společnosti, dodavatelé či partneři.

Ideálním případem je sepsat závazný dokument s postupem celkové zabezpečovací politiky firmy. Jakým způsobem se bude postupovat a co všechno bude obsahem daného projektu.[10]

2.2 Analýza rizik IS

Analýza rizik informačního systému je klíčová aktivita v procesu bezpečnosti, která nám dává odpověď na tři základní otázky. [10]

1. Co se může stát, pokud nebudou informace dostatečně chráněny?
2. Jakým způsobem můžeme porušit bezpečnost informací?
3. Jaká je pravděpodobnost, že tato situace nastane?

Aby bylo možné zjistit, jaké vlivy působí na danou organizaci je potřeba provést analýzu rizik. Cílem analýzy rizik je identifikovat a kvantifikovat rizika, tedy zhodnotit velikost

dopadu na pravděpodobnost výskytu daného rizika, následně rozhodnout o opatřeních, která by snížila hodnotu rizik na minimum. [10]

Výstupem analýzy rizik by se měl stát přehledný dokument, eventuálně dokumenty, obsahující popis úrovně ochrany stávajícího systému, výsledky analýzy a následná opatření pro zvýšení ochrany. [10]

Pro provedení analýzy rizik je nutné mít k dispozici dostatek času, protože taková analýza pro větší organizace je časově náročná a různé hrozby představují různou míru rizika, které je u každé společnosti individuální. V takových organizacích není potřeba provádět podrobnou analýzu rizik. Standard ISO/IEC TR 13335 nám definuje *čtyři způsoby provádění rizik*, vhodných pro různé typy organizace. Nyní si jednotlivé přístupy popíšeme blíže. [10]

2.2.1 Základní přístup – metoda rychlého zavedení sady bezpečnostních opatření bez podrobnější analýzy

Jedná se o sadu bezpečnostních opatření přejatých z katalogu nápravných opatření, který je součástí některých softwarových nástrojů. Z daných opatření jsou zvolena ta, která jsou vhodná pro danou organizaci a která dosud nebyla implementována. Tato metodika je nejvhodnější pro malé organizace s nízkou závislostí na IT. [10]

Výhodou takového přístupu je zejména jeho rychlost. Pro aplikaci analýzy není potřeba mnoho zdrojů. [10]

Nevýhodou této metody je implementace sady opatření, což může vést k nastavení některých opatření zbytečně vysokých a jiných naopak příliš nízkých. To samozřejmě může vést k dodatečnému zvyšování nákladů na implementaci bezpečnostní politiky. [10]

2.2.2 Neformální – pragmatický – přístup k analýze rizik

Tento přístup je postaven na rychlé, orientační analýze založené na definovaných metodologiích, vychází ze zkušeností jednotlivců a znalosti prostředí. *Výhodou* je rychlost a nízké náklady na realizaci. [10]

Tento způsob provádění analýzy rizik má však i své nevýhody, např. [10]:

- závislost na znalostech a zkušenostech jednotlivců – možnost opomenutí významných proměnných sledovaného procesu,

- špatná obhajitelnost výsledků analýzy založené na zkušenostech, ne na faktech.

Existuje několik způsobů provedení této analýzy, nicméně v literatuře je doporučováno provádět tuto analýzu pouze jako první krok analýzy rizik tam, kde je nutné urgentně zvýšit úroveň bezpečnosti. Níže je uveden jeden z možných postupů takovéto analýzy.[10]:

1. definice rizik a oblastí hrozeb,
2. provedení odhadu dopadu každého rizika a pravděpodobnosti jeho výskytu, viz. Tabulka 1, *Tabulka 2* a *Tabulka 3*
3. identifikace ochranných opatření pro odstranění či zmírnění určených rizik
4. posouzení zbytkového rizika

Tabulka 1 Rozhodovací tabulka pro posuzování rizik a pravděpodobnosti jejich výskytu [10]

pravděpodobnost	dopad				
	katastrofický	kritický	vážný	okrajový	zanedbatelný
časté	nepřijatelné	nepřijatelné	nepřijatelné	poškozující	poškozující
pravděpodobné	nepřijatelné	nepřijatelné	poškozující	poškozující	přijatelné
příležitostné	nepřijatelné	poškozující	poškozující	přijatelné	přijatelné
málo pravděpodobné	poškozující	poškozující	přijatelné	přijatelné	zanedbatelné
nepravděpotoné	poškozující	přijatelné	přijatelné	zanedbatelné	zanedbatelné

Tabulka 2 Příklad definování dopadu rizika (náklady jsou definovány jako násobek proměnné V)[10]

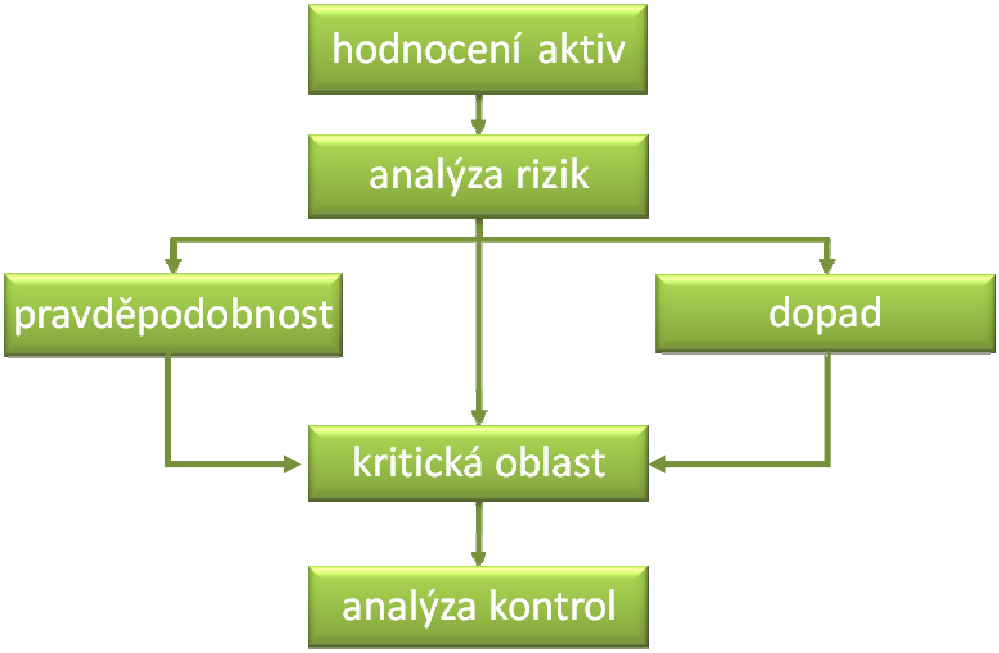
popis	návod	náklady
katastrofický	ztráta klíčového systému, nevratná situace, přerušení provozu	100*V
kritický	významné škody, dlouhodobější ohrožení provozu	10*V
vážný	přerušení provozu, je třeba aktivace havarijních plánů	V
okrajový	drobná škoda, která může být napravena v rámci pravidelné údržby	0,1*V
zanedbatelný	zanedbatelné následky	0,01*V

Tabulka 3 Příklad popisu výše rizika [10]

riziko	popis
nepřijatelné	nelze tolerovat, riziko musí být odstraněno
poškozující	je vhodné riziko odstranit, ale je třeba zvážit náklady s tím spojené
přijatelné	riziko je přijatelné, pokud je monitorováno
zanedbatelné	riziko není třeba analyzovat

2.2.3 Podrobná analýza rizik - formální přístup

Jedná se o detailní analýzu rizik, kdy se provádí hodnocení aktiv, hrozeb a zranitelností. Tato metoda AR se řadí do nejpřesnějších, ovšem finančně nejnáročnějších. [10]



Obrázek 3 Postup analýzy rizik dle standardu BS7799:2 [12]

Krok *hodnocení a identifikace aktiv* zahrnuje následující kroky [10] [12]:

- vymezení části IS, kde bude AR provedena,
- identifikace aktiv,
- ohodnocení aktiv finančními i nefinančními měřítky,
- sběr informací za pomocí dotazníků, formulářů, apod.

Dle původu a úmyslu je třeba *hrozby posoudit* [10] [12]:

1. identifikace kategorií hrozeb dle katalogu hrozeb a normy ISO/IEC TR 13335,

2. odhad pravděpodobnosti výskytu hrozby dle jejího typu (interní, externí, přírodní, fyzické…),
3. vytvoření seznamu hrozeb s evidencí pravděpodobností jejich výskytu

Dalším krokem při provádění analýzy rizik je provedení *odhadu zranitelnosti*, kdy jsou odhalena slabá místa na úrovni fyzické, organizační, procedurální, personální, administrativní, řídící, softwaru, hardwaru nebo informací. Je proveden odhad stupně zranitelnosti a proveden rozbor možností využití jejich zranitelnosti. Slouží jako podklad pro vytvoření rizikového (havarijního) scénáře. [10]

Poté co je odhalena zranitelnost systému, jsou *vytvořena ochranná opatření*. Kontrolní opatření jsou shrnuta a rozdělena dle důležitosti a typu na [10]:

- preventivní – plán preventivní ochrany,
- následná – havarijní plán, plán obnovy.

Výsledkem je pak přehled stávajících i plánovaných ochranných opatření, včetně plánu implementace a užívání. [10]

Posledním z kroků je *akceptování rizik,* kdy není cílem rizika eliminovat v celém rozsahu, ale pouze zmírnit jeho následky. Jsou identifikována zbytková rizika po implementaci navrhovaných opatření. [10] [12]

Tabulka 4 Rozhodovací tabulka pro analýzu zbytkových rizik [10]

hrozba	zranitelnost		
	nízká	střední	vysoká
velmi nízká	přijatelná	přijatelná	nepřijatelná
nízká	přijatelná	poškozující	poškozující
střední	přijatelná	poškozující	poškozující
vysoká	poškozující	nepřijatelná	nepřijatelná
velmi vysoká	poškozující	nepřijatelná	nepřijatelná

Míra rizika udává význam implementace nových bezpečnostních opatření. [12] Správný výběr ochranného opatření ulehčuje následující rozhodující matice.

Obrázek 4 Rozhodovací schéma pro výběr ochranných opatření [12]

2.2.4 Kombinovaný přístup

Podrobná analýza rizik celého subjektu je zdlouhavý proces, proto se na základě provedené orientační analýzy zjišťují kritická aktiva, která působí na organizaci či procesy v ní. Detailní analýza se pak aplikuje pouze na důležité části. [10]

2.3 Bezpečnostní politika IS

Další fází procesu zavádění informační bezpečnosti v podniku je ustanovení bezpečnostní politiky. V tomto kroku vzniká základní dokument zabývající se celkovou bezpečnostní politikou. Dokument se po přijetí managementu společnosti stává závazným a má dlouhodobou platnost pro celou společnost, musí být v souladu s jejím řádem. Definuje všechny aktivity a východiska v oblasti informační bezpečnosti a jeho hlavním cílem: [10]

- definovat hlavní cíle pro ochranu informací,
- vymezení citlivých dat, stanovení míry zabezpečení a bezpečnostních mechanismů,
- stanovení zodpovědnosti a pravomocí pro subjekty a objekty IS.

2.4 Bezpečnostní standardy

Aby bylo možné realizovat cíle stanovené v rámci bezpečnostní politiky, je nutné stanovit bezpečností standardy a detailně definovat jednotlivé procedury, které poskytují podrobné informace nutné k dosažení cílů bezpečnostní politiky. [10]

Na rozdíl od bezpečnostní politiky, která má spíše dlouhodobý charakter, jsou standardy více dynamické a přizpůsobují se změnám v činnostech a procesech společnosti i se změnami informačních technologií. Styl standardů by měl odpovídat firemní kultuře a měl by být jasně stanovený, čitelný a v přiměřeně stručný. Standardizované by měly být všechny procesy a aspekty týkající se bezpečnosti, nejen počítačové, ale i fyzické, postupy, personální otázky apod. Vytvoření standardu vždy reaguje na dané bezpečnostní riziko a stanovuje, jakým způsobem bude toto riziko ve společnosti pokryto. Příkladem takovýchto bezpečnostních standardů mohou být např. [10] :

- postup administrace systémů,
- záložní postupy a postupy obnovy,
- provádění auditů a monitoringu systémů,
- reakce na bezpečnostní incidenty,
- řízení změn,
- provádění analýzy rizik a stanovení jejích period, apod.

Veškerá aplikace standardů v dané společnosti je závislá jak na stávajících, tak i na budoucích procesech společnosti i na její technické infrastruktuře. [10]

2.5 Implementace bezpečnosti

V této fázi se informační bezpečnost přenáší do praxe a přivádí se v „život“. Postupně se implementují dílčí projekty a zavádí se systém monitorování, bezpečnostního vzdělávání, zavádí se informační bezpečnost, stanovuje se rozsah politiky atd. Při implementaci může docházet k mnoha chybám, jednou z nejzávažnějších je, že implementátor ustoupí a zavádí mnoho kompromisů, což může mít negativní vliv na výkonnosti IS. Další častou chybou je nedostatečná propagace BP a kopírování špatně definovaných vzorů. [10]

2.6 Monitoring a audit

Tato fáze je věnována průběžné kontrole provozu IS, dále vyhodnocuje stupeň jejich zabezpečení, dokáže vytvořit adekvátní zpětnou vazbu spolu se všemi fázemi implementace IB, na základě auditů se doporučují nápravná a preventivní opatření systému – zajišťuje se prevence bezpečnostních incidentů, detekce pokusů o průnik do systému a obnova po bezpečnostním incidentu[10].

Při provádění auditů je možné spolupracovat s externími a delegovat tak řešení informační bezpečnosti. Nicméně před tím, než je IB outsourcována je nutno prověřit a zajistit následující[10].

- reference a důvěryhodnost externisty,
- profesní certifikáty řešitelského týmu,
- metodiky řízení a řešení projektů používané řešitelským týmem,
- smluvní podložení ochrany dat a informací,
- ekonomická stabilita dodavatelské firmy.

3 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ A JEHO LEGISLATIVNÍ ZABEZPEČENÍ

Trendem posledních let je stále vzrůstající počet firem zabývajících se činností související s informačními technologiemi a informacemi samotnými. Proto také vyvstala potřeba tyto informace chránit a zabezpečit tak, aby bylo riziko úniku informací minimální. Aby měla tato ochrana dat nějaký řád, začaly vznikat nejrůznější systémy řízení bezpečnosti informací, které byly posléze standardizovány jak na úrovni státních tak i mezinárodních norem.

3.1 Tvorba norem v oblasti bezpečnosti IT

Normy zabývající se bezpečností zahrnují [10]:

- bezpečnostní techniky,
- obecné bezpečnostní protokoly,
- specifické aplikační protokoly.

Mezinárodní normy jsou vyvíjeny a vydávány organizacemi ISO, IEC, ITU a IEEE. Část norem je vydána i pod společnou záštitou těchto organizací – ISO/IEC, ISO/ITU-T. [10] Normy na národních úrovních (např. BSI, ČSNI) pak většinou vychází či dále navazují právě na normy vydané těmito institucemi. Nebo naopak řada národních norem byla zakomponována či dále rozšířena do norem nadnárodních.

Výjimkou však mohou být americké normy ANSI a NIST určené primárně pro uplatnění na americkém území, ale díky nadnárodním korporacím a společnostem mají mezinárodní dosah. Kromě těchto dokumentů ještě existují normy s evropskou působností CEN/CENELEC.[10]

3.2 Normy upravující tvorbu systému řízení bezpečnosti informací

Zavádění systému řízení bezpečnosti informací může být prováděno dle metodiky vycházející z následujících standardů:

- ČSN ISO/IEC 17799
- ČSN ISO/IEC 27001

- ČSN ISO/IEC TR 13335
- ČSN ISO/IEC 15408
- ČSN EN ISO 19011

Na tyto standardy se odvolávají i legislativní předpisy ČR, např. zákon o utajovaných informacích 412/2005 Sb. [9]

Samozřejmě jednotlivé projekty zaměřené na zavádění do praxe se liší a nemusí se striktně držet těchto norem, mohou být dle potřeby korigovány a upřesňovány, aby vyhovovaly i jiným standardům či legislativě. [9]

3.2.1 ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT

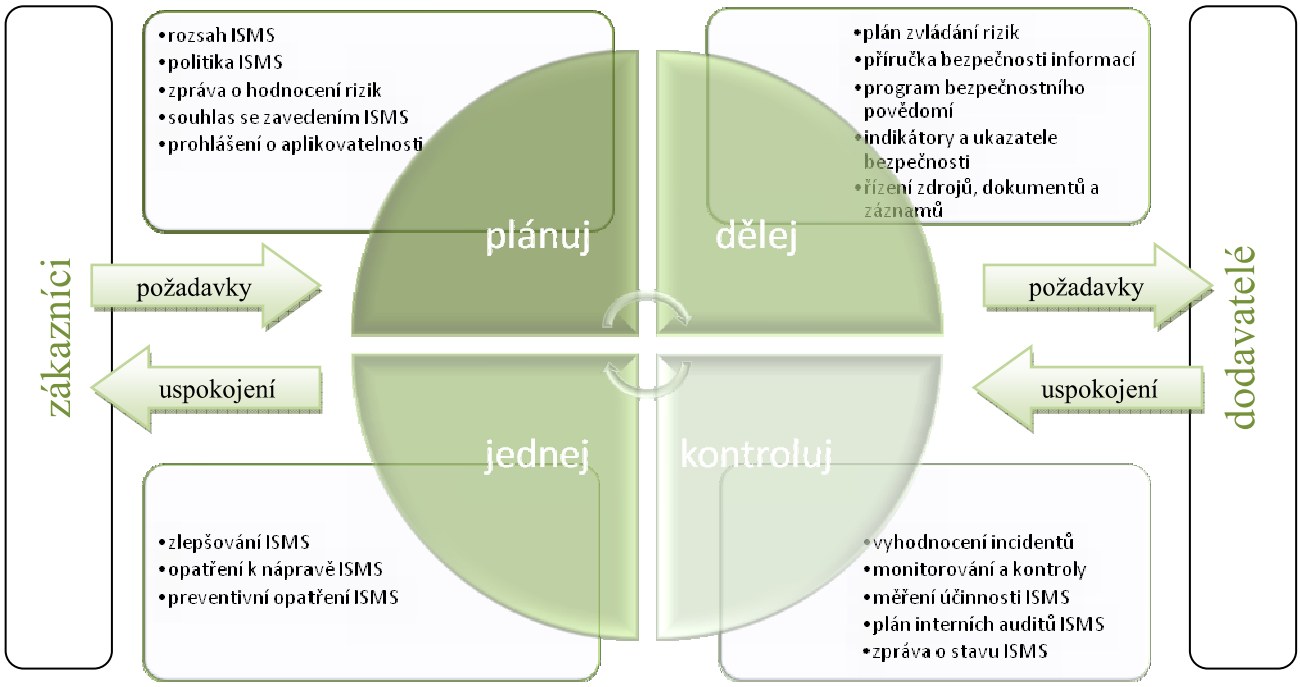
Tato směrnice sestává ze čtyř částí [13]:

1. ISO/IEC TR 13335-1 **Pojetí a modely BIT** – obsahuje popis základní koncepce a modelů používaných pro správu a BIT a její vztah ke správě IT, dále jsou definovány základní pojmy BIT.
2. ISO/IEC TR 13335-2 **Řízení a plánování BIT** – popisuje plánovací a řídící aspekty IT, tuto část lze aplikovat na organizaci a řízení BIT v organizaci. Jsou definovány role a odpovědnosti zainteresovaných pracovníků.
3. ISO/IEC TR 13335-3 **Techniky pro řízení BIT** – obsahuje přehled nejdůležitějších bezpečnostních technik, včetně struktury a kategorizace, rovněž jsou zde uvedeny způsoby provádění analýzy rizik a volba strategie.
4. ISO/IEC TR 13335-4 **Výběr bezpečnostních opatření** – má formu doporučení výběru bezpečnostních protiopatření s ohledem na specifické potřeby organizace.

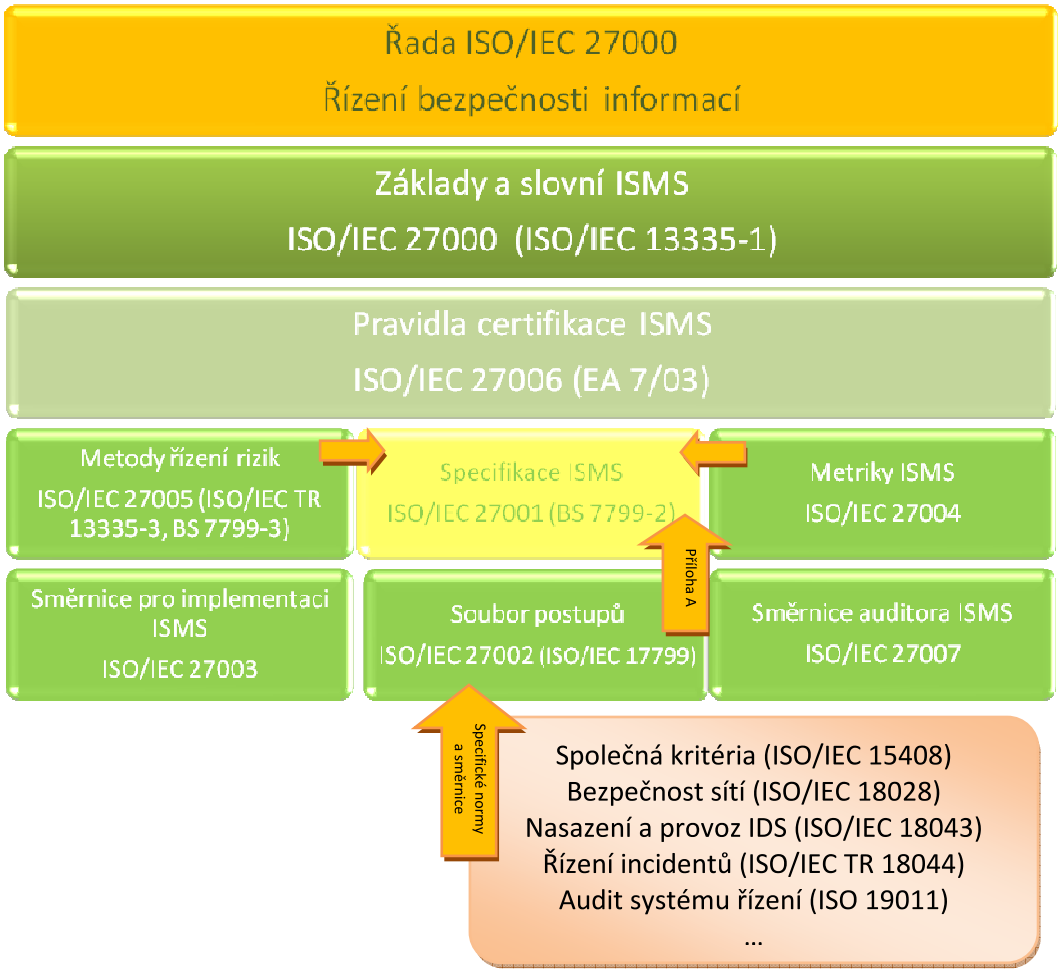
3.2.2 Rodina norem ISO/IEC 27000 Řízení bezpečnosti informací

Normy řady ISO/EC 27000 je ideově postavena na koncepci PDCA (*Obrázek 5*) a jejím základem jsou normy uvedené ve schématu (

Obrázek 6) níže. Sama norma ISO/EC 27000 obsahuje základy a slovník pro SŘBI. Stavebním kamenem je pak norma ISO/IEC 27001 **Systém řízení bezpečnosti informací - požadavky**, vycházející z britského standardu BS 7799-2, obsahující definici systému. [6]

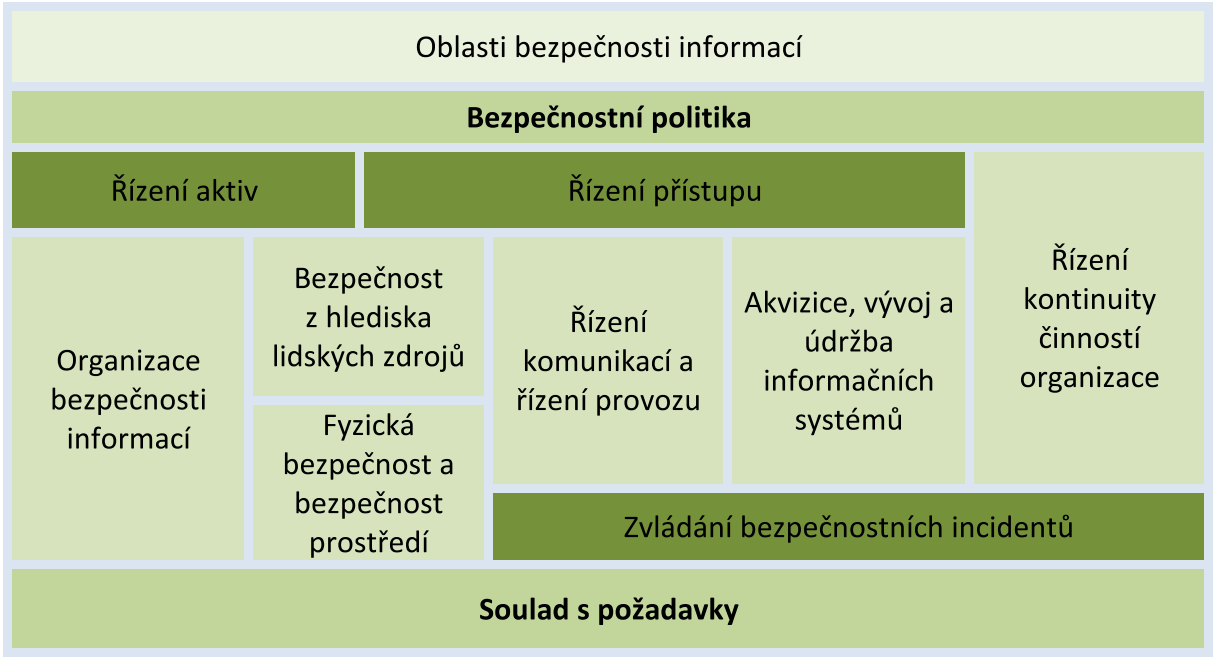


Obrázek 5 Model PDCA [4]



Obrázek 6 Koncepce řady norem ISO/IEC 27000 [6]

Další část této skupiny norem je norma ISO/IEC 27002 **Soubor postupů pro řízení bezpečnosti informací,** obsahuje detailní výklad vhodných bezpečnostních opatření (rozdělení opatření do jednotlivých skupin je uvedeno v následujícím schématu (*Obrázek 7*). Před zařazením do řady norem ISO/IEC 27000 figurovala pod označením ISO/IEC 17799:2005.



Obrázek 7 Oblasti bezpečnosti informací [5]

Dalším dílem řady je norma ISO/IEC 27003 **Směrnice pro implementaci SŘBI**, obsahující vhodná nicméně nezávazná doporučení a návody. [6]

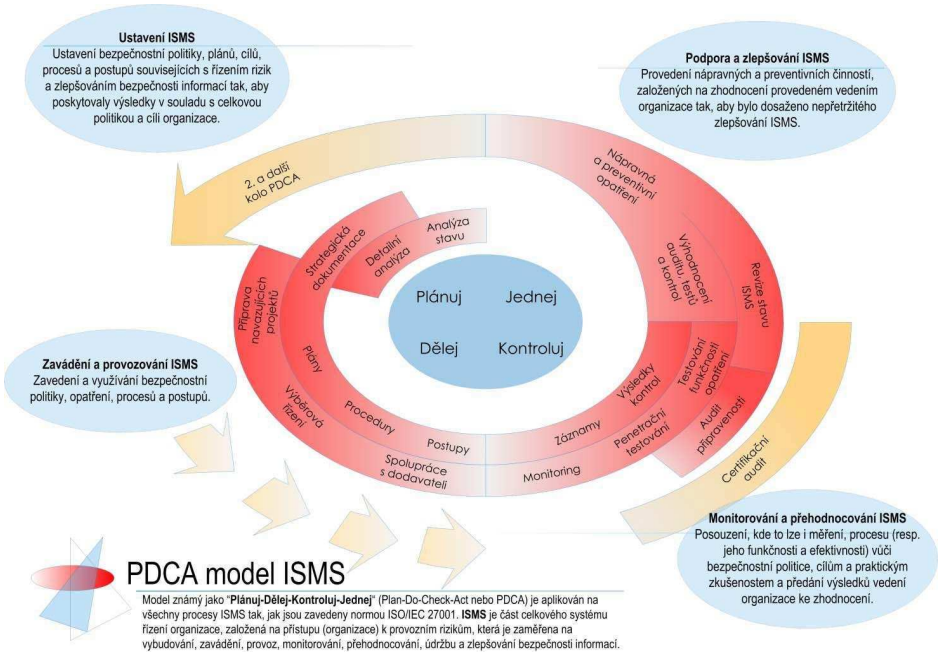
ISO/IEC 27004 **Měření účinnosti řízení BI** upřesňuje pravidla a způsoby využívání nástrojů pro sledování účinnosti a efektivnosti zavádění a prosazování ISMS, především je předepsána struktura ukazatelů. [6]

ISO/IEC 27005 **Řízení rizik bezpečnosti informací** definuje pravidla a postupy řízení rizik a obsahuje katalogy hrozeb a zranitelností. Je nástupcem normy ISO/IEC TR 13335-3. [6]

ISO/IEC 27006 **Požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti** – konkretizuje podmínky udělení certifikace ISMS a stanovuje postupy pro certifikační orgány, které poskytují služby spojené s udělením certifikátu ISMS. Nahrazuje evropský dokument EA 7/03 z roku 2000. [6]

Dalším dokumentem této řady je ISO/IEC 27007 **Směrnice auditora ISMS**, která stanovuje postupy a pravidla pro provádění jak interních, tak i externích auditů sytému ISMS. [6]

Kromě těchto norem jsou dále jako součást norem řady 27000 připravovány normy zabývající se doporučeními a výkladem ISMS pro specifické použití a užším bezpečnostním okruhům. [6]



Obrázek 8 PDCA model ISMS [17]

3.3 Přehled české legislativy zabývající se problematikou bezpečnosti informací a dat [22]

- Zákon č. 148/1998 Sb., o utajovaných skutečnostech.
- Zákon č. 513/1991 Sb., Obchodní zákoník.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů.
- Zákon č. 138/2002 Sb., o regulaci reklamy.
- Zákon č. 227/2000 Sb., o elektronickém podpisu.
- Zákon č. 480/2004 Sb., o službách informační společnosti
- Zákon č. 240/2000 Sb., o krizovém řízení.

4 METODIKY ANALÝZY RIZIK

Přístupy k AR můžeme v zásadě rozdělit do tří skupin [17]:

1. **Dodavatelský přístup** – Hlavní výhodou tohoto přístupu je, že velmi málo zatěžuje danou organizaci. Musí se absolvovat pouze pohovory a dotazníky. Není nutné interesovat vlastní odborníky. Veškerá odpovědnost za provedení je na straně dodavatele. Není nutné vynakládat finanční prostředky na pořízení metodiky nebo nástroje. Tento přístup má však také řadu nevýhod: může docházet k tvorbě nesrozumitelných výstupů, cena poradenské firmy je také poněkud vyšší a a posledním expertem, který napomáhá implementaci, odejde i celé know-how.
2. **Vlastní přístup** – V případě provádění AR vlastními prostředky všichni rozumí výstupním dokumentům, které vznikly při jejím zpracování. Jedná se o nejlevnější metodu, i když je potřeba koupit metodiku nebo nástroj pro vypracování analýzy. Implementátoři dokonale znají prostředí, ve kterém se analýza provádí. Zaměstnanci mívají také větší ochotu komunikovat a spolupracovat se svými kolegy než s neznámými externisty. Nevýhodou ovšem je, že velmi zatěžuje danou organizaci. Nikdy nemáme jistotu, že se ubíráme ke správnému výsledku, pokud organizace nevlastní vlastní odborníky znalé problematiky. Může docházet k neefektivní spotřebě zdrojů a to za předpokladu, že analýzu provádí správce sítě společně se svými každodenními povinnostmi. Také interní pracovníci občas nevidí problémy, které vidí externista.
3. **Partnerský přístup** – Dle mého názoru vůbec nejlepší volba. Všichni aktéři účastnící se projektu rozumí jeho výstupům. Není nutné mít ve svých řadách vlastní odborníky. Odpovědnost za vedení a zavádění bezpečnostní politiky má konzultant. Ve většině případů není nutné nakupovat vlastní metodiku ani nástroj, ale obvykle se nástroj kupuje. Je možné rozdělit náklady do více projektů (např: nákup metodik či nástrojů). Nevýhodou je, že velmi zatěžuje organizaci, ale v tom dobrém slova smyslu **"efektivně"**. Relativně vysoká cena. Pracovník, který je zainteresován do projektu je vyškolen a stává se tak odborníkem a poté organizaci opustí.

Dále v textu je uvedeno členění metod analýzy rizik a stručné charakteristiky jednotlivých metodik.

4.1 Členění metod analýzy rizik

4.1.1 Kvalitativní metody

Pro kvalitativní metody je příznačné, že se rizika **vyjadřují určitou stupnicí** (příkladem může být škála v intervalu od 1 do 10, nebo ohodnocení rizik pravděpodobností dané hodnoty v intervalu od 0 do 1, apod.) Tyto úrovně se v převážné většině určují kvalifikovaným odhadem, jsou **rychlejší, jednodušší**. Mínusem však může být fakt, že jsou i velice **subjektivní**. Často vznikají problémy při zvládání rizik a to především při hodnocení přijatelnosti nákladů, které jsou zapotřebí k eliminaci hrozby, která za pomocí této metody může být charakterizována jako kritická. **Chybí zde jednoznačné finanční ohodnocení** a to znesnadňuje efektivnost kontroly nákladů. [20]

4.1.2 Kvantitativní metody

Kvantitativní metody jsou založeny na **matematickém výskytu rizika** z četnosti výskytu hrozeb a dopadu na ně. Dopad se obvykle vyjadřuje za pomoci finančního ohodnocení např: v CZK nebo EUR. Velmi často se toto riziko vyjadřuje jako roční předpokládaná ztráta vyjádřená konkrétní částkou. Tyto metody jsou **přesnější,** ale zato méně kvalitní, **vyžadují více času a úsilí**, ale **poskytují finanční vyjádření rizik** a to je pro jejich zvládání mnohem výhodnější. [20]

Mezi nevýhody takového přístupu lze zařadit [20]:

- náročnost na provedení a zpracování výsledků,
- formalizovaný přístup, tzn., nemusí být postihnuta všechna specifika sledovaného subjektu.

4.2 Popis jednotlivých metodik AR

4.2.1 @RISK

Jedná se o obecnou metodiku pro kvantitativní analýzu s využitím simulačních metod Monte Carlo (zpracování problematiky do tabulek). Je spíše kvantitativní metoda, která určuje pravděpodobnostní rozdělení hrozeb a rizik. [15]

4.2.2 COBRA

Tato metodika využívá expertního systému pro analýzu rizik. Školitel s pomocí tohoto systému identifikuje stávající hrozby a stanovuje velikost rizika. Systém dokáže také pomoci s návrhem a aplikací nových řešení.

Softwarový nástroj COBRA pro tvorbu této metodiky lze zakoupit v přepočtu za 40 000 CZK a odpovídá normám pro ISO 17799, ISO 27000. [18]

4.2.3 CRAMM

Slouží pro provádění analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních protiopatření, ke stanovení havarijních plánů a určovaní požadavků na informační systém.

4.2.4 Delphi

Takzvaná metoda účelových interview. Hlavním úkolem této metody je dodržení kontaktu mezi jednotlivými respondenty. Jedná se o metodu dotazníků, je zejména vhodná pokud jsou známy informace (např. doba mezi jednotlivými poruchami). Respondenti sepíší rizika a sjednotí jejich přehled společně s odhadem pravděpodobností. Tyto dotazníky poté kolují mezi jednotlivými respondenty a ty si je opravují. Je důležité zachovat anonymitu vyplněných informací. Většinou se tato operace provádí ve 2-3 kolech při dalším nárůstu kol vzrůstá statistická chyba. Touto metodou dochází k relativně přesnému odhadu rizik, informace pomocí jí získané lze poté použít jako základ pro výpočet jednotlivých pravděpodobností a dopadů hrozeb. Je vhodné ji použít, protože dokáže určit co, a za jakých podmínek se může stát. Výhodou je menší spotřeba zdrojů a času.

Je zde kritizována absence finančního vyjádření. V rámci této metody se používají různé inovace, metoda scénářů, metoda anketní analýzy a metoda matic.[11] [20]

4.2.5 RiskPAC

Tato metodika usnadňuje vytváření přehledu rizik, který dále slouží k provedení analýzy. Za pomoci metodiky je navržen autorizační dotazníkový přístup. Ten zahrnuje techniky pro zpracovávání odpovědí z dotazníků. Dále nám poskytuje výstupní podklady pro snadnější vytvoření závěrů. [7]

4.2.6 RiskWatch

Obsahuje dvě základní části - *management rizik*, která je shodná s požadavky normy (ISO-17799, ISO-27001). Druhá část obsahuje *software* pro hodnocení rizik, fyzické bezpečnosti a ochrany kritických částí infrastruktury. Tato metodika využívá k výpočtům simulačních metod Monte Carlo.[19]

4.2.7 Další metodiky

Níže je pro úplnost uvedeno srovnání dalších používaných metodik pro analýzu rizik, které jsou ovšem používány pro odhalování rizik v jiných oblastech než je bezpečnost informací.

Tabulka 5 Srovnání dalších metodik sloužících k analýze rizik ve vztahu k vybraným oblastem [1]

	SR	CL	RR	PHA	W-I	W-I/CL	HAZOP	FMEA	FTA	ETA	CCA	HRA
výzkum a vývoj	□	□	■	■	■	□	□	□	□	□	□	□
koncepční návrh	□	■	■	■	■	■	□	□	□	□	□	□
poloprovoz	□	■	□	■	■	■	■	■	■	■	■	■
detailní inženýring	□	■	□	■	■	■	■	■	■	■	■	■
konstrukce / najíždění	■	■	□	□	■	■	□	□	□	□	□	■
běžný provoz	■	■	■	■	■	■	■	■	■	■	■	■
rozšíření / modifikace	■	■	■	■	■	■	■	■	■	■	■	■
vyšetřování událostí	□	□	□	□	■	□	■	■	■	■	■	■
vyřazení z provozu	■	■	□	□	■	■	□	□	□	□	□	□

Pozn.: □ metoda používaná výjimečně, nebo nevhodná metoda

■ metoda běžně používaná

II. PRAKTICKÁ ČÁST

5 VYBRANÉ SOFTWAREOVÉ NÁSTROJE PRO AR

Softwarových nástrojů i metod analýzy rizik je celá řada, nicméně vzhledem k frekvenci využívání ve světě jsou v práci přiblíženy především softwarové nástroje RANIT a CRAMM 5.1, které jsou rovněž pro analýzu rizik v oblasti hardwaru a softwaru z nejvhodnějších. Mimo jiné oba umožňují provádět analýzu rizik dle zásad norem řady ISO 27000.

Metodika i soubor SW nástrojů CRAMM jsou v současné době používány více než 300 organizacemi v 27 zemích světa. Česká verze tohoto SW nástroje se na tomto čísle podílí 10 procenty.

Ranit je převážně vytvořen pro podporu, provádění a následné zavádění analýzy rizik v oblasti bezpečnosti informací. Vychází z metodiky Ranit.

Kromě programu RANIT existuje spousta dalších neméně vhodných softwarových aplikací zaměřujících se na provádění analýzy rizik, např. RISK, RiskPac, Riskan, CRAMM, RiskWatch… Veskrze všechny umožňují provádění dle zásad norem ISO 27000, obsahují číselníky i katalogy nápravných opatření. Velmi často tyto programy umožňují provádění AR dle stejných zásad, pouze s jemnými ekvivalenty v číselnících či hodnotících škálách.

Pro ukázku práce s analytickým softwarem jsem volil software RANIT zejména kvůli jeho jednoduchému používání a snadné dostupnosti demoverze umožňující provedení jednoduché analýzy včetně zahrnutí vlivu nápravných opatření na celý systém.

5.1 RANIT

Tento software založený na stejnojmenné metodice byl vytvořen jako podpora pro provádění analýzy rizik v oblasti BI, slouží jako pomocník pro ukládání údajů, získaných pohovory s vlastníky aktiv a komponent, a jejich vyhodnocování, správu dat i pro větší množství projektů. Součástí programu je katalog hrozeb a protiopatření i sada číselníků, které je možno importovat do nového/stávajícího projektu.[16]

RANIT implementuje metodiku vyhodnocování rizik dle norem ČSN ISO/IEC 13335 a ČSN ISO/IEC 27005 kombinovanou metodou.

Tento software tedy umožňuje:

- analyzovat rizika IS,
- analyzovat rizika s decentralizovanou správou,
- popsat a udržovat vazby mezi jednotlivými komponentami i aktivy systému,
- stanovení hodnoty aktiv jak relativně, tak i finančně
- opakovat analýzy,
- přistupovat k hodnocení řízení BI systémově a systematicky.

Software má tři základní verze, lišící se rozsahem funkcí. Kromě toho ho lze samozřejmě také zakázkově upravit „na míru“.

Tabulka 6 Srovnání základních verzí produktu RANIT [23]

	RANIT CLASSIC	RANIT EXPERT	RANIT MALÉ ORGANIZACE
Správa více projektů, editace	✓	✓	×
Přednastavené vzorce pro výpočet míry rizika	✓	×	✓
Přednastavené číselníky	✓	✓	✓
Automat. volba hrozba pro aktiva na základě vazeb	×	✓	×
Práce s číselníky	✓	✓	×
Přiřazení aktiva a komponent vlastníkům	✓	✓	×
Práce více uživatelů	✓	✓	×
Export/import číselníků, komponent, hrozeb,...	✓	✓	×
Změna jazyka prostředí	✓	✓	×
Přidávání dalších uživatelů	✓	✓	×
Síťová verze	✓	✓	×
Zobrazovaní sloupce s mírou rizika, podoba.	✓	✓	×
Vyhodnocení rizika ve formátu RTF	✓	✓	✓
Dle aktiva	✓	✓	✓
Dle aktiva (rizika)	✓	✓	✓
Dle rizika	✓	✓	✓
Dle komponentů (TOP 10)	✓	✓	✓
Dle komponentů (TOP 30)	✓	✓	✓
Dle aktiva (TOP 10)	✓	✓	✓
Dle aktiva (TOP 30)	✓	✓	✓
Dle hrozby (TOP 10)	✓	✓	✓
Dle hrozby (TOP 30)	✓	✓	✓
Vyhodnocení přehledu rizik	✓	✓	×
Export dat do CSV / XLS dle zvoleného kritéria	✓	✓	×

5.2 CRAMM 5.1

Tento systém umožňuje zpracovat analýzu rizik za pomoci seznamu zranitelností a hrozeb. Původní systém byl vytvořen pro vládu VB za pomocí normy BS7799. Analýza rizik je řízena podle norem GLBA, HIPAA, BS7799, ISO17799, ISO 27001 a dále zpracovává protiopatření, implementaci i audit. [1][17]

Většina lidí si pod pojmem CRAMM představí metodiku používanou k řízení rizik. Ovšem CRAMM je také jeden z nejužívanějších softwarových nástrojů, který zjednodušuje shromažďování informací o zkoumaném systému, dokáže provádět výpočet hodnot aktiv, rizik, navrhovat protiopatření atd. Výstupem z procesu hodnocení rizik jsou zpracované reporty.

Za podpory softwarového nástroje je mnohem snazší připravit danou organizaci na certifikaci podle normy ISO/IEC 27001:2005, usnadňuje nález efektivnějších opatření s cílem zlepšení informační bezpečnosti, provádí ohodnocení rizik v IS, analyzuje současný stav k ISO/IEC 27001:2005, vytváří bezpečnostní dokumentaci havarijního plánu, řídí informační rizika a zajišťuje kontinuitu v provozu.

Umožňuje provádění analýzy třemi způsoby, což umožňuje přizpůsobení stylu práce, délky analýzy, objemu vstupů i výstupů…

Tabulka 7 Výhody a nevýhody programového nástroje CRAMM 5.1 [23]

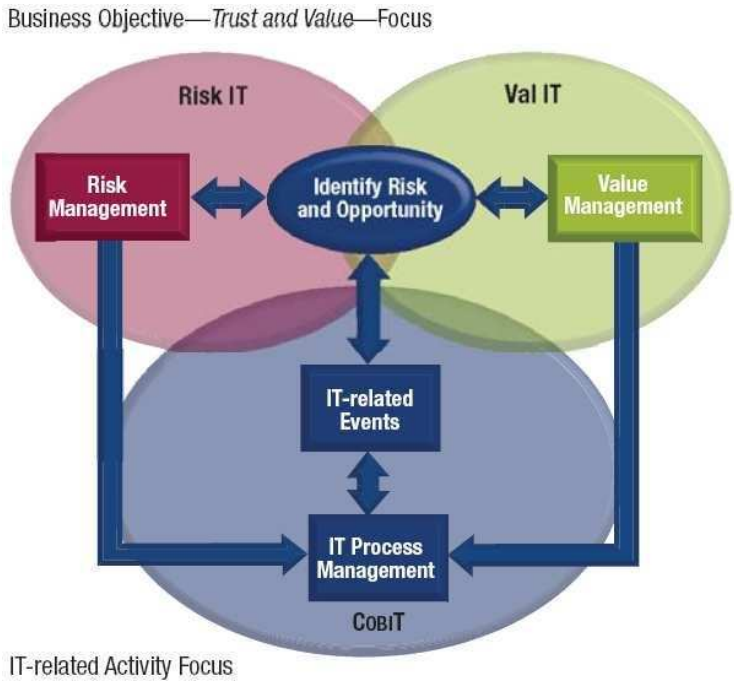
Výhody	Nevýhody
+ umožňuje zavádění a podporu ISMS	- starší design
+ doporučená protiopatření (knihovna rizik)	- nelze měnit design
+má v sobě implementována důležitá vodítka pro stanovení dopadů	- nelze pracovat na více počítačích najednou
+ šablony bezpečnostní dokumentace využitelné při tvorbě ISMS	- vysoká cena za pořízení SW nástroje a proškolení analytika
+ možnost výběru detailní nebo rychlé analýzy rizik	

Analytický nástroj CRAMM lze aplikovat dvěma přístupy:

- CRAMM Expert – slouží k provedení detailní (ale zdlouhavé) analýzy rizik IS a návrhu protiopatření,
- CRAMM Express – rychlejší alternativa, analýzu je možno provést v řádu několika hodin.

5.3 Risk IT based on COBIT

Softwarový nástroj Risk IT je jedním z rodiny produktů (viz. *Obrázek 9*) organizace ISACA, jejíž produkty se navzájem doplňují a jako celek poskytují oporu managementu firmy pro kompletní správu a poradenství v oblasti IT. [8]



Obrázek 9 Rodina produktů organizace ISACA a jejich provázanost [8]

Mimo informační bezpečnost se Risk IT zaměřuje i na související rizika, jako je zpoždění dodání projektu, nedosahování dostatečné hodnoty z IT, neflexibilní či zastaralé IT architektury, zpoždění dodávek IT služeb, apod.

Risk IT umožňuje managementu klást klíčové otázky tak, aby byl více informován o rizicích a mohl tak efektivněji rozhodovat a řídit rizika. Pomáhá ušetřit čas, náklady i nástroje pro řízení rizik. Integruje řízení IT a souvisejících rizik do celkového řízení podnikatelských rizik.

Risk IT shromažďuje všechny aspekty rizik, včetně hodnot, změn, dostupnosti, bezpečnosti, projektu a nápravy. Umožňuje provádění analýzy rizik s odkazem na celopodnikové přístupy, např. COSO ERM, ARMS, ISO 31000…

Risk IT může být přizpůsoben pro potřeby malých obchodů i pro nadnárodní konglomerace. Z jeho využívání můžou těžit tyto zájmové skupiny:

- výkonný management a představenstvo,

- firemní i externí risk manažeři,
- IT management, IT manažeři služeb a IT bezpečnostní manažeři,
- auditoři, apod.

5.4 RiskPAC software

RiskPAC je software navržený pro provádění hodnocení rizik a obchodních projektů efektivním a důsledným způsobem. Jedná se o analytický nástroj, kterým lze odhalit jak kvalitativní tak i kvantitativní rizika.

Jedná se o software postavené relační databázové technologii, umožňující pružné, snadné a efektivní používání. Obsahuje šablony dotazníků, pomocí kterých lze posoudit zabezpečení počítačových systémů, zařízení, fyzického a logického zabezpečení, síťové bezpečnosti a telekomunikace. Mimo to lze samozřejmě navrhnout vlastní dotazník pro zvolené téma. Součástí softwaru je také katalog doporučení nápravných opatření, která jsou poskytována na základě úrovně rizika. Lze exportovat a tisknout standardní retorty a grafy – dotazníky, výsledky průzkumu, doporučení, rizik / dopad na úroveň a obchodní analýzu dopadů.

6 ANALÝZA PODNIKATELSKÉHO PROSTŘEDÍ

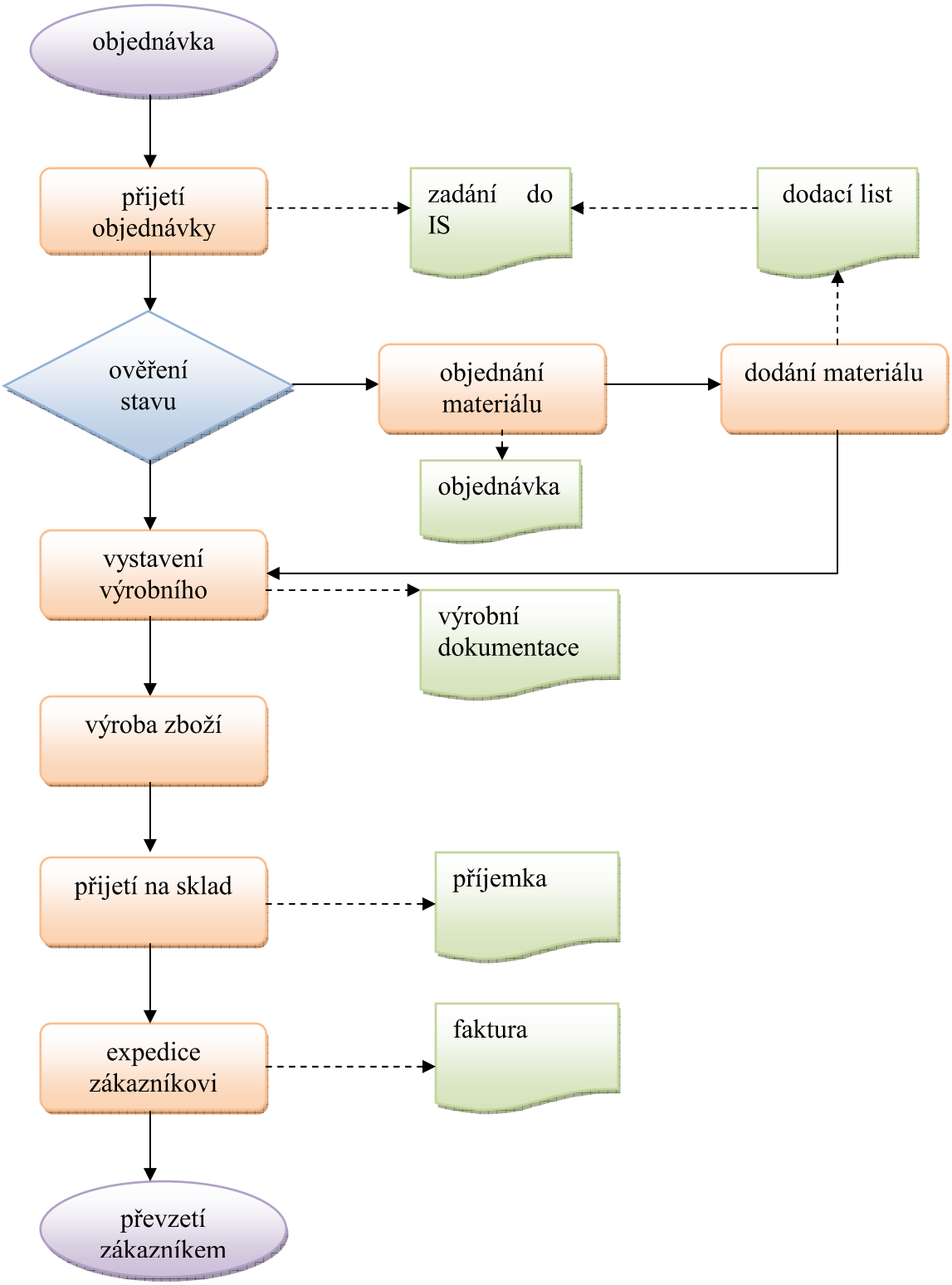
Tato kapitolka je věnována stručnému popisu firmy, kde je prováděna analýza rizik. Jsou zde obsaženy základní informace o firmě. Způsob zapojení podnikové sítě, hardwarová konfigurace.

6.1 Popis činnosti firmy

Společnost XY se zabývá výrobou originálního kovového zahradního nábytku dle vlastních návrhů již řadu let. Kromě vzorkových prodejen sloužících k prezentaci a prodeji zboží, prezentuje společnost své výrobky i na webových stránkách, které zároveň obsahují i sekci e-shop. Společnost komunikuje se svými zahraničními i českými partnery především pomocí e-mailové a telefonické komunikace.

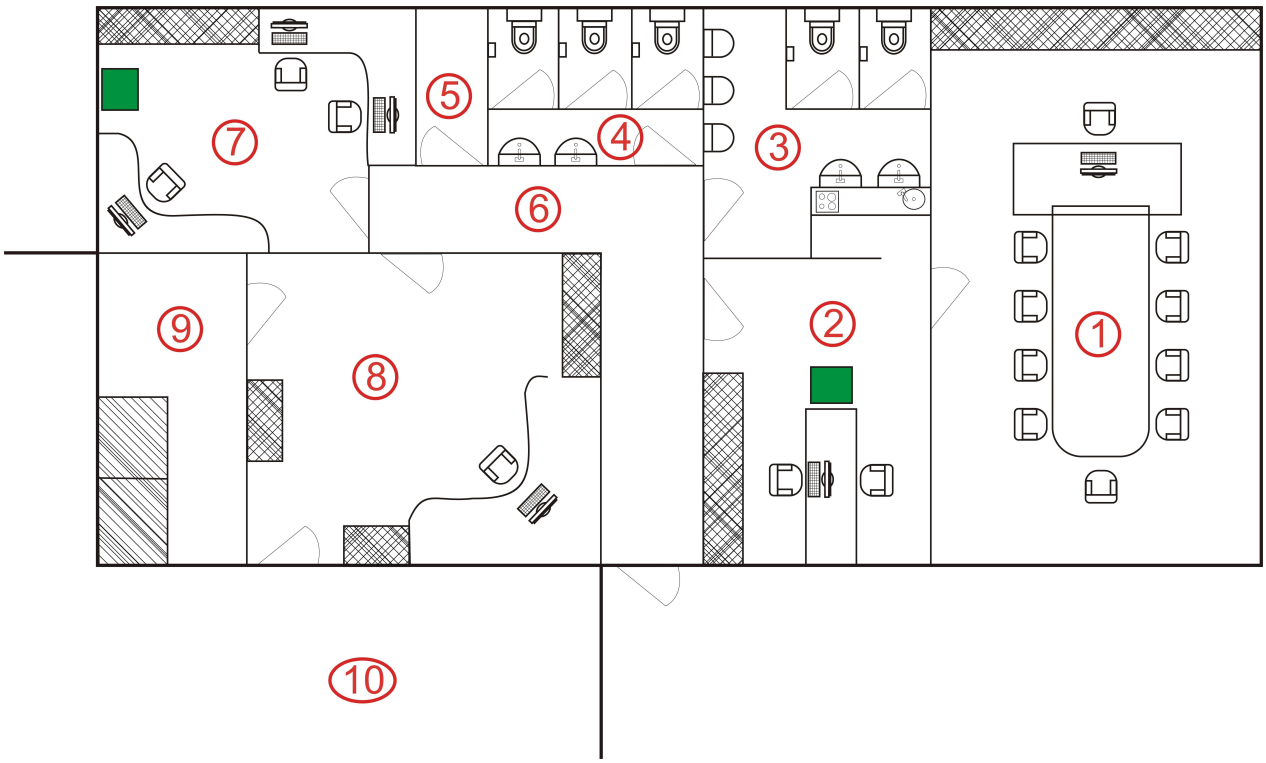
6.2 Výrobní a administrativní proces

Vše začíná přijetím objednávky od zákazníka a jejím zpracováním. Jelikož se jedná o zakázkovou výrobu je objednávka zadána do IS a poté co je prověřeno, zda je dostatek výrobního materiálu, je vystaven výrobní příkaz a ten je postoupen mistrovi. Mistr zadává příkazy do výroby dle termínů dodání. Pokud materiál není k dispozici, tak je objednán u externího dodavatele. Poté co je zakázka vyrobena, je odvedena na sklad a vyexpedována zákazníkovi. Celý výrobní i administrativní proces samozřejmě doprovází potřebná dokumentace od technických výkresů až po technologické postupy.



Obrázek 10 Schéma procesu zpracování zakázky (vlastní)

6.3 Dislokace pracoviště



Obrázek 11 Rozložení jednotlivých místností ve firmě [23].

Legenda:

1. Zde se nachází kancelář ředitele a zároveň tvořitele průmyslových vzorů. Je v samostatné místnosti sloužící rovněž jako zasedací místnost, kde probíhají firemní porady.
2. V této místnosti se nachází asistentka ředitele a síťová tiskárna, kterou mohou využívat všichni zaměstnanci organizace. Nachází se zde síťové multimediální zařízení.
3. Sociální zařízení pro muže.
4. Sociální zařízení pro ženy.
5. Úklidová místnost.
6. Vstupní chodba organizace.
7. Kancelář, kterou obývají 2 pracovníci obchodního oddělení a účetní/personalistka. Kvůli častému využívaní tisku se zde nachází síťová tiskárna.

8. Kancelář vedoucího výroby, těsně sousedí s výrobními prostory, z této místnosti je přístup do hlavní serverovny.
9. Serverovna, zde se nachází mozek celé počítačové sítě a samozřejmě datový server, který slouží k záloze dat.
10. Výrobní prostory.

7 ANALÝZA RIZIK

Vzhledem k tomu, že komplexní analýza rizik ve společnosti by překročila rámec diplomové práce, byla v rámci pilotního projektu řešení bezpečnostní politiky zvolena problematika bezpečnosti interních dat, hardwarových a softwarových prostředků užívaných ve firmě.

7.1 Identifikace aktiv společnosti a kategorizace hrozeb

Obecně lze specifikovat aktiva společnosti do následujících tříd:

1. Technické prostředky
    - počítače a jejich komponenty – např. osobní počítače, servery, rozhraní, přídavná zařízení…
    - periferní zařízení – např. tiskárny, scannery, čtečky čárových kódů…
    - provozní materiál – např. papír do tiskáren, cartrige, flash disky,…
    - dokumentace k technickému vybavení
    - síťové komunikační prostředky – např. kabeláže, rozbočovače, modemy, síťové karty…
    - další podpůrná a doplňková zařízení – např. záložní zdroje napětí, klimatizace, …
2. Programové prostředky
    - operační systémy a jejich přídavná zařízení,
    - systémové řídící a provozní programy,
    - vývojové prostředky – např. programovací jazyky, knihovny programovacích jazyků, testovací a vývojová prostředí,
    - databáze a jejich součásti,
    - aplikační programy – tabulkové a textové editory, správce e-mailové pošty,…
    - speciální programy zhotovené dle požadavků společnosti.

3. Organizační prostředky
    - pracovní postupy a obslužné a manipulační návody,
    - pokyny pro provoz informačního systému,
    - směrnice dělby a koordinace práce,
    - směrnice přiřazující zodpovědnost za správnost vkládaných dat,
    - vymezení oprávněnosti přístupu k datům a manipulaci s daty,
    - pravidla archivace dat a pořizovaní bezpečnostních kopií,
    - provádění antivirové ochrany, zabezpečení dat před zneužitím,
    - sledování a vyhodnocování informačního systému a evidence nákladů na něj,
    - provádění údržby a inovací informačního systému,
    - zajišťování bezpečnosti informačního systému,…

Aktiva identifikována **ve společnosti** byla rozčleněna do následujících skupin:

- hardware,
- software,
- data,
- komunikační zařízení – sítě, telefony, modemy…
- dokumenty, smlouvy, zápisy…
- know – how,
- image a firemní kultura organizace,…

Kromě toho by bylo možné zařadit mezi aktiva i ostatní hmotný a nehmotný majetek společnosti, např. výrobky, materiál, budovy… **V rámci pilotního projektu analýzy rizik je však řešena pouze oblast hardware, software a dat.**

Pro každé z aktiv existuje určitá míra ohrožení s určitou pravděpodobností výskytu. Hrozby lze rozčlenit do následujících oblastí:

- falšování uživatelské identity, neoprávněné používání aplikací, virové napadení, apod…, tzv. *logické infiltrace,*

- *komunikační infiltrace* – odposlechy komunikace, její narušení či selhání, …
- *selhání zařízení* – výpadky serverů, poruchy napájení, …
- chyby zaměstnanců, uživatelů, operátorů apod., tzv. *chyby způsobené lidským faktorem,*
- *fyzické hrozby,* tzn. živelné pohromy, krádeže, úmyslné poškození, atd.

7.1.1 Hardwarové prostředky

Hlavním stavebním kamenem celé firemní infrastruktury je *hlavní server* a *datový server* (konfigurace viz. *Tabulka 8*). Celá firma je propojena v rámci podnikové sítě. Připojení k internetu je zprostředkováno pomocí Wi-fi routeru a UTP kabelů. Router je připojen ke switchi (konfigurace viz. *Tabulka 9*).

Konfigurace jednotlivých pracovních stanic je opět uvedena v tabulce *Tabulka 10*. Ve firmě se nalézají síťová tiskárna a multifunkční zařízení. Telefonní spojení s okolním světem zajišťují VoIP telefony, které mají THP pracovníci k dispozici.

Tabulka 8 Konfigurace serveru[23].

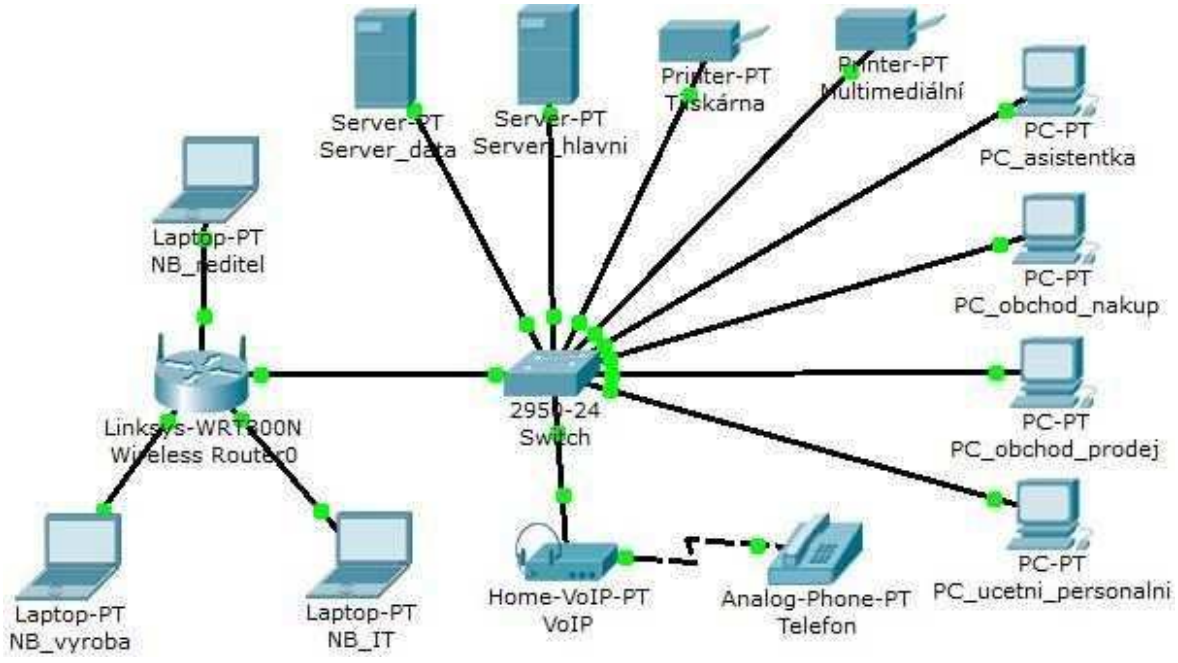
Server	
Operační systém	Windows Server 2003
Procesor	Intel Xeon X3220
Frekvence	2,4 GHz
Operační paměť	4 GB DDR2 ECC
Čipová sada	Intel 3200 + ICH9R
Pevný disk	2x 500 GB SATA

Tabulka 9 Konfigurace switche [23].

Switch	
Konektory	48x RJ-45 + 4x Mini GBIC
Rychlost	10/100/1000 Mbit/s
Standardy	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE802.1p, IEEE 802.1q, IEEE 802.1d

Tabulka 10 Standarizované HW vybavení počítačových jednotek[23].

PC / NB	ředitel	asistentka	nákup	prodej	účet. / person.	výroba	IT
Operační systém	Windows 7 Professional	Windows XP Professional	Windows 7 Home	Windows 7 Home	Windows 7 Home	Windows 7 Professional	Windows 7 Professional
Procesor	Intel Core i7	Intel Pen III Xeon	AMD Athlon X2 4200+	Intel Core 2 Duo E7500	AMD Athlon X2 3200+	Intel Core i5-460M	Intel Core2 Duo T5870
Frekvence	2300 MHz	2621 MHz	2200 MHz	2930 MHz	1800 MHz	2530 GHz	2001 MHz
Architektura	x64	x86	x64	x64	x64	x64	x64
Operační paměť	16GB,DDR 3,SODIMM	4GB, DDR2, DIMM	2GB,DDR2, DIMM	4GB,DDR2, DIMM	1GB,DDR2, DIMM	4GB,DDR3, SODIMM	4GB,DDR2, SODIMM
Pevný disk	1500 GB	320 GB	250 GB	500 GB	120GB	750 GB	500 GB
Síť	Wireless LAN (WiFi)	Síťová karta 10 / 100 / 1000	Síťová karta 10 / 100 / 1000	Síťová karta 10 / 100 / 1000	Síťová karta 10 / 100 / 1000	Wireless LAN (WiFi)	Wireless LAN (WiFi)
	Bluetooth					Bluetooth	Bluetooth
	Síťová karta 10/100/1000					Síťová karta 10/100/1000	Síťová karta 10/100/1000



Obrázek 12 Rozložení počítačové sítě ve firmě [23].

7.1.2 Softwarové aplikace

Podnik využívá u osobních počítačů OS Windows různých verzí, počítačové stanice nepoužívají heslovaný přístup. Každý, kdo má přístup k danému zařízení, má přístup i k datům na nich obsažených, servery jsou spravovány OS Windows Server 2003. Tabulka níže obsahuje přehled nejčastěji používaných programů a jejich práv použití licencí. U každého programu je uvedena aktuální nainstalovaná verze, výrobce, a k čemu daný SW slouží. Tyto informace byly získány provedením SW auditu společnosti s využití programu *Free PC Audit*. Přehled nejčastěji používaných softwarových aplikací a nástrojů je uveden v tabulce níže.

Tabulka 11 *Seznam nejčastěji využívaných aplikací firmy[23].*

software	verze	výrobce	popis
POHODA	2011	Stormware s.r.o	Ekonomický a informační systém
Adobe Photoshop CS4	11.0	Adobe Systems Incorporated	Kreslící program
Adobe Reader X - Czech	10.0.1	Adobe Systems Incorporated	Prohlížeč souborů ve formátu .PDF
AutoCAD 2010	2010	Autodesk	Kreslící a projektovací program
CCleaner	3.2	Piriform	Nástroj na pročištění registrů
CorelDRAW Graphics Suite 11	11	Corel Corporation	Kreslící program
Google Chrome	10.0.648.204	Google Inc.	Internetový prohlížeč
Internet Explorer 8	20090308.140743	Microsoft Corporation	Internetový prohlížeč
LogMeIn	2.0.2.85		Program pro zprostředkování vzdáleného přístupu
Microsoft Office systém 2007	12.0.6425.1000	Microsoft Corporation	Sada kancelářského softwaru
Microsoft Security Essentials	2.0.657.0	Microsoft Corporation	Antivirový program
Mozilla Firefox	3.6.2016	Mozilla	Internetový prohlížeč
Nero Burning ROM 10	10.2.11000.12.100	Nero AG	Vypalování CD a DVD
Opera 11.01	11.01.1190	Opera Software ASA	Internetový prohlížeč
QIP 2010	10.9.6.4103		Komunikační „chatovací“ program
Skype™ 5.0	5.0.156	Skype Technologies S.A.	Komunikační VoIP a „chatovací“ program
Total Commander	7.50a	Ghisler Software GmbH	Program pro efektivní srpávu souborů

7.1.3 Datová aktiva

Všechna důležitá data jsou uložena v datovém serveru. Ať už se jedná o stávající projekty, na kterých se pracuje, pro snadnější editaci více lidmi najednou, nebo ukončené zálohované projekty. Jednotliví uživatelé mají ke složkám s dokumenty přidělena přístupová práva.

Datová aktiva byla identifikována za pomocí rozhovorů s personálem společnosti:

- **Technologická a výrobní dokumentace**

  Jedná se o podklady pro výrobu produktů společnosti. Zahrnují následující dokumenty:

  - technologické předpisy a normy,
  - balící předpisy,
  - výrobní příkazy,
  - výkres produktu,
  - pracovní postupy,
  - soupis materiálu potřebného pro výrobu,
  - záznamy o plnění zakázek,
  - výkazy práce,
  - standardy bezpečnosti práce,
  - kontrolní plány, …

  Tyto dokumenty se dostanou do rukou výrobním dělníkům pouze v papírové podobě. V elektronické podobě jsou spravovány zejména vedoucím výroby. Jedná se veskrze o dokumenty vytvořené za pomocí programů MS Office a AutoCAD.

- **Návrhy nových výrobků a průmyslové vzory**

  Návrhy nových výrobků provádí ředitel společnosti v programu AutoCAD. Databázi stávajících i rozpracovaných vzorů spravuje ředitel. Originální návrhy jsou registrovány jako průmyslové vzory na patentovém úřadě. Jedná se o citlivá data.

- **Databáze dodavatelů a odběratelů**

Jedná o evidenci kontaktních údajů jak o zákaznících společnosti, tak i o jejích dodavatelích. Tato data jsou důležitá zejména ve vztahu k dodavatelům materiálu a smluvním cenám. Přístup k nim má pouze obchodní úsek a ředitelství.

- **Osobní data zaměstnanců**

  Tato data podléhají zákonu na ochranu osobních údajů (v České republice regulován zákonem č. 101/2001 Sb., o ochraně osobních údajů a o změně některých zákonů). Jsou velmi citlivá a přístup k nim by měla mít pouze účetní/personalistka, eventuálně ředitel společnosti.

- **Strategie a vize firmy**

  V elektronické podobě je spravuje ředitelství (asistentka). Jedná se o dokumentaci, ve které jsou stanoveny dlouhodobé i krátkodobé cíle firmy, obchodní a marketingová strategie, kterou se firma hodlá ubírat a vize o tom kam společnosti směřuje. S těmito informacemi by měli být seznámeni všichni

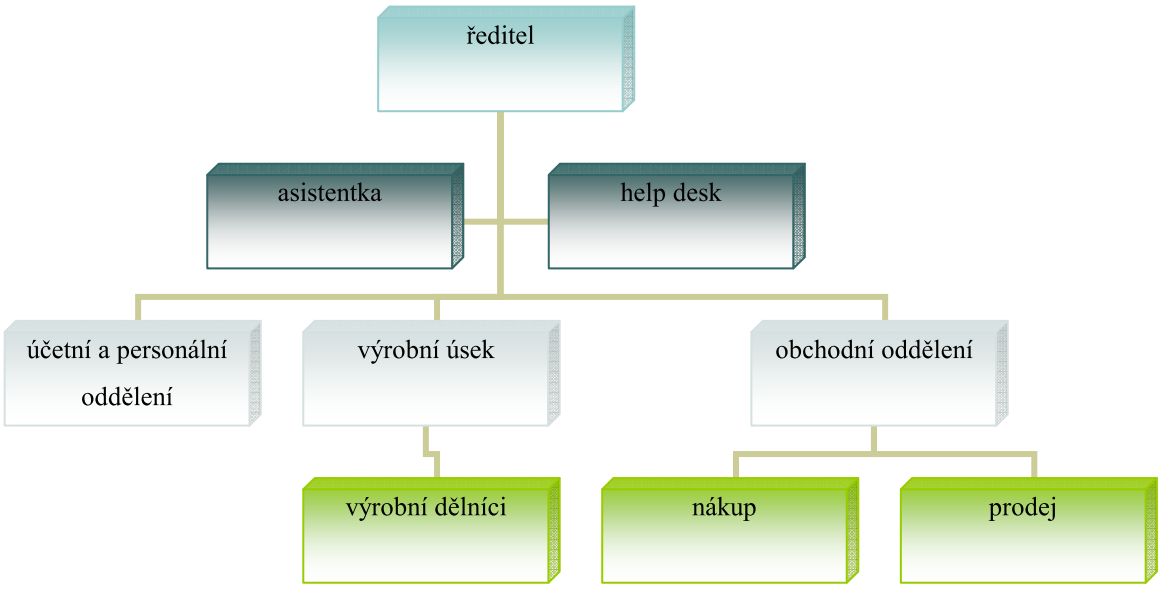
- **Účetnictví**

  Pravidla účetní evidence jsou dána zákonem. Ve společnosti XY je spravováno účetní/personalistkou jak v elektronické podobě v programu Pohoda, tak i v papírové podobě. Přístup k účetnímu programu má účetní/personalistka, zaměstnanci obchodního oddělení i asistentka ředitele.

7.2 Uživatelé informačního systém a osoby s přístupovými právy k datům

Společnost má 15 zaměstnanců pracujících ve výrobě, kteří dostávají výrobní podklady v papírové podobě, oběh této dokumentace není blíže řízen. A 7 THP pracovníků včetně ředitele, který rovněž vytváří průmyslové vzory.

7.2.1 Organizační struktura firmy



Obrázek 13 Organizační struktura firmy[23].

Nad chodem společnosti dohlíží majitel ve funkci ředitele, má k ruce asistentku. O chod výroby a realizaci zakázek se stará vedoucí výrobního úseku. Sjednávání nových zakázek, reprezentaci společnosti, nákupní, prodejní a logistické toky obstarává obchodní oddělení, které je rozčleněno na nákupní a prodejní sekci. HelpDesk poskytuje externí pracovník, který v případě problému je schopen většinu problémů řešit operativně na dálku. Účetní a personální oddělení se stará o příjem nových zaměstnanců a samozřejmě obstarává účetnictví celé firmy.

7.2.2 Přístupová práva pracovníků

Ne ke všem souborům a citlivým datům mají přístup všichni pracovníci společnosti. Pro přehlednost byly vytvořeny tabulky s přehledem přístupů jednotlivých skupin pracovníků k hardwarovým jednotkám (*Tabulka* 12), softwarům využívaným nejčastěji ve firmě (*Tabulka* 13) a datovým aktivům firmy (*Tabulka 14*).

Jako identifikátor přístupu k těmto jednotkám je v tabulce uveden symbol ✓ , naopak pokud pracovníci přístup nemají, byl volen symbol ×.

Tabulka 12 *Přístup pracovníků k hardwarovým jednotkám[23].*

Oddělení		Hlavní setrver	Datový server	Tiskárna	Multifunkční zařízení	Router	Switch	NB ředitel	NB výrobní úsek	NB IT	PC sekretariát	PC nákup	PC prodej	PC účetní/personální
ředitelství	ředitel	✓	✓	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓
	asistentka	×	×	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓
obchodní	nákup	×	×	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
	prodej	×	×	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
výrobní	vedoucí	×	×	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
	výrobní pracovníci	×	×	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
účetní/personální		×	×	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
help desk		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Tabulka 13 *Přístup pracovníků k softwaru[23].*

Oddělení		ABRA G2	Adobe Photoshop CS4	Adobe Reader X - Czech	AutoCAD 2010	CCleaner	CorelDRAW Graphics Suite 11	Google Chrome	Internet Explorer 8	LogMeIn	Microsoft Office systém 2007	Microsoft Security Essentials	Mozilla Firefox	Nero Burning ROM 10	Opera 11.01	QIP 2010	Skype™ 5.0	Total Commander
ředitelství	ředitel	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	asistent.	✓	×	✓	×	✓	×	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓
obchodní	nákup	✓	×	✓	×	✓	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
	prodej	✓	×	✓	×	✓	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
výrobní	vedoucí	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓
	výr. prac.	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
účetní/personální		✓	×	✓	×	✓	×	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓
help desk		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Tabulka 14 Přístupová práva k datům[23].

Oddělení		technologické předpisy a normy - elektronicky	technologické předpisy a normy - papírově	balící předpisy	výrobní příkazy	výkres produktu	pracovní postupy	soupis materiálu potřebného pro výrobu	záznamy o plnění zakázek	výkazy práce	standardy bezpečnosti práce	kontrolní plány
ředitelství	ředitel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	asistentka	×	✓	×	×	×	×	×	×	×	✓	×
obchodní	nákup	✓	✓	×	×	×	×	✓	×	×	✓	×
	prodej	✓	✓	✓	×	×	×	×	×	×	✓	×
výrobní	vedoucí	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	výr. prac.	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
účetní/personální		×	✓	×	×	×	×	✓	×	✓	✓	×
help desk		✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓

7.3 Ohodnocení aktiv

Na základě rozhovorů se zaměstnanci společnosti byly stanoveny dopady teoreticky nejhorších scénářů, které by mohly nastat. Z důvodů omezené časové kapacity byl pro reprezentativní vyhotovení analýzy rizik zvolen následující:

nedostupnost dat vlivem selhání serveru.

Pokud to bylo možné, tak byla stávající protiopatření ignorována, aby bylo zamezeno pochybnostem a dohadům o jejich účinku.

7.3.1 Hodnotící stupnice používané při analýze v softwaru RANIT

Pro provedení analýzy rizik u pilotního projektu byly převzaty číselníky standardně uvedené v nástroji RANIT.

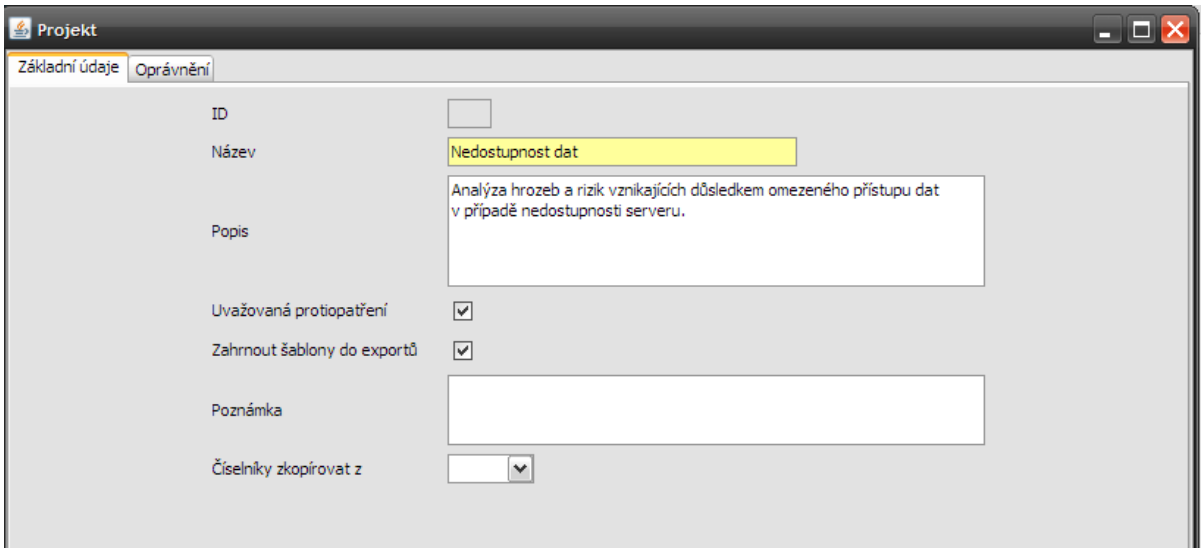
Tabulka 15 Ohodnocení rizik [16]

dosažená hodnota	riziko
0	akceptovatelné
5	nízké
20	střední
40	vysoké
60	kritické

Program standardně obsahuje také databázi aktiv, intervaly finančního ohodnocení aktiv i hrozeb. Pro jejich rozsah však jsou v této práci uvedeny pouze ve formě náhledů při zadávání případové studie do softwaru.

7.3.2 Zadávání případové studie do softwaru

Následující obrázky zobrazují postup zadávání údajů do programu RANIT. Nejprve je nutné založit projekt – v tomto případě zaměřený na nedostupnost dat vlivem omezeného přístupu k datovému serveru.

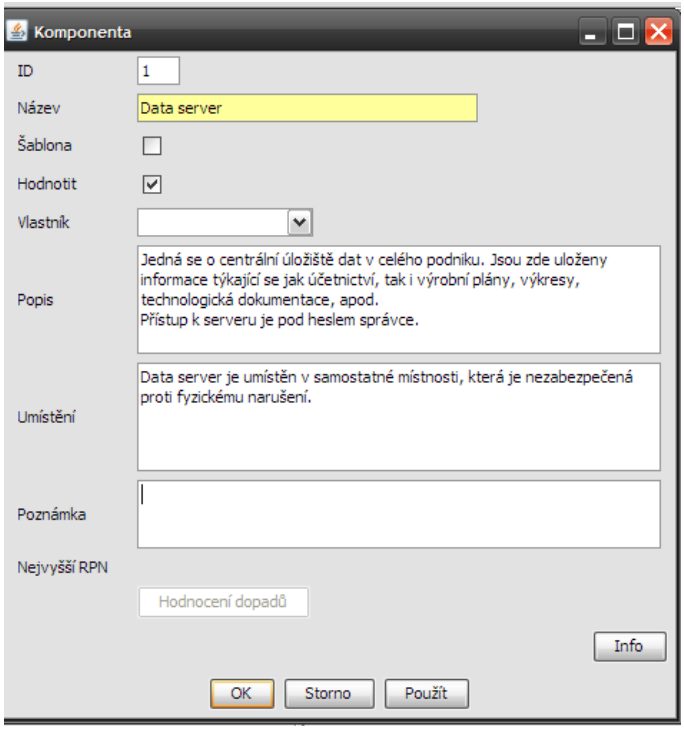


Obrázek 14 Založení projektu v SW RANIT [23].

Pro analýzu rizik je nutné definovat jednotlivé komponenty analyzovaného systému, zadává se název komponenty, její co nejpřesnější popis a umístění.

Ukázkový příklad byl směřován na analýzu nedostupnosti dat, proto byl jako jedna z komponent také nadefinován server, jakožto úložiště dat celého podniku. Na server mohou ukládat data všichni zaměstnanci dle přidělených přístupových práv. Ke všem datům a správě serveru má však přístup pouze správce sítě. Tento přístup je heslován.

Samotný server je umístěn v samostatné místnosti, která však není žádným způsobem zabezpečená.

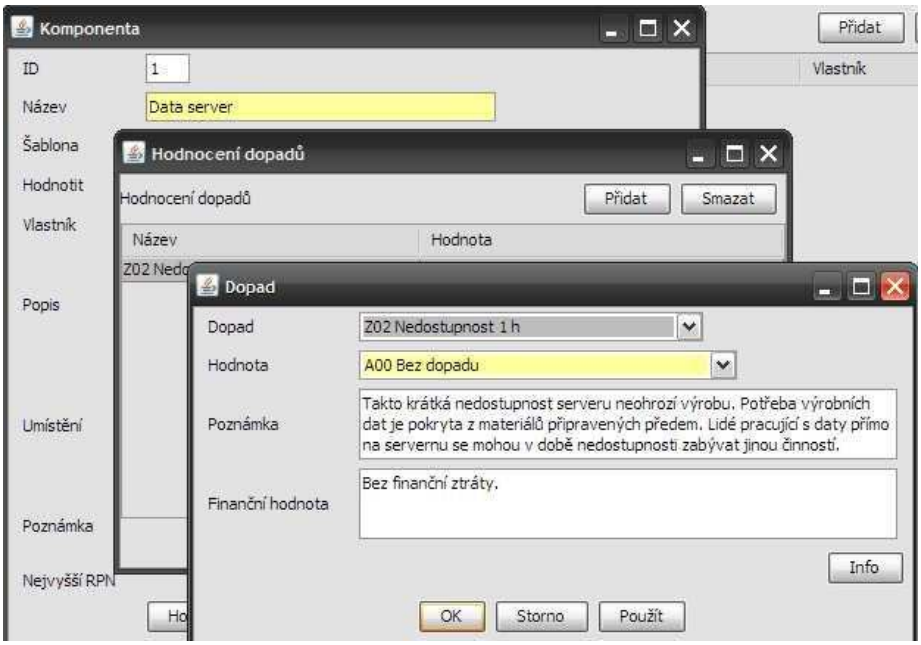


Obrázek 15 Přidání komponenty systému [23].

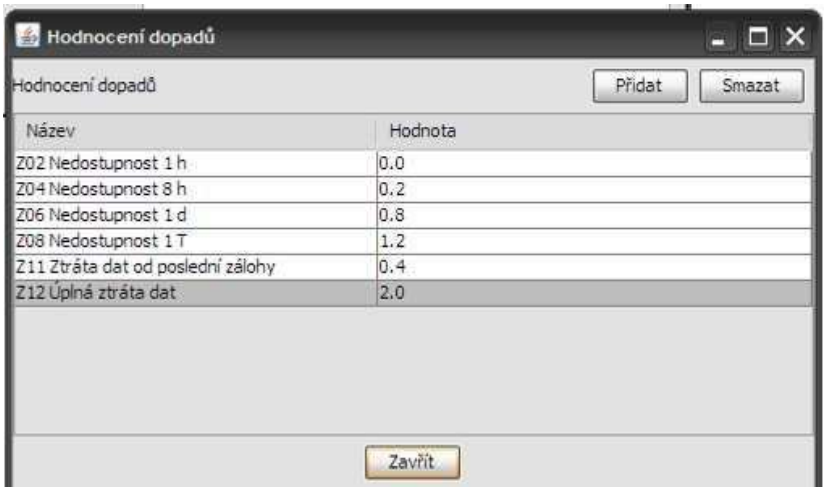
Tabulka 16 Specifikace scénářů [23].

nedostupnost	hodnota	finanční hodnota	poznámka
1 h	bez dopadu	bez finanční ztráty	Takto krátká nedostupnost serveru neohrozí výrobu. Potřeba výrobních dat je pokryta z materiálů připravených předem. Lidé pracující s daty přímo na serveru se mohou v době nedostupnosti zabývat jinou činností.
4 h	zanedbatelná do 10 tis. Kč	mzdové náklady na administrativní pracovníky 400 Kč / hod. / os.	Vzhledem k tomu, že výrobní dokumentace je připravována s předstihem ve formě výrobních příkazů, výrobu by takovýto výpadek ovlivnit neměl. Ale pozdržel by práci administrativních pracovníků.
1 den	nízká 100 – 300 tis. Kč	průměrné os. náklady na THP, náklady na vícepráce mistra a dělníků ve výrobě – 500 Kč / hodina	Takovýto výpadek serveru nejen, že znemožní práci administrativním pracovníkům, ale i výrazně ohrozí chod výroby, nicméně zkušený mistr je schopen výrobu uřídit i bez potřebných výrobních podkladů.
1 týden	střední 300 – 1 000 tis. Kč	mzdové náklady všech pracovníků, sankce za zpoždění dodávek…	Nedostupnost dat delší než 1 týden může zapříčinit zpoždění dodávek, omezená možnost fakturace či provádění plateb.
ztráta dat od poslední zálohy	střední 300 – 1 000 tis. Kč	náklady na administrativní práci za poslední cca měsíc	Záloha dat je prováděna jednou za asi měsíc prostřednictvím externí administrátora, který data zálohuje na externí úložiště.
úplná ztráta dat	vysoká 1 000 – 3 000 tis. Kč	náklady na nový server, náklady na ztracená data	Úplné selhání úložiště dat. Ztráta může být až nevyčíslitelná.

Pro každou komponentu jsou hodnoceny různé scénáře v případě její nedostupnosti. Je určen dopad včetně jeho finančního vyjádření. Pro datový server byly tyto scénáře a dopady určeny následovně – viz tabulka výše.

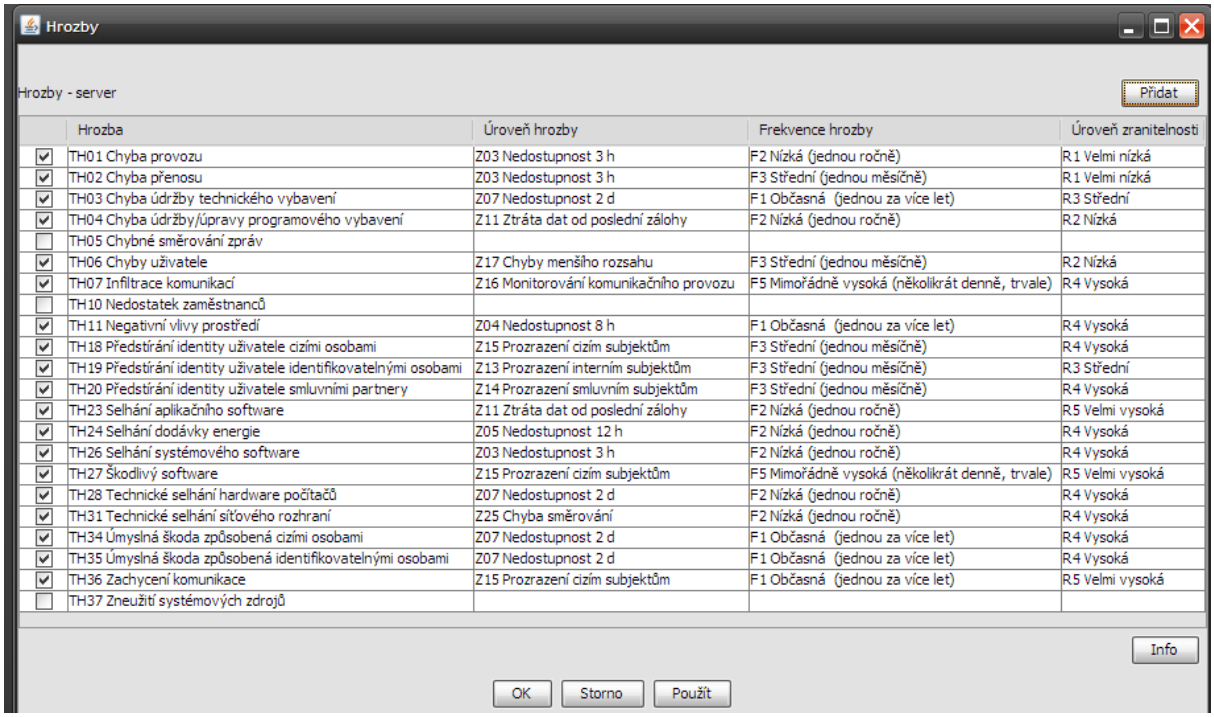


Obrázek 16 Hodnocení dopadů v různých alternativách v případě nedostupnosti komponenty [23].



Obrázek 17 Hodnocení dopadů [23].

Po zadání scénáře program vždy na základě zadaných dat přiřadí ohodnocení jeho dopadu (viz. *Obrázek 17*). Jakmile jsou ohodnoceny dopady nedostupnosti komponenty, je nutné se blíže zaměřit na jednotlivé hrozby, definovat její úroveň, frekvenci a vliv na zranitelnost komponenty. (*Obrázek 18*)



	Hrozba	Úroveň hrozby	Frekvence hrozby	Úroveň zranitelnosti
☑	TH01 Chyba provozu	Z03 Nedostupnost 3 h	F2 Nízká (jednou ročně)	R1 Velmi nízká
☑	TH02 Chyba přenosu	Z03 Nedostupnost 3 h	F3 Střední (jednou měsíčně)	R1 Velmi nízká
☑	TH03 Chyba údržby technického vybavení	Z07 Nedostupnost 2 d	F1 Občasná (jednou za více let)	R3 Střední
☑	TH04 Chyba údržby/úpravy programového vybavení	Z11 Ztráta dat od poslední zálohy	F2 Nízká (jednou ročně)	R2 Nízká
☐	TH05 Chybné směrování zpráv			
☑	TH06 Chyby uživatele	Z17 Chyby menšího rozsahu	F3 Střední (jednou měsíčně)	R2 Nízká
☑	TH07 Infiltrace komunikací	Z16 Monitorování komunikačního provozu	F5 Mimořádně vysoká (několikrát denně, trvale)	R4 Vysoká
☐	TH10 Nedostatek zaměstnanců			
☑	TH11 Negativní vlivy prostředí	Z04 Nedostupnost 8 h	F1 Občasná (jednou za více let)	R4 Vysoká
☑	TH18 Předstírání identity uživatele cizími osobami	Z15 Prozrazení cizím subjektům	F3 Střední (jednou měsíčně)	R4 Vysoká
☑	TH19 Předstírání identity uživatele identifikovatelnými osobami	Z13 Prozrazení interním subjektům	F3 Střední (jednou měsíčně)	R3 Střední
☑	TH20 Předstírání identity uživatele smluvními partnery	Z14 Prozrazení smluvním subjektům	F3 Střední (jednou měsíčně)	R4 Vysoká
☑	TH23 Selhání aplikačního software	Z11 Ztráta dat od poslední zálohy	F2 Nízká (jednou ročně)	R5 Velmi vysoká
☑	TH24 Selhání dodávky energie	Z05 Nedostupnost 12 h	F2 Nízká (jednou ročně)	R4 Vysoká
☑	TH26 Selhání systémového software	Z03 Nedostupnost 3 h	F2 Nízká (jednou ročně)	R4 Vysoká
☑	TH27 Škodlivý software	Z15 Prozrazení cizím subjektům	F5 Mimořádně vysoká (několikrát denně, trvale)	R5 Velmi vysoká
☑	TH28 Technické selhání hardware počítačů	Z07 Nedostupnost 2 d	F2 Nízká (jednou ročně)	R4 Vysoká
☑	TH31 Technické selhání síťového rozhraní	Z25 Chyba směrování	F2 Nízká (jednou ročně)	R4 Vysoká
☑	TH34 Úmyslná škoda způsobená cizími osobami	Z07 Nedostupnost 2 d	F1 Občasná (jednou za více let)	R4 Vysoká
☑	TH35 Úmyslná škoda způsobená identifikovatelnými osobami	Z07 Nedostupnost 2 d	F1 Občasná (jednou za více let)	R4 Vysoká
☑	TH36 Zachycení komunikace	Z15 Prozrazení cizím subjektům	F1 Občasná (jednou za více let)	R5 Velmi vysoká
☐	TH37 Zneužití systémových zdrojů			

Obrázek 18 Přiřazení hrozeb komponentě [23].

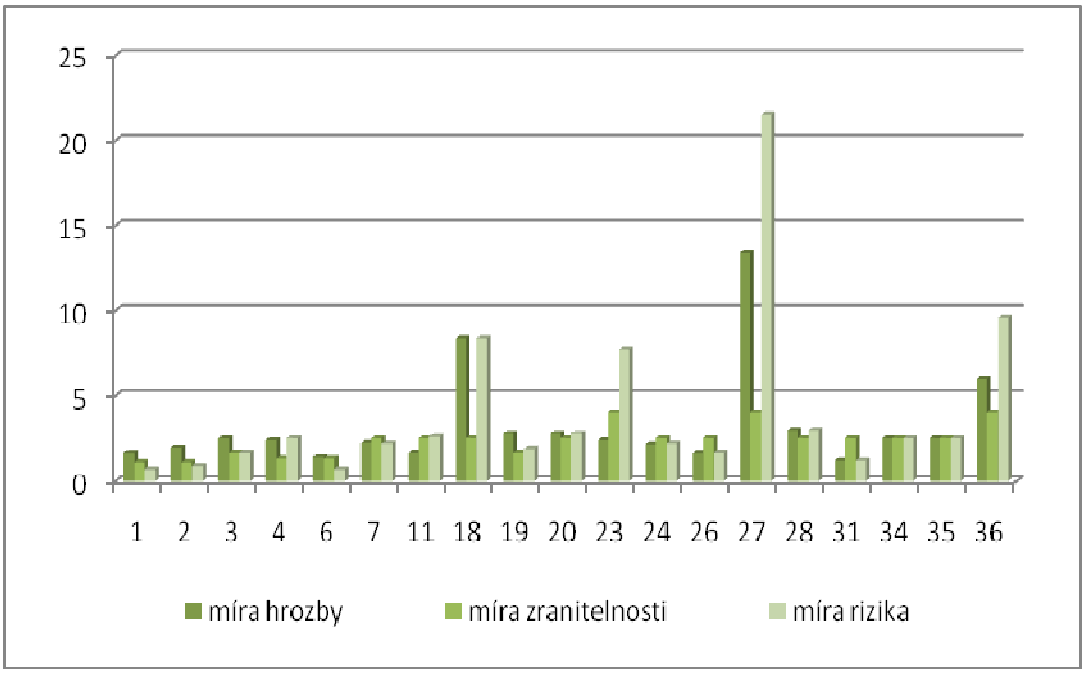
8 ANALÝZA V SW RANIT - VÝSTUPY

8.1 Stávající rizika – datový server

Po zadání všech hrozeb souvisejících se zvoleným aktivem je softwarem provedeno vyhodnocení míry hrozby, míry zranitelnosti a míry rizika. Pro objektivní stanovení nejkritičtějších rizik byly tyto koeficienty vynásobeny. Hrozby s nejvyššími dosaženými hodnotami pak byly vybrány pro další zpracování v softwaru a za pomocí katalogu nápravných opatření, bylo riziko sníženo.

Tabulka 17 Vyhodnocení hrozeb [23].

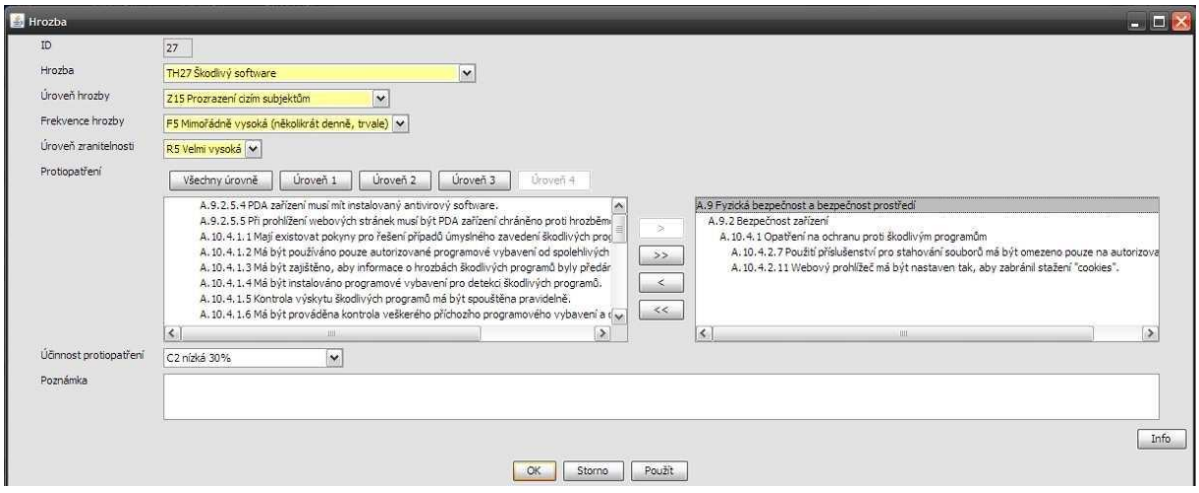
Data server		stávající stav			
číslo hrozby	pojmenování hrozby	míra hrozby	míra zranitelnosti	míra rizika	součinitel hodnot
1	Chyba provozu	1,68	1,1	0,7	1,29
2	Chyba přenostu	1,96	1,1	0,9	1,94
3	Chyba údržby technického vybavení	2,5	1,7	1,7	7,23
4	Chyba údržby/úpravy programového vybavení	2,4	1,3	2,5	7,80
6	Chyby uživatele	1,4	1,3	0,7	1,27
7	Infiltrace komunikací	2,24	2,5	2,2	12,32
11	Negativní vlivy prostředí	1,7	2,5	2,6	11,05
18	Předstírání identity uživatele cizími osobami	8,4	2,5	8,4	176,40
19	Předstírání identity uživatele ident. Osobami	2,8	1,7	1,9	9,04
20	Předstírání identity smluvními partnery	2,8	2,5	2,8	19,60
23	Selhání aplikačního software	2,4	4	7,7	73,92
24	Selhání dodávky energie	2,16	2,5	2,2	11,88
26	Selhání systémového software	1,68	2,5	1,7	7,14
27	Škodlivý software	13,44	4	21,5	1 155,84
28	Technické selhání hardware počítačů	3	2,5	3	22,50
31	Technické selhání síťového rozhraní	1,2	2,5	1,2	3,60
34	Úmyslná škoda způsobená cizími osobami	2,5	2,5	2,5	15,63
35	Úmyslná škoda způsobená ident. osobami	2,5	2,5	2,5	15,63
36	Zachycení komunikace	6	4	9,6	230,40



Obrázek 19 Srovnání míry hrozeb, míry zranitelnosti a míry rizika [23].

8.2 Protiopatření navržená pomocí katalogu nápravných opatření pro pilotní projekt

Hrozbám s největšími součiniteli, jsem se pokusil s pomocí softwaru přiřadit nápravná opatření a snížit jejich dopad.



Obrázek 20 Srovnání míry hrozeb, míry zranitelnosti a míry rizika [23]

Protiopatření zvolená pro hrozbu 27 škodlivý software s účinnosti protiopatření 20%:

- bezpečnost zařízení,
- opatření na ochranu proti škodlivým programům,

- použití příslušenství pro stahování souborů má být omezeno pouze na autorizovaný personál,
- webový prohlížeč má být nastaven tak, aby zabránil stažení „cookies“.

S účinností 50 % byla pro hrozbu 36 zachycení komunikace určena tyto protiopatření:

- fyzická bezpečnost a bezpečnost prostředí,
- bezpečnost zařízení,
- správa bezpečnosti sítě,
- řízení přístupu,
- všechny modemy musí být autorizovány.

Pro hrozbu 18 předstírání identity uživatele cizími osobami byla s účinností 80 % stanovena tato protiopatření:

- bezpečnost zařízení,
- monitorování,
- požadavky na řízení přístupu,
- odpovědnosti uživatelů,
- řízení přístupu k síti,
- řízení přístupu k operačnímu systému,
- mobilní výpočetní zařízení a práce na dálku.

Poslední hrozbou zvolenou pro stanovení protiopatření je 23 selhání aplikačního software, s účinností 80 % byla v softwaru vybrána tato protiopatření:

- veškeré příchozí programové vybavení musí být zkontrolováno, aby bylo zajištěno, že v něm během přepravy nebyly provedeny žádné neautorizované změny,
- programové vybavení má být zasíláno důvěryhodným distribučním mechanismem,
- u dodavatele má být ověřena správnost informací popisujících dodávané programové vybavení,
- integrita programového vybavení má být chráněna kontrolními součty,

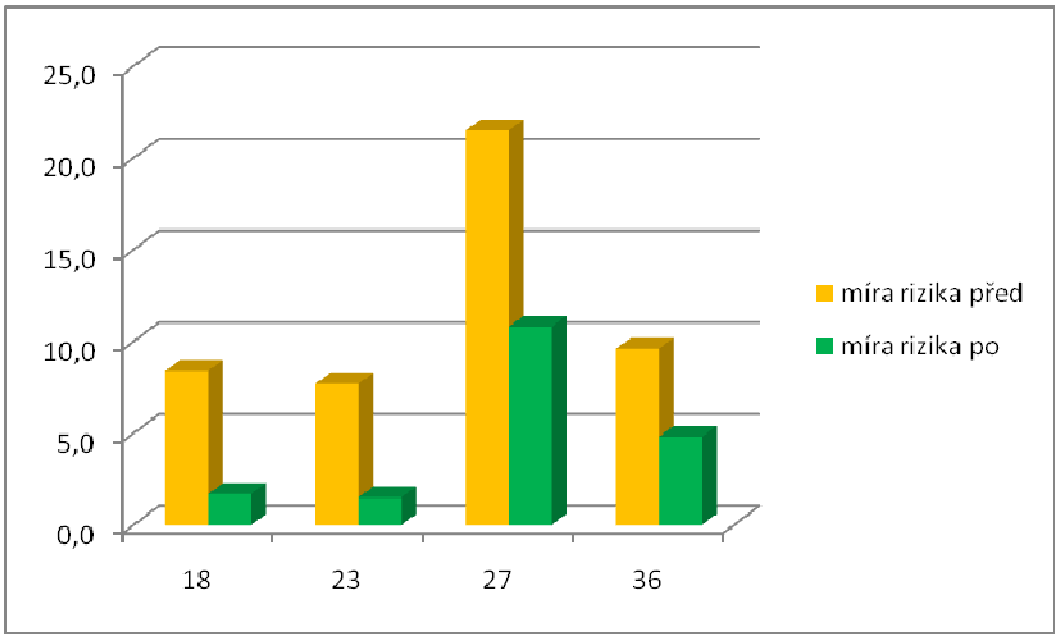
- balení programového vybavení má být takové, aby bylo možné odhalit jeho případné otevření,
- příjemci mají být zaslány informace o programovém vybavení v samostatné obálce,
- pro programové vybavení mají být provedeny kontrolní součty,
- vývoj aplikací musí být veden tak, aby byly minimalizovány chyby programového vybavení,
- použití řádných vývojových metod má zajistit, že bude dostupná úplná specifikace zdokumentovaných a splněných požadavků uživatele,
- pro minimalizování výskytu chyb má být provedena analýza rizik navržených aplikací,
- má být zabezpečeno, aby výsledky analýzy rizik vymezily bezpečnostní požadavky aplikace,
- má být zajištěno dodržování standardů analýzy / návrhu,
- má být zajištěna namátková kontrola vývoje,
- má být zajištěno dodržování standardů programování,
- má být zajištěno dodržování standardů testování,
- má být zajištěno dodržování standardů implementace,
- změny v operačním systému musí být autorizovány,
- změny v operačním systému mají procházet přes procedury řízení změn programového vybavení,
- pro autorizaci změn v operačním systému se má udržovat kontrola nad nástroji pro realizaci aktualizace programového vybavení,
- bezpečnostní dopad změny v operačním systému musí být analyzován.

Po zadání těchto protiopatření byla znovu vygenerována míra rizika. Tabulka níže uvádí srovnání její výše před a po zavedení těchto protiopatření.

Tabulka 18 Srovnání míry rizika před a po realizaci protiopatření [23].

Data server								
číslo hrozby	míra hrozby před	míra hrozby po	míra zranitelnosti před	míra zranitelnosti po	míra rizika před	míra rizika po	součinitel hodnot před	součinitel hodnot po
18	8,4	8,4	2,5	2,5	8,4	1,7	176,4	35,7
23	2,4	2,4	4,0	4,0	7,7	1,5	73,9	14,4
27	13,4	13,4	4,0	4,0	21,5	10,8	1 155,8	580,6
36	6,0	6,0	4,0	4,0	9,6	4,8	230,4	115,2

Jak je z tabulky patrné, došlo pouze ke změně míry rizika. Míra ohrožení a zranitelnosti zůstává stejná, protože míra ohrožení i zranitelnosti systému zůstává pořád stejná. Pouze správně zvolenými protiopatřeními lze snížit míru rizika, které daná hrozba systému způsobuje.



Obrázek 21 Srovnání míry rizika u vybraných hrozeb před a po zavedení protiopatření [23].

9 NÁVRHY BEZPEČNOSTNÍCH PROTIOPATŘENÍ

Nejprve bych v krátkosti shrnul běžné bezpečnostní problémy číhající ve firemním prostředí. Častým problémem je podceňování bezpečnostních rizik a hlavně to, že neexistuje bezpečnostní politika, což je i náš případ.

Dalším velkým problémem je podcenění zabezpečení přístupu k serveru, pracovním stanicím a v neposlední řadě i síťovým prvkům jak aktivním tak i pasivním, špatná konfigurace firewallů a neaktualizovaný software. Ve výčtu problémů můžeme dále pokračovat např., nejednotný přístup k ochraně pracovních stanic, kdy se používají nevhodné formáty e-mailů a nehlídaný pohyb informací prostřednictvím e- mailů. Ve firmě se také často nachází nebezpečné notebooky s konektivitou na VPN, nebezpečné je také připojení těchto notebooků a pracovních stanic k jiným než firemním serverům.

Kromě softwarového, technického a komunikačního zabezpečení, kterému se budu věnovat dále v textu. Je potřeba provést také fyzické zabezpečení:

- elektronický zabezpečovací systém – komplexní zabezpečení budovy s pomocí pohybových čidel, jako prevence vloupání,
- identifikace přístupu pomocí čipových karet do prostor s omezeným přístupem,
- fyzicky zabezpečit všechny počítačové stanice zámkem, když už nic tak to alespoň narušitele zpomalí.

9.1 Zabezpečení sítě

Základní úrovní pro zabezpečení podnikové sítě je překlad adres. Což znamená skrytí jednotlivých částí vnitřní sítě do tzv. neviditelné skupiny za veřejnou IP adresu. Důležité upozornění ale je, že takové zabezpečení nebrání přístupu do vnitřní sítě, pouze ji skrývá. Nejjednodušším nástrojem bezpečnosti je **paketová a stavová paketová filtrace**. Nejvyšší úroveň zabezpečení představují aplikační brány.

Jaké nebezpečí na nás číhá z Wi-Fi sítě? Tyto sítě často pokrývají větší prostor, než potřebujeme. Útoky na takovou síť mohou přijít z velké vzdálenosti. Po připojení do takové sítě může útočník získat nejen připojení do podnikové sítě, ale také přístup ke všem interním zařízením připojených do této sítě. Tyto sítě jsou snadněji infiltrované zvenčí než metalické sítě.

K podnikové síti by mělo být přistupováno, jako by se jednalo o síť veřejně přístupnou. Nepředpokládejte, že provoz sítě bude bezpečný a soukromý. Problém se zabezpečením podnikové bezdrátové sítě je velice obsáhlý, nicméně je potřeba držet se základních doporučení uvedených níže.

Aplikovat šifrovaní WEP, změnit implicitní identifikátor SSID, přepnout Wi-Fi router do neviditelného režimu, změnit implicitní heslo nastavené na přijímači, popřemýšlet nad umístění m přístupového bodu co nejvíce do středu organizace tak, aby signál nezasahoval vně budovy, a v neposlední řadě je třeba zajistit, aby správce sítě prováděl preventivní prohlídky sítě, např. nástrojem NetStumbler, zvážit omezení připojení k přístupovému bodů dle MAC adres a také vypojení DHCP a přiřazení statických IP adres.

Další možné zabezpečí je na zvážení organizace. Možností je zabezpečení pomocí certifikátů, kde v zásadě existují 3 možnosti. *Autentizace* – před povolením přenášet data v bezdrátové síti, musí být klient ověřen pomocí platných přihlašovacích údajů. *Šifrování* – před odesláním dat musí proběhnout jejich zašifrování, aby bylo zaručeno utajení dat proti možným monitorováním sítě. *Integrita dat* – do paketu musí odesílatel vložit informace, které umožní příjemci provést kontrolu, zda paket nebyl po cestě modifikován.

9.2 Zabezpečení serveru

Na serveru bych doporučil aplikovat kombinovaný Firewall a FTP / WWW server dané firmy. Server je vystaven trvalému nebezpečí 7 dní v týdnu, 24 hodin denně. Jako operační systém byl doporučen Linux, který je pro tyto účely vhodnější než Windows, kde je potřeba po instalaci zkontrolovat jeho nastavení, vypnout nepoužívané služby a především správně nastavit firewall a provést další důležité úkony. Server spravovaný pod takovýmto operačním systémem je mnohem bezpečnější před napadením viry a tím pádem je zde i menší riziko poškození a ztráty dat.

I nejlépe nastavený firewall však systém neochrání před viry, tím spíše pokud společnost používá MS Windows. I za předpokladu, že je na serveru nainstalován OS Linux, který viry pro Windows neohrozí, na koncových stanicích je ve většině případů nainstalován právě OS Windows, a ten již může být virem ohrožen. Proto je nutné udržovat na počítačích aktualizované antivirové programy.

Lepším a vhodnějším řešením by bylo v instalaci antivirového programu přímo na nový Linuxový server. Ovšem k tomuto je nutné, aby linuxový server byl zároveň i emailovým serverem. Na trhu je obrovské množství bezplatných i komerčních řešení pro linuxový emailový antivirový podsystém. Levným ale v neposlední řadě účinným nástrojem je nasazení filtračních mechanizmů, které nám zajišťují odstranění potencionálně nebezpečných částí emailů. Většina virů tímto ztratí možnost se dále šířit. Mezi uživateli rozšířeným programem může být např. Email Security through Procmail.

Na serveru máme dvě diskové jednotky, doporučil bych je zapojit jako RAID 1 – jedna z nejjednodušší, ale poměrně efektivních ochran dat. Provádí zrcadlení obsahu disku. Celý obsah disku se současně zaznamenává na dva disky. V případě výpadku či poruchy jednoho z disků se pracuje s kopií, která je hned k dispozici. Z důvodu lepšího zabezpečení dat na nich obsažených při selhání disku.

9.3 Zabezpečení pracovních stanic

Samozřejmou součásti zabezpečení počítačových stanic je nastavení hesla pro přístup do BIOSu a hesla pro přihlášení do Windows, nastavení by měl měnit pouze správce. Také by měla být stanovena doba, po které by si měli jednotliví uživatelé změnit své přístupové heslo, které by mělo být maximálně bezpečné. Jak vypadá takové správně zabezpečené heslo je uvedeno v příloze P I. Měly by být zpřístupněny jen ty služby, které jsou nezbytné k chodu.

Nápravným krokem, který dokáže napomoci se zabezpečení jednotlivých stanic je také instalace Firewall, personální firewall, antivir softwaru na všechny stanice připojené k internetu. Samozřejmostí je tyto programy udržovat aktualizované, u antiviru navíc čas od času zkontrolovat databázi známých virů. Pokud necháme stanici jen měsíc neaktualizovanou, počítač je tím nechráněn a je jedno, že antivirus na počítači je, když není aktualizovaná databáze hrozeb.

Jedním z dalších doporučení je také zavést jednotný a stále aktualizovaný internetový prohlížeč. Možností máme mnoho. Pro organizaci bude nejvhodnější použít Internet Explorer 9 a udržovat jej aktualizovaný. Ovšem na Internet Explorer působí také nejvíce hrozeb, protože je nejvíce rozšířený. Proto stojí za zmínění i alternativní prohlížeče jako Mozilla Firefox či stále více oblíbený Google Chrome, který podle testů vykazuje větší

rychlost. Ať už se jedná o dobu, za jak dlouho se prohlížeč otevře, nebo dobu načítání internetových stránek.

Zabezpečení všech počítačových stanic je velice důležitým krokem pro zabezpečení nerušené práce a ochrany dat. Omezit uživatele v přístupu na vybrané webové stránky, např. s erotickou tématikou, nelegálním obsahem… Všude tady nás může potkat škodlivý SW, který se nejčastěji nachází v podobě kódů ukrytých na stránkách, které nemusíme ani postřehnout. Proto by si zaměstnanci měli dávat velký pozor, na jakých stránkách se nacházejí.

Je velice nepravděpodobné, že by byl vinut dokonalý software, který by nás dokázal uchránit přede všemi nástrahami. Boj široké škály výrobců programů s viry je nekonečná cesta. Uživatelům a firmám nezbývá nic jiného než stále sledovat nové verze programů a pro ochranu je instalovat a neustále aktualizovat.

9.4 Zálohování dat

Nynější zálohování dat cca jednou za měsíc je nevyhovující. A to, že tuto práci provádí externí pracovníci, je zarážející. Záloha by měla být prováděna každých 24 hodin, ať už se jedná o účetnictví, projektové návrhy, soupis skladů atd. Typů záloh je celá škála, ale nejvhodnější bude použít zálohu Úplná + rozdílová. Po realizaci úplné zálohy každá částečná záloha zachytí všechny soubory vytvořené nebo změněné od poslední úplné zálohy, i když některé jsou již obsaženy v předešlé částečné záloze.

Také není od věci zavést šifrovací program pro šifrování důležitých dat. Příkladem může být *TrueCrypt* (dostupná z http://www.truecrypt.org/) , jedná se o volně šiřitelný SW pro šifrování dat. Dokáže šifrovat celé diskové oddíly i systémové soubory a složky. Využívá šifer AES, Serpent, TwoFish. Nevyžaduje instalaci a můžeme jej přenášet jen na USB klíči. Proti šifrování AES není v současně době znám útok na prolomení. Šifra je považována za bezpečnou. Používá se varianta s délkou klíče 256 bitů.

9.5 Školení uživatelů

Většina bezpečnostních odporníků se shodne na tom, že uživatelé pracovních stanic představují nejslabší článek bezpečnosti informací dané organizace. Hlavním důvodem je to, že zaměstnanci nejsou ochotní číst interní směrnice, a důsledkem toho nedodržují

striktně daná nařízení. Jak ale zařídit aby zaměstnanci znali bezpečnostní protiopatření a chovali se podle nich? Jediným východiskem je neustálá informovanost bezpečnostních pravidel a návyků pro práci do podvědomí uživatelů.

Řešením našeho problému by mohlo být sestavení školení zaměstnanců, které bude sestaveno přímo na míru společnosti. Školení může být například rozčleněno do úrovní. Po základní bezpečnostní úrovni běžných uživatelů, tak může být realizována pokročilá úroveň pro manažery a bezpečnostní správce.

Školení by mělo být provedeno formou workshopu nebo prezentace. Posluchači budou mít možnost reagovat a přispívat k diskuzi na daná témata, což určitě přispívá lepšímu zapamatování problematiky a také je to pro posluchače zajímavější.

Součástí takového školení může být závěrečný test posluchačů. Zde mohou být zařazeny všechny aspekty související s přednášenou problematikou. Na uživatelích mohou být např. odzkoušeny praktiky sociálního inženýrství, které jistě vypoví o jejich podvědomí o bezpečnosti.

Přínosem takového školení by měly být jasně definované povinnosti zaměstnanců a zvýšení podvědomí posluchačů o informační bezpečnosti a sníží riziko vzniku incidentu vinou neznalosti problematiky.

Doporučená struktura školení:

- základní problematika informační bezpečnosti,
- definování hrozeb, které na nás číhají, sociální inženýrství, nebezpečí el. komunikace, hrozby z internetu, trojští koně, internetový červy, spyware, malware, pretexting, phishing, pharming, cross site scripting, DoS útoky, DDoS …
- definice pravidel, kterých se má řídit každý zaměstnanec,
- shrnutí,
- diskuse.

9.6 Shrnutí

Nespoléhejte na myšlenku, že vaší organizaci se přece nemůže stát, že by ji chtěl někdo poškodit. Řešte bezpečnost komplexním přístupem k bezpečnosti, včetně bezpečnosti fyzické. Vypracovanou bezpečností politiku udržujte stále aktualizovanou. Pravidelně ověřujte funkčnost bezpečnostních protiopatření. Například formou nečekaných auditů.

Udržujte aktuální verze operačních systémů a pravidelně aktualizujte antivirový software na poslední známé viry. Používejte pro vaši organizaci vhodný SW (firewall, personální firewall, antivir). Mějte povoleny a zpřístupněny jen ty služby, které jsou nezbytné pro vaše fungování.

10 PROJEKT CHARTER

10.1 Definice projektu

Projekt zavedení a implementace bezpečnostní politiky ve firmě XY.

10.2 Cíle projektu

Hlavním cílem diplomové práce je analyzovat softwarové nástroje pro analýzu rizik informační bezpečnosti a jejich využití v projektu. Neméně důležitou součástí DP je vytvoření návrhů protiopatření s cílem dosažení vyšší bezpečnosti firmy.

Za dílčí cíle pak lze považovat identifikaci problémů pracoviště a nalezení potenciálu pro zlepšení celého procesu, zejména pak:

- analyzovat podnikové prostředí,
- popsat činnost firmy, rozložení pracoviště,
- provedení pilotního projektu analýzy rizik ve společnosti,
- identifikace aktiv a kategorizace hrozeb (HW, SW prostředky),
- identifikace zabezpečení a přístupových práv pracovníků,
- ohodnocení aktiv společnosti.

Práce vznikla pouze jako návrh pro management podniku. Projekt proto může a nemusí být realizován v celém svém rozsahu. V práci také není zahrnuto časové hledisko případné realizace.

10.3 Harmonogram projektu

Tabulka 19 Harmonogram projektu [23].

měsíc		leden				únor				březen				duben				květen			
týden		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
činnost	Vypracování teoretické části práce																				
	Kontaktování výrobců softwarů																				
	Analýza softwarových nástrojů																				
	Analýza procesů na pracovišti																				
	Rohovory s respondenty																				
	Vytvoření návrhů projektového řešení																				
	Fimální úpravy diplomové práce																				
	Představení práce managementu																				
	Odevzdání diplomové práce																				
	Obhajoba práce																				

10.4 Omezení projektu

Omezení projektu je převážně spatřováno v:

- neochotě pracovníků přistupovat na nové věci,
- finanční omezení v případě realizace projektu,
- omezené časové možnosti pro zpracování diplomové práce.

10.5 Projektový tým

Projektový tým byl sestaven po dobu nutnou k analýze firmy a spolupráce s respondenty.

Členové týmu:

Mgr. Roman Jašek, Ph.D.	vedoucí diplomové práce
Ing. Vendula Ambrožová	externí konzultant
Bc. Tomáš Račák	student UTB
Josef Lukšík	mistr

11 SHRNUTÍ

Práce se zabývá problematikou analýzy rizik s ohledem na mezinárodní legislativní opatření. Teoretická část obsahuje stručný úvod do problematiky analýzy rizik a do přístupů k řízení rizik. Nedílnou součástí řízení riziky je stanovení bezpečnostní politiky a strategie, v rámci jejího zavádění je také nezbytné nastavit bezpečnostní standardy a snažit se o jejich neustálé zlepšování tak, aby byl celý systém řízení bezpečnosti informací neustále aktualizován.

Řízení informační bezpečnosti je legislativně upravováno a řízeno na mezinárodních i národních úrovních. Byla vytvořena řada mezinárodních norem (např. ISO/IEC 27 000, ISO/IEC TR 13 335, …), které jsou velmi často přebírány do legislativy evropských států a často doplňovány nejrůznějšími zákony, např. zákonem o utajení informací, o ochraně osobních údajů,…

Následující část práce se zaměřuje na metody provádění samotné analýzy rizik. V zásadě existují dva přístupy analýzy rizik – kvalitativní a kvantitativní. Kvalitativní přístup je rychlejší a jednodušší, analýza je de facto prováděna na základě rozhovorů a hodnocení zaměstnanců dané společnosti, které může být často subjektivní. Naproti tomu kvantitativní přístup je založen na matematickém výskytu rizika a četnosti jeho výskytu. Takovéto metodiky jsou přesnější, časové náročnější, ale i méně kvalitní. Oba dva přístupy pokrývá řada metodik, které se analýzou rizik zabývají, např. CRAMM, COBRA (kvalitativní), @Risk, RiskWatch (kvantitativní).

Nedílnou součástí této práce bylo vyhledání vhodných softwarových nástrojů pro provádění analýzy rizik. Protože jsem se dále v práci rozhodl nastínit postup právě kvalitativního přístupu, zaměřil jsem se ve vyhledávání softwarových prostředků spíše na programy umožňující provést komplexní analýzu od vytvoření vhodných dotazníků, po zakomponování návrhů protiopatření a analýzu jejich dopadů na míru rizika.

K bližšímu popisu jsem zvolil programové prostředky RANIT, CRAMM 5.1, RiskIT a RiskPac. Po bližším prozkoumání jsem došel k závěru, že většina těchto softwarových nástrojů pracuje na velmi podobných principech, ať už se týkají kvalitativního či kvantitativního provádění analýzy rizik.

Pro to, aby bylo možné provést pilotní studii analýzy rizik ve zvolené firmě, bylo nejdříve nutné důkladně poznat a popsat prostředí ve firmě a její jednotlivé procesy. Proto byl

v práci uveden stručný popis činnosti firmy i jejích administrativních a výrobních procesů. Kvůli následné analýze hardwaru a přístupu k němu, byla také vytvořena zjednodušená ilustrace dislokace pracoviště.

Základním stavebním kamenem každé analýzy rizik je identifikace aktiv společnosti, těch má každá společnost celou řadu. V této práci jsem se zaměřil především na hardwarové prostředky, softwarové aplikace a především datová aktiva. Dalším krokem pak bylo stanovení přístupů k těmto aktivům. Vzhledem k tomu, že se jedná spíše o malou firmu, tak je řada těchto aktiv přístupná téměř všem uživatelů systému, často bez jakéhokoliv fyzického zabezpečení.

Všechna identifikovaná aktiva by měla být také v rámci analýzy rizik řádně ohodnocena a stanovena rizika jejich nedostupnosti. V práci jsem pro tyto účely využil hodnoticí stupnice dostupné v softwaru RANIT, ve kterém také byla provedena ukázková analýza rizik – nástin zadávání do zvoleného nástroje je uveden pomocí print screenů aplikace, současně s nimi jsou i uvedeny komentáře a doplnění, tak jak byly vybrané informace do softwaru zadávány.

Na základě výstupu z analýzy provedené softwarem, pak byla doporučena nápravná a preventivní opatření tak, aby bylo dosaženo větší míry bezpečnosti společnosti. Tato doporučení byla navržena dvěma způsoby. Nejprve pomocí katalogu nápravných opatření, obsaženém přímo v softwaru, kdy bylo nutné rovněž zadat procento účinnosti zvoleného nápravného opatření.

Dále byla stanovena bezpečnostní protiopatření dle jednotlivých aktiv, tzn. serveru, pracovních stanic a dat. Tato doporučení již byla stanovena na základě „best practice“ dle zkušeností a znalostí autora.

V první řadě bylo navrženo dotáhnout zabezpečení serveru – bylo doporučeno opustit stávající operační systém Windows a přejít na Linux. Součástí protiopatření rovněž bylo doporučení vhodného nastavení zabezpečení serveru a zálohování datových aktiv ve dvou rovnocenných kopiích každých 24 hodin, místo občasného a nesystematického vytváření záloh.

Součástí navržených protiopatření týkajících se bezpečnosti sítě bylo také školení zaměstnanců zaměřené na škodlivý a nebezpečný obsah nejen webových aplikací a e-

mailů. S tím přímo souvisí i správná volba webového prohlížeče, protože právě nejvíce využívaný Internet Explorer nejvíce podléhá útokům z vnější sítě.

Poslední součástí této diplomové práce je nastínění project charteru, ve kterém je uvedena definice projektu, včetně jeho hlavních a vedlejších cílů, dále je zde vyobrazen předpokládaný průběh projektu v přehledném harmonogramu. Součástí každé definice projektu samozřejmě musí být rovněž stanovení projektového týmu a odhad reálných omezení, které by mohly bránit jeho realizaci.

V následující tabulce je uveden přehled cílů práce, tak jak byly stanoveny v project charteru a zhodnocení, zda jich bylo dosaženo, ev. zda jsou v této práci obsaženy.

Tabulka 20 Zhodnocení dosažení cílů práce [23]

Cíl	Splněno?	Kapitola
Analýza softwarových nástrojů vhodných pro AR	✓	5
Návrh protiopatření pro bezpečnostní politiku firmy	✓	8.2, 9
Analýza podnikového prostření	✓	6
Popis činnosti firmy	✓	6.1
Popis rozložení pracoviště	✓	6.3
Vytvoření pilotní studie analýzy rizik	✓	7
Identifikace aktiv a kategorizace hrozeb	✓	7.1
Identifikace zabezpečení a přístupových práv pracovníků	✓	7.2
Ohodnocení aktiv společnosti v rámci pilotní studie	✓	7.3

ZÁVĚR

Co tedy říci závěrem? Každá organizace se den co den setkává s nástrahami rizik a musí jim čelit. Před těmito riziky nemá smysl utíkat, je více než nutné, aby se organizace těmto problémů postavily a naučily se tyto rizika řídit a ne jim podléhat. K tomuto účelu je nutné tyto rizika co nejlépe popsat a dívat se na ně z pohledu dané organizace, každá má jiné priority.

K řízení těchto rizik je zapotřebí správně zvolit metodiku, která by byla vhodná pro danou organizaci. Jak tedy poznáme, že je daná metodika pro organizaci vhodná? Na tuto otázku bohužel nelze nalézt jednoduchou, jednoznačnou odpověď. Nutností je dívat se na tento problém s určitým nadhledem, komplexně, s jistou systematičností. A v neposlední řadě se na problém zaměřit z pohledu organizace.

Hlavní otázkou, kterou si musíme položit je, co vlastně, tedy jaké riziko chceme eliminovat a jak ho chceme řídit. V tomto případě jsme se zaměřili na eliminaci rizik spojenou se zabezpečením datových aktiv. Na základě provedené analýzy pak byla navržena a stanovena doporučení týkající se správného zabezpečení jednotlivých pracovních stanic. Správné pochopení vztahů v organizaci bylo pro úspěšné provedení analýzy rizik klíčové.

Má inženýrská práce se, jak už bylo několikrát řečeno, zabývá srovnáním několika softwarových nástrojů, které jsou k dispozici k nahlédnutí ať už v demo verzích či tzv. flash verzích. Softwarových nástrojů pro analýzu rizik existuje celá škála a komplexní srovnání všech by překročilo rámec této práce. Co lze však s jistotou říci je, že většina těchto nástrojů používá k analýze stejných principů. Pouze jsou měněny hodnotící škály.

Jako nejvhodnější pro použití ve firmách se mi jeví software CRAMM, Ranit či Riskan mohl bych ve výčtu programů jistě dále pokračovat. Všechny tyto nástroje podporují legislativu EU. Podle jejich výrobců také využívají normy, jako např. ČSN ISO/IEC 17799, ČSN ISO/IEC 27001, ČSN ISO/IEC TR 13335 a dalších.

Analýza rizik je velice složitá zdlouhavá záležitost a nejvhodnější je ji řešit v týmu v rámci cíleného projektu, s využití principů projektového řízení.

ZÁVĚR V ANGLIČTINĚ

What to say in conclusion? Every organization meets day by day risks which they must face. It is necessary to encounter these risks and learn to manage them. For these purposes it is necessary to describe risks and look at them from organization's perspective, because each has different priorities.

To control these risks every company needs to properly choose an appropriate methodology of analysis. How do we know that the methodology is appropriate for the organization? There is no bright answer, unfortunately. We must regard the problem with certain complex and systematic overview. And last but not least, focus on the problem from the perspective of the organization.

The main question to ask is, what risks we need or want to eliminate and / or control. In this case, we have focused on risks associated with securing data assets. There were suggested some recommendations based on performed analysis, mostly focused on the appropriate arrangements for individual workstations. For proper understanding of the relationships in the organization, was successful implementation critical.

This paper contains, as it was mentioned several times, comparison of several software tools for risk analysis, which were available for consultation either in demo-versions or flash-versions. There are many tools for risk analysis realization, and complete comparison would have gone beyond this work. But we should say certainly, that the most of them is based on similar principles.

In my opinion, the most useful is CRAMM software, RANIT or Riskan. Each of these tool supports making of analysis due to European union's legislation and standards such as ISO/IEC 17 799, ISO/IEC 27001, ISO/IEC TR 13 335 etc.

Risk analysis is complex and mostly lengthy thing and it is best to be addressed within the team targeted project, using project management principles.

SEZNAM POUŽITÉ LITERATURY

[1] BUMBA, Jan; KELNAR, Lubomír; SLUKA, Vilém. *Postupy a metodiky analýz a hodnocení rizik pro účely zákona o prevenci závažných havárií* [online]. Praha : Výzkumný ústav bezpečnosti práce, v.v.i., 2000 [cit. 2011-04-03]. Dostupné z WWW: <http://www.vubp.cz/index.php/component/docman/doc_download/152-postupy-a-metodiky-analyz-a-hodnoceni-rizik-pro-uely-zakona-o-prevenci-zavanych-havarii>.

[2] *Cramm* [online]. 2011 [cit. 2011-03-18]. Cramm. Dostupné z WWW: <www.cramm.com>.

[3] ČERMÁK, Miroslav. Řízení informačních rizik v praxi . 1. Brno : Tribun EU, 2009. 134 s. ISBN 978-80-7399-731-1.

[4] ČSN ISO/IEC 27001:2006. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. [s.l.] : Český normalizační institu, 2006-10. 35 s.

[5] ČSN ISO/IEC 27002:2006. , Informační technologie – Soubor postupů pro management bezpečnostiinformací.. [s.l.] : ČSN, 2007-06-18. 36 s.

[6] DOUCEK, Petr; NOVÁK, Luděk. Systém řízení bezpečnosti informací : mezinárodní normy a zkušenosti z praxe. In *Responding to Global Economic Challenges with IT* [online]. Praha : Proceedings of the 17th International Conference on Systems Integration 2009, 2009 [cit. 2011-03-26]. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2009/system-rizeni-bezpecnosti-informaci-mezinarodni-normy-a-zkusenosti-z-praxe.pdf>. ISBN 978-80-245-1534-2.

[7] Haxer [online]. 2006 [cit. 2011-02-03]. Dostupné z WWW: <http://www.haxerweb.com/>.

[8] *ISACA : Trust in, and value from, information systems* [online]. 2011 [cit. 2011-04-23]. Dostupné z WWW: <https://www.isaca.org/Pages/default.aspx>.

[9] *ISMS : bezpečnost informací, řízení rizik, ochrana osobních údajů* [online]. 2008-2011 [cit. 2011-03-26]. Dostupné z WWW: <http://www.isms.cz/>.

[10] Kolektiv autorů. Příručka manažera I - Informační bezpečnost. Praha : TATE International s.r.o., 2001. 124 s. ISBN 80-902858-4-8.

[11] Krajské zařízení pro další vzdělávání pedagogických pracovníků. Kvic [online]. 2009-10-15 [cit. 2011-03-31]. Kvic. Dostupné z WWW: <http://www.kvic.cz/GetFile/?ID=2157>.

[12] KUNDEROVÁ, Ludmila. *Bezpečnost IS/IT* [online]. 2010 [cit. 2011-03-12]. Analýza rizik. Dostupné z WWW: <https://akela.mendelu.cz/~lidak/bis/3ar.htm>.

[13] KUNDEROVÁ, Ludmila. *Bezpečnost IS/IT* [online]. 2010 [cit. 2011-03-26]. Výstavba bezpečnostní politiky. Dostupné z WWW: < https://akela.mendelu.cz/~lidak/bis/2vystavba.htm>.

[14] MARTINOVIČOVÁ, D. Pojištění podnikatelských subjektů. 1. vydání. Ostrava: KEY Publishing s.r.o., 2007. 236 s. ISBN 978-80-87071-08-3.

[15] *Palisade : Maker of the world's leading risk and decision analysis software, @RISK and the DecisionTools Suite* [online]. 2011 [cit. 2011-03-31]. Palisade. Dostupné z WWW: <http://www.palisade.com/risk/>.

[16] RANIT - Risk Analysis Information Tool [online]. 2011 [cit. 2011-03-09]. Dostupné z WWW: <http://www.ranit.cz/>.

[17] *Risk Analysis Consultants* [online]. 2010 [cit. 2011-03-18]. RAC ISMS: Zavedení systému řízení bezpečnosti informací. Dostupné z WWW: <http://www.rac.cz>.

[18] *RiskWorld : Security Risk Analysis & Assessment, and ISO 27000 Compliance* [online]. 2010 [cit. 2011-04-03]. Dostupné z WWW: <http://www.riskworld.net/>.

[19] Security Risk Assessment Headquarters [online]. 2010 [cit. 2011-04-03]. Dostupné z WWW: <http://www.riskwatch.com/>.

[20] SMEJKAL, Vladimír; RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. Praha : Grada Publishing a.s., 2006. 296 s. ISBN 80-247-1667-4.

[21] SVOJANOVSKÝ, Petr; KRESLÍKOVÁ, Jitka. Risk management [online]. 2.8.2010 [cit. 2011-03-20]. Řízení rizik v bezpečnosti IT. Dostupné z WWW: <http://www.risk-management.cz/clanky/Rizeni-rizik-v-bezpecnosti-sluzeb-IT-Svojanovsky_Kreslikova.pdf>.

[22] Úřad pro ochranu osobních údajů [online]. 2000 [cit. 2011-04-20]. Dostupné z WWW: <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5>.

[23] *Vlastní zdroj*.

SEZNAM ZKRATEK

ALE	Annualized Loss Expectancy - Předpokládaná roční ztráta
ANSI	American National Standards Institute
AR	Analýza rizik
BIOS	Basic Input-Output System
BIT	Bezpešnostní informační systémy
BP	Bezpečnostní politika
CBP	Celková bezpečnostní politika
CCTA	Central Computing and Telecommunications Agency
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CL	Checklist Analysis Analýza kontrolním seznamem
CRAMM	CCTA Risk Analysis and Management Method
ČR	Česká republika
DoS	Denial of Service
DDos	Distributed Denial of Service
ETA	Event Tree Analysis Analýza stromu událostí
FMEA	Failure Modes and Effects Analysis Analýza způsobů a důsledků poruch
FTA	Fault Tree Analysis Analýza stromu poruch (poruchových stavů)
FTP	File Transfer Protocol - protokol pro přenos souborů
HAZOP	Hazard and Operability Analysis Studie nebezpečí a provozuschopnosti
HRA	Human Reliability Analysis Analýza lidské spolehlivosti
IB	Informační bezpečnost
IEC	International Electrotechnical Commission - Mezinárodní elektrotechnická komise
IEEE	Institute of Electrical and Electronics Engineers - Institut pro elektrotechnické a elektronické inženýrství
IP	Internet Protocol
IS	Informační systém
ISMS	Information security management systém –Systém řízení informační bezpečnosti

ISO	International Organization for Standardization
IT	Informační technologie
MAC	Media Access Control - jedinečný identifikátor síťového zařízení
NAPŘ	Například
NIST	National Institute of Standards and Technology
OS	Operační systém
PDCA	Plan Do Check Act - „plánuj, udělej, zkontroluj, jednej“
PHA	Preliminary Hazard Analysis - Předběžná analýza zdrojů rizika
RiskPAC	Risk Analysis and Business Impact Analysis
RiskWatch	Risk management and Risk Assessment
RR	Relative Ranking - Relativní klasifikace
SR	Safety Review - Bezpečnostní prohlídka
SŘBI	Systém řízení bezpečnosti informací
THP	Technicko hospodářský pracovník
VPN	Virtual Private Network
W-I	What-If „Co se stane, když …“
W-I/CL	What-If/Checklist „Co se stane, když …“ / kontrolní seznam
Wi-Fi	Wireless Fidelity - komunikační standard pro bezdrátový přenos dat
WWW	World Wide Web – celosvětová síť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ZABEZPEČENÍ PŘÍSTUPU DO SYSTÉMU

Zabezpečení přístupu do systému

V řadě systémů je využíván autorizovaný přístup, který lze zajistit následujícími mechanismy:

- autorizace pomocí hesla,
- autorizace pomocí předmětu, např. identifikační karty,
- autorizace pomocí biometrických prvků.

Autorizace pomocí hesla

Autorizace pomocí hesla je založena na principu posloupnosti daných znaků, které využívá optimálně jeden uživatel, který se jeho prostřednictvím dostane do chráněné oblasti. Je nejjednodušším a nejlevnějším systémem, proto je v praxi také hojně využíván především při zabezpečení počítačů a počítačových sítí, e-mailů, bankovních účtů apod. Tento systém však poskytuje nižší stupeň zabezpečení a doprovází jej také řada nevýhod, např. vyzrazení hesla nebo jeho dekódování či vysledování při zadávání znaků nebo zapomenutí hesla.

Zásady vytvoření bezpečného hesla

Bezpečnost používání hesel se dá zvýšit za předpokladu použití správně vytvořeného hesla. To se dá vytvořit s dodržování několika jednoduchých zásad :

- **Délka hesla** – obecně můžeme říci, že čím delší heslo tím lépe, obecně však platí, aby heslo mělo minimálně 8 znaků.
- **Kombinace znaků** – co dělá heslo bezpečnějším je kombinace velkých a malých písmen, doplněná o speciální znaky a kombinaci čísel. Vyhnul bych se extrémním znakům, které by mohly způsobovat problémy na jiné než české klávesnici.
- **Slovníkové výrazy** – lámání hesel hrubou silou (Brute Force) je časově náročné. Hekři mají připraveny často používaná slova a při troše štěstí se jim takové heslo podaří odhalit. Jistou malou obranou je nahrazovat některé znaky jinými. (př: @-a, &-a, 3-e, 4-a.)

- **Osobní údaje** – nikdy nepoužívejte ve svém hesle. Jakékoliv své osobní údaje (příjmení, jméno, jména svých blízkých a mazlíčků, přezdívky, datum narození, rodná čísla, telefonní čísla, atd.)
- Přihlašovací jméno – dejte si pozor, aby heslo neosahovalo stejný text jako přihlašovací jméno. Velkým nesmyslem je používat heslo typu (heslo, heslo123, 12345, atd.)

PŘÍLOHA P II: ISMS V MALÝCH A STŘEDNÍCH FIRMÁCH

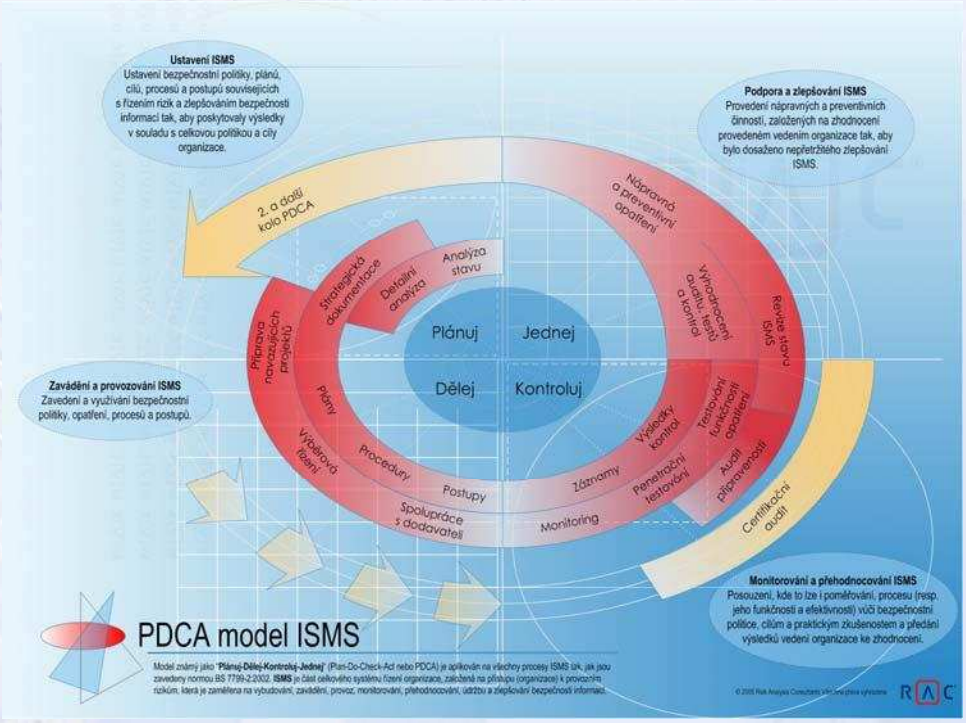
ISMS v malých a středních firmách

1.díl Plan - Plánuj

Zásady budování a využívání systému řízení bezpečnosti informací (ISMS – Information Security Management System) stanovené dnes platnými a v českém jazyce dostupnými normami (tj. ISO/IEC 17799:2005 a ISO/IEC 27001:2005) se dají interpretovat různými způsoby v závislosti na velikosti organizace. Jejich podstata však zůstává stejná – informační bezpečnost musí být řízena. Velikost organizace a rozsáhlost jejího systému jsou jedním ze základních parametrů při určování způsobu zavádění ISMS. Tento čtyřdílný seriál popisuje kroky zavádění a využívání ISMS podle modelu Plánuj – Dělej – Kontroluj – Jednej - (PDCA - procesní diagram používaný ISO 27001). První část srovnává, podle velikosti firmy, činnosti v zřejmě nejtěžším kroku Plánuj (Plan), o dalších krocích pojednávají následující díly.

Zavedení ISMS

Doporučení, zda zavést ISMS, zní pro všechny organizace **jednoznačně *ANO*** a otázka jejich velikosti je irelevantní. ISMS lze zavést a používat v organizaci s deseti pracovníky, a stejně tak i v obřím holdingu, kde se každý den můžete potkat s tisíci zaměstnanci. Zjednodušeně lze říci, že ISMS je jen jeden a to ten, který je popsán v normě ISO 27001. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobů zpracování dat a jejich hodnoty apod. Například bezpečností politika, jako ten nejvyšší dokument o bezpečnosti informací v organizaci, může být velmi podobná pro živnostníka i pro obrovskou akciovku. Naopak tomu je o organizace bezpečnosti. Pokud se ISMS zavádí ve velké společnosti, je nutné pro tisíce uživatelů zřídit samostatné bezpečností oddělení s 5-10 lidmi, ve střední firmě na to stačí 2 pracovníci a pokud máme systém pro 10 lidí, tak jeden člověk na půl úvazku je až moc.



Strategie bezpečnosti

Strategie bezpečnosti nebývá ve středních firmách popsána nijak detailně, jako je tomu zvykem ve velkých společnostech. Zpravidla stačí, aby ředitel středně velké organizace měl vůli řešit bezpečnostní otázky a pak není nutné sepisovat rozsáhlý dokument o koncepci řízení bezpečnosti. Je dostatečné, pokud se ředitel na své poradě s dalšími vedoucími pracovníky shodne na strategii a ta se začne prosazovat. V malých firmách je toto ještě jednodušší, protože od první úvahy ředitele je k započetí realizace stejně daleko, jako od jeho dveří k zasedací místnosti

Správná volba a způsob prosazení strategie řízení bezpečnosti není jednoduchá záležitost a už v tuto chvíli je vhodné se obrátit na odborníky, pokud tito nejsou ve vlastních řadách. Pro střední a malé firmy je však samotnou strategií už jen to, že se organizace roz-

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

1.díl Plan - Plánuj

hodla řídit bezpečnost svých informací. Pokud se rozhodnutí rozšíří na řízení bezpečnosti v souladu se standardem ISO 27001 (definující způsob aplikace opatření z ISO 17799), je strategie vcelku rozumně nalajnována a další diskuse o tom, co a jak a kdy provádět je zbytečná, protože zavedení ISMS má své pevné zásady a postupy.

Bezpečnostní politika

Proces vytvoření a schválení *Bezpečnostní politiky* je **společný pro všechny typy organizací** včetně publikování politiky vůči všem zaměstnancům. Také rozsah a obsah dokumentu je velmi podobný. Nedávno jsme v rámci projektu zavádění ISMS tvořili bezpečnostní politiku pro velkou telekomunikační společnost (cca 3000 lidí). Souběžně jsme podobný projekt prováděli ve státní organizaci se stovkou zaměstnanců. Oba dokumenty měly strukturu podle ISO 17799 a na první pohled byly velmi podobné. Bezpečnostní politika **definuje zásady a pravidla na úrovni cílů** a ty jsou zpravidla shodné pro všechny organizace. Musí také obsahovat odkaz na dokument popisující rozsah ISMS, protože systém řízení bezpečnosti v malé ani střední firmě nemusí být zaveden pro celý informační systém (stejně jako systém řízení kvality podle ISO řady 9000).

V dokumentu by měla být popsána mj. **organizační struktura bezpečnosti**, v které se také lišily obě výše zmiňované politiky. Popis bezpečnostních rolí a jejich odpovědností musí odpovídat velikosti systému a počtu uživatelů. Navíc je nutné respektovat zavedenou organizační strukturu a proto je možné pro stejně velké společnosti použít různé modely organizace bezpečnosti.

V malých firmách nemusí být jmenován bezpečnostní ředitel na plný úvazek. Jeho kompetence zpravidla bere na sebe ředitel firmy, který prosazuje bezpečnostní zásady kombinací direktivního a osobního přístupu. Ředitel má na starosti mj. účinnou implementaci bezpečností politiky a vyhodnocování (ne analýzu) rizik a rozhodnutí o způsobu jejich pokrytí. Podobně je tomu i s dalšími bezpečnostními rolemi. Administrátor sítě má odpovědnost za praktické provedení bezpečnostních zásad a metodik, o kterých rozhodl ředitel. Některé činnosti z oblasti bezpečnostní dokumentace mohou být v kompetenci vybraného pracovníka, který může mít na starosti také audit. Kumulace práv a pravomocí souvisejících s bezpečností informací a se správou systému je pro malé organizace rizikem, které je nutné přijmout.

Podle Průzkumu informační bezpečnosti 2003, mají 3 firmy ze 4 bezpečnostní oddělení jako součást útvaru IS/IT a lze předpokládat, že spíše velké společnosti vytváří separátní tým lidí s odpovědností za oblast bezpečnosti. Pokud má systém pouze několik desítek uživatelů, je možné jednotlivé kompetence rozdělit mezi několik stávajících pracovníků nejen z IT. **Nemusí však být vždy efektivní** pro 150 lidí **jmenovat bezpečnostního ředitele na plný úvazek**. Tímto se může stát například zástupce ředitele a ne zřídka spadnou dané kompetence na vedoucího IT oddělení. Kumulace pravomocí zejména ve výkonu bezpečnosti je rizikem i pro firmu střední velikosti.

Příkladem může být projekt analýzy rizik který jsme prováděli ve společnosti s cca 80ti uživateli. Celý systém měli na starosti dva administrátoři, kteří mezi sebou sdíleli přístupová práva ke všemu. Analýza ukázala, že pochybnosti vedení o jejich loajalitě vůči firmě jsou více než oprávněné a obava z poškození systému (vymazání nebo modifikace dat) je zcela na místě. Nicméně bylo nutné jmenovat pracovníka odpovědného za výkon bezpečnosti a situace nedovolovala okamžitou výměnu obou administrátorů ani najmutí nového zaměstnance.

Řešení bylo jednoduché: bezpečnostním manažerem byl jmenován zástupce ředitele, každá hlavní aplikace (celkem měli tři) dostala svého vlastníka a při správě např. při definici uživatelských přístupových práv, bylo zavedeno tzv. „pravidlo čtyř očí“ (také známé jako „pravidlo dvou osob“). Pokud byl zakládán nový uživatel nebo měněna práva stávajícímu, bylo vyžadováno potvrzení administrátora sítě a správce aplikace. Ani jeden toto nemohl provést samostatně. Sám administrátor neměl přístup ke konkrétním datům, protože ho nepotřeboval. Je zřejmé, že původní administrátoři ztratili neomezenou vládu nad systémem a tím také možnost cokoli poškodit.

Organizace bezpečnosti v souvislosti s kumulací práva a povinností v oblasti bezpečnosti není vyřešena ani v mnoha velkých organizacích. Téměř v každé se najde jeden nebo několik „neomezených vládců systémů“, na jejichž oddanost firmě všichni spoléhají. Pro tyto situace nelze nalézt univerzální řešení a proto jsou prosazována a uplatňována různá pravidla a technologická opatření, jejichž popis je na samostatný článek.

Analýza rizik

Znalost bezpečnostních rizik je základním kamenem pro vytvoření a správně řízení ISMS. Proto provedení analýzy rizik je nutná nikoli však postačující podmínka pro všechny organizace. Rozhodnutí, zda provést detailní či jen základní analýzu, je na vedení firmy, nicméně pouze detailní analýza provedená podle vybrané metodiky může poskytnou podklady pro efektivní výběr a implementaci bezpečnostních opatření.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

1.díl Plan - Plánuj

Analýza musí zabrat celý rozsah ISMS a její hloubka závisí na dostupných zdrojích a požadovaných výstupech. V malé firmě lze provést detailní analýzu (například metodikou CRAMM) **za dva až tři týdny**. Je možné spolupracovat s konzultační firmou nebo vše udělat za pomoci vlastních (znalých) pracovníků. Zatížení firmy je minimální a počet respondentů nepřevýší 5 lidí. Pro hodnocení dat se vyberou 2-4 zaměstnanci, kteří nejvíce znají charakter a použití definovaných datových aktiv, a administrátor sítě provede hodnocení hrozeb a zranitelností včetně identifikace existujících protiopatření.

Detailní analýza ve středně velké organizaci trvá zpravidla **3-5 měsíců** a důvodem není ani tak rozsah, který je samozřejmě větší než u malých firem, ale rychlost odezvy od respondentů či recenzentů (schvalovatelů) výstupů z analýzy. Pro malou firmu jsou závěry shrnuty v jedné zprávě o analýze rizik, po které následuje návrh implementačního plánu. Prezentace takových závěrů je velmi rychlá a jednoduchá a odezva na ni téměř okamžitá. Ve středních firmách se projevují první známky nutné byrokracie a pro schválení závěrů je nezbytné (občas však zbytečné), aby výstupní dokumenty prošli minimálně 3 pracovníci.

Pokud je analýza prováděna dodavatelským či partnerským přístupem, jsou v týmu dva až tři **externí pracovníci** a stejný počet interních. Analýza prochází vždy napříč celou organizací a tomu odpovídá i zatížení dotčených pracovníků. Počet respondentů pro hodnocení dat se pohybuje mezi 5 až 15 uživateli a hodnocení hrozeb a zranitelností včetně zavedených protiopatření je úkolem pro 3-5 administrátorů sítě či další respondenty odpovědné za různé oblasti bezpečnosti (např. pracovník s odpovědností za fyzickou bezpečnost).

Obsah dokumentace, která je výstupem z projektu analýzy rizik, je velmi podobný pro všechny typy organizací. Liší se jen rozsahem podpůrných reportů, které jsou zpravidla výstupem z použité metodiky, ale manažerský styl zpráv o aktivech a dopadech či o analýze rizik je shodný. Pro malé firmy je možné vytvořit jen jednu zprávu, ale pro střední organizace je vhodné závěry separovat minimálně do dvou dokumentů.

Plán implementace a Prohlášení o aplikovatelnosti

Krokem logicky navazujícím na analýzu a poslední činností v části plánování podle modelu PDCA je vytvoření **Plánu implementace** a následně Prohlášení **o aplikovatelnosti (opatření)**. Bezpečnostní protiopatření by měla být vybrána na pokrytí zjištěných rizik a způsob jejich výběru je nezávislý na velikosti organizace. Jejich implementace bude rozdílná, ale například pro všechny organizace lze použít BIS-PD 3005 nebo knihovnu protiopatření CRAMM. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. Při výběru bezpečnostních opatření je vždy nutné zohlednit jejich **dopad na uživatele a na procesy organizace**. V malé firmě je možné jednouše a rychle změnit téměř jakýkoli proces, aby byl více bezpečný. Stačí vůle ředitele a o změně je rozhodnuto. Čím je organizace větší, tím je složitější měnit procesy a zavedené postupy. Proto je nutné při výběru protiopatření ve střední firmě více respektovat současný stav.

Prohlášení o aplikovatelosti (opatření) je jedním z dokumentů nutných k certifikaci. Obsahuje informace o implementovaných opatřeních normy, případně dalších protiopatřeních navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, proč dané protiopatření bylo či nebylo vybráno k zavedení. Pokud firma neplánuje být v budoucnosti certifikována, není nutné vytvářet samostatný dokument. Pro malou i střední firmu je plně dostačující, pokud se vhodným způsobem zaznamená rozhodnutí o výběru tak, aby i za několik měsíců bylo jasné, proč není nutné určité protiopatření implementovat.

Závěr 1.dílu

Zavedení systému řízení bezpečnosti informací je správným krokem pro každou organizaci, která chce zabezpečit své informace a dostatečně řídit rizika. S ohledem na její velikost je však nutné velmi rozdílně a hlavně „s citem“ interpretovat jednotlivá doporučení normy. Úvodní, výše popsaný krok Plánuj (Plan) je v prvním průchodu modelu PDCA vždy velmi složitý a poměrně zdlouhavý, nicméně velmi důležitý.. V následujících třech dílech budou podobně srovnány činnosti v dalších krocích vedoucích k implementaci a provozu (Dělej/Do), monitorování a kontrole (Kontroluj/Check) a zlepšování ISMS (Jednej/Act) včetně následné certifikace systému řízení a dokumentů k ní nutných.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

1.díl Plan - Plánuj

V celém seriálu jsou detailně popsané činnosti pro zavedení a provoz ISMS. Jejich souhrn pro jednotlivé kroky PDCA je uveden za každým dílem. Pro rychlé srovnání jsou popisy činností, případně výstupů, uvedeny

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	**Plán / projekt bezpečnosti**	Schválení strategie/plánu pro bezpečnost	Schválení celkové koncepce bezpečnosti Schválení projektu bezpečnosti	Schválení celkové koncepce bezpečnosti Vymezení rozsahu projektu + odhad zdrojů a harmonogramu Schválení projektu bezpečnosti Analýza stavu bezpečnosti (GAP analýza)
	Bezpečnostní politika	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů i strategií pro jejich dosažení včetně závazku podpory a alokace zdrojů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS
	Organizace bezpečnosti	Oddělení/Odbor bezpečnosti: NE Bezp. ředitel: ředitel firmy Bezp. administrátor: administrátor IS Bezp. auditor: odpovědnost delegována na pracovníka (mimo administrátora IS)	Oddělení/Odbor bezpečnosti: ANO (pod IT) Bezp. ředitel: jmenován člen vedení Bezp. manažer: jmenováni 1-3 Bezp. auditor: pracovník interního auditu, nebo delegováno na pracovníka mimo IS Bezp. administrátoři: administrátoři částí systémů	Oddělení/Odbor bezpečnosti: ANO (v IT i mimo) Bezp. ředitel: jmenován člen vrcholového managementu Existuje oddělení bezp. s odpovědnostmi za řízení i správu všech oblastí bezpečnosti Bezp. auditor: zajišťuje oddělení interního auditu
	Analýza rizik	Nutné provést: ANO Čas: max. 1 měsíc Členové projektového týmu: jeden interní pracovník a/nebo konzultant Respondenti: max. 5 Výstupy: Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 3 - 5 měsíců Členové projektového týmu: 2-3 interní pracovníci a/nebo 2-3 konzultanti Respondenti: 5-20 Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 4 - 12 měsíců Členové projektového týmu: 2-n interních pracovníků a/nebo 2-3 konzultanti Respondenti: desítky Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán
	Výběr opatření a plán implementace	Protiopatření vyplývají z AR Prosazuje: ředitel firmy	Protiopatření vyplývají z AR Prosazuje: ředitel a vedoucí oddělení společně	Protiopatření vyplývají z AR Prosazuje: podle významu protiopatření od vedení společnosti po vedoucí oddělení
	Prohlášení o aplikovatelnosti	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace	Dokument Prohlášení o aplikovatelnosti
ISMS	**Doporučení zavést ISMS**	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

Seriál článků s názvem „ISMS v malých a středních firmách“ popisuje proces zavádění, využívání a zlepšování systému řízení bezpečnosti informací (dále ISMS) tak, aby splnil požadavky pro zajištění bezpečnosti informací dle normy ISO/IEC 17799:2005 a požadavky pro zavedení a provoz ISMS dle normy ISO/IEC 27001. Způsob naplnění těchto požadavků lze vždy přizpůsobit specifickým podmínkám každé organizace a ne jinak je tomu i v prostředí malých a středních firem. Tento 2.díl popisuje činnosti kroku Dělej (Do), ve kterém jsou potřebná opatření ISMS zaváděna do praxe a využívána

Provoz ISMS

Úvodní díl tohoto seriálu pojednával o hlavních krocích první fáze Plánuj (Plan) procesu zavádění a využívání ISMS v organizacích, dle procesního modelu PDCA (Plan-Do-Check-Act), obecně používaného pro implementaci a provoz systémů řízení. Jeho obsahem bylo mj. stanovení rozsahu ISMS, vytvoření bezpečnostní politiky, definování organizace bezpečnosti a provedení analýzy rizik. Výstupem z analýzy jsou doporučení na zajištění bezpečnosti, která by měla být implementována, zdokumentována a správně používána právě v kroku Dělej (Do).

Způsob implementace opatření a metody prosazení

Výběr okruhů opatření ISMS je podobný pro malou i středně velkou firmu. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. V malé firmě rozhoduje zpravidla ředitel o tom, kdo bude mít přístup k jakým datům. Ve středně velké firmě je nutné vytvořit proces přidělování uživatelských oprávnění, aby nemohla nastat situace, se kterou jsme se setkalí v jedné softwarové firmě (cca 70 uživatelů): Administrátor sítě byl odpovědný za přidělování přístupu na základě požadavků vedoucích oddělení. Ti však zásadně odmítali vyplnění jakéhokoli formuláře (zdržovalo je to) a administrátor odmítal přidělovat práva na základě telefonické žádosti. Situaci vyřešilo zavedení administrativního procesu přidělování přístupu pro všechny uživatele systému.

V malých firmách je běžné, že **bezpečnostní ředitel** (zpravidla ředitel firmy) **rozhodne ráno** o změně délky hesla z 6 na 9 znaků. Bezpečnostní administrátor (zpravidla správce sítě) protiopatření zavede ještě před obědem a v rámci příjemně strávené siesty si všichni uživatelé rádi změní heslo. Následující den je protiopatření v systému již zcela zavedeno a automaticky používáno a akceptováno. Taková rychlost implementace je typická pouze pro malé firmy. Ve středně velkých organizacích je nutné vzít v úvahu akceptovatelnost protiopatření ze strany uživatelů a další souvislosti jejich realizace. Prosadit například změnu délky hesla vyžaduje revizi příslušné směrnice, **zapojení několika administrátorů** do práce a seznámení desítek uživatelů se změnou, například formou školení. Poté by měla následovat kontrola funkčnosti opatření.

Bezpečnostní dokumentace

Značné rozdíly mezi malou a středně velkou firmou jsou ve formě a míře detailu dokumentace bezpečnosti. Není příliš známo, že uvedené normy **striktně nevyžadují** papírovou formu dokumentace ani její pevnou strukturu, ale ponechávají na preferencích jednotlivých firem, jakou formu a obsah zvolí. Přitom právě obava z přílišné formální administrativy nejčastěji odpuzuje malé a středně velké organizace od zavádění doporučení těchto norem. Dokumentace ISMS požadovaná k certifikaci podle ISO 27001 pochopitelně musí obsahovat určité, taxativně uvedené typy dokumentů, dané jednotlivými kroky procesu ISMS, ale jejich rozsah, obsah a forma může být překvapivě jednoduchá a flexibilní, jak si popíšeme dále.

Pracovníci malých firem se osobně znají a velká část bezpečnosti je založena na jejich vzájemné důvěře. Není nutné vytvářet složitý systém politik, směrnic a postupů. Postačí stručné pravidlo, že bezpečnostní dokumentace je vedena ve sdílené složce elektronické pošty, definovat role a přístupy zodpovědných osob a nezbytné typy bezpečnostních dokumentů realizovat formou elektronických záznamů, obsahující stručný popis realizace daného pravidla, postupu nebo odpovědnosti.

Středně velká firma se v této oblasti opatření blíží firmě velké. Zde je již **nutné zavádět podrobnější administrativní procedury**, neboť existuje více oddělených rolí a odpovědností a také více definovaných pravidel. Tato administrativa je nutná, aby byly eliminovány činnosti, které se dějí při práci s daty jen tak, na „dobré slovo“. Pracovníci středně velkých firem se většinou také znají, ale jistá úroveň anonymity může být impulsem k tomu, že se někteří budou snažit bezpečnostní procedury obejít zejména, když nebudou přesněji definovány a kontrolovány.

Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky no-

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

rem. Příklady rozsahu bezpečnostní dokumentace pro typické kvalitativní úrovně řízení bezpečnosti v organizacích, jak se s nimi nejčastěji setkáváme v praxi, jsou uvedeny v tabulce na konci celého seriálu.

Program zvyšování bezpečnostního povědomí

Mezi další metody prosazení bezpečnosti v organizacích patří program zvyšování bezpečnostního povědomí v organizacích. Tento krok, jakkoliv komplikovaně znějící, je ve skutečnosti poměrně **jednoduchá, levná a velice účinná metoda**, která bývá bohužel mnohdy v malých a středně velkých organizacích opomíjena. Má za cíl zvýšit u všech zaměstnanců informovanost jednak o obecných principech a souvislostech informační bezpečnosti a o konkrétních rizicích, opatřeních, odpovědnostech a pravidlech, vyplývajících ze zaváděného nebo již provozovaného ISMS.

V čem vlastně spočívá „síla jednoduchosti" tohoto opatření? Program je zaměřen na zaměstnance (a na externí spolupracující osoby apod.), kteří jsou často zdrojem bezpečnostních incidentů a kteří mohou, pokud jsou správně informováni, svým včasným jednáním šíření a škodám incidentů zabránit. Stále se ještě při každém bezpečnostním školení firem různých velikostí setkáváme s mnoha užaslými tvářemi, když vysvětlujeme, že nejvyšší hodnotu pro organizaci mají v informačním systému data a nikoliv hardware a software. Existuje stále také mnoho uživatelů, kteří pokládají svou disketu nebo lokální harddisk „svého PC" v kanceláři za mnohem bezpečnější místo, než síťový disk s transparentně nastavenými přístupovými právy a pravidelným zálohováním.

U malých firem postačí, pokud zvyšování bezpečnostního povědomí opřeme o stručné **vstupní školení všech zaměstnanců** a občasné prodiskutování aktuálních bezpečnostních otázek dle potřeb organizace a vývoje nových potencionálních hrozeb (může být využito outsourcingu).

U středně velkých organizací se zvyšují nároky na informovanost zaměstnanců a rozsah jejich znalostí o bezpečnostní problematice, realizovaných opatřeních, povinnostech a odpovědnostech z nich vyplývajících. **Základní bezpečnostní školení** se doporučuje realizovat pro všechny nové zaměstnance bez rozdílu. Zde se však vyplatí potrápit zaměstnance trochu déle a více se zaměřit na popis a rozbor typických hrozeb a bezpečnostních incidentů. Bohužel právě **odstrašující příklady**, včetně **zmínky o sankcích** při nedodržování pravidel, zaberou i tam, kde dobrá rada nepřesvědčí. Samozřejmě i u středně velkých organizací by nemělo být opomenuto informovat všechny zaměstnance dle potřeby o aktuálních hrozbách a opatřeních, např. formou zřízení centrálního informačního místa o bezpečnostních otázkách na firemním intranetu.

Způsob zvládání rizik za provozu

Jedním z hlavních důvodů proč zavádět ISMS, je potřeba zajistit kontinuální proces zvládání a řízení informačních rizik. Základem pro jejich úspěšné řízení je identifikace a analýza všech potencionálních rizik a následné rozhodnutí o způsobu jejich zvládání a sledování v čase. Účelem řízení rizik není veškerá identifikovaná rizika bezezbytku pokrýt (mnohdy s vynaložením neadekvátních zdrojů), ale pokrýt zvolenými opatřeními pouze taková, u kterých je to efektivní. Ostatní **rizika** může organizace **akceptovat a sledovat**, některá může přenést na jinou organizaci, případně je pojistit. Pouze pokud organizace zná a sleduje všechna rizika související se zabezpečením informací a adekvátně rozhoduje o způsobu jejich zvládání, potom může prohlásit, že tyto rizika řídí (má je pod kontrolou).

Tyto zásady jsou opět společné pro všechny velikosti a typy organizací. Otázkou je, jak se s nimi malé a středně velké organizace efektivně vypořádají. U těchto firem bude většinou velikost negativního dopadu bezpečnostního incidentu i pravděpodobnost jeho výskytu průměrně nižší než u velkých společností. Je tedy zřejmé, že vedení těchto firem bude mít **tendence více rizika akceptovat** a přesune svůj zájem spíše do oblasti jejich sledování a efektivního zvládání případných bezpečnostních incidentů.

Pro sledování nových typů rizik a rozpoznání bezpečnostních incidentů je nutné **aktivovat generování záznamů** o nejdůležitějších bezpečnostních událostech (v papírové i elektronické formě) a tyto záznamy vyhodnocovat. Mezi takové záznamy patří minimálně záznamy o přístupech do budov a zabezpečených místností, přihlašování a odhlašování do počítačových systémů a citlivých aplikací, přístupy a manipulace se zvlášť citlivými informacemi apod. Řada těchto záznamů je generována automaticky po instalaci jednotlivých systémů (EZS, doménový řadič, účetní aplikace apod.).

Na co se však často zapomíná, je jejich systematické ukládání, zabezpečení a vyhodnocování. Jeden příklad za všechny: Při forenzním zkoumání zneužití systému el. bankovnictví v jedné malé firmě se ukázalo, že oprávnění zaměstnanci této firmy se všichni přihlašovali do systému elektronického bankovnictví pod stejným uživatelským účtem, i když tato aplikace samozřejmě nabízela individuální přihlašovací účty. Protože byl tento sytém provozován na samostatném PC, se zastaralou verzí Windows, navíc nepřipojeném k firemní

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

LAN, neexistovaly žádné jiné typy záznamů o jeho využívání. Z bankovního účtu této firmy byly převedeny částky na cizí účty transakcemi ověřenými platnými privátními elektronickými klíči této firmy. Naštěstí byly tyto transakce zrealizovány ve dnech, kdy nikdo ze zaměstnanců elektronického bankovnictví nepoužil. Vyšetřování nakonec prokázalo, že částky byly převedeny pracovníkem uživatelské podpory banky z jiného PC, na které privátní elektronické klíče poškozené firmy zkopíroval (poté, co je zcizil při jejich instalaci). Pracovník banky však smazal část nezabezpečených logů na straně serverů banky a tím ztížil prokázání činu. Tento příklad demonstruje nutnost vedení, zabezpečení a občasného vyhodnocování důležitých bezpečnostních záznamů u všech typů společností bez rozdílu.

U malých organizací bude **proces řízení a zvládání rizik realizován neformálním způsobem**, bez stanovení speciálních pravomocí a oddělení rolí. Je zde totiž účelné dosáhnout shodné úrovně informovanosti a pravomocí u všech zaměstnanců. Pro středně velké firmy je již doporučeno **rámcově definovat postupy, oddělit pravomoci** a provádět namátkové revize tohoto procesu. Pro získání přehledu o způsobu a důslednosti plnění povinností při zvládání rizik a incidentů je namístě zřídit evidenci závažných hrozeb a zranitelností a způsobů jejich pokrytí.

Nároky na provoz opatření a zajištění bezpečnosti

Součástí plánu zvládání rizik je i sledování nároků na provoz jednotlivých opatření a celkového zajištění bezpečnosti. Zatímco u malých firem není potřeba plánovat ani **vyhrazovat samostatný rozpočet**, neboť případný nákup a provoz nezbytných opatření je operativně schválen ředitelem a hrazen dle aktuálních potřeb organizace, u středních a velkých firem je nezbytné provádět alespoň rámcové plánování potřebných finančních i lidských zdrojů.

Z hlediska preferencí při výběru opatření hrají celkové nároky na jejich zavedení a provoz hlavní roli. Zatímco pro malé organizace není překážkou pružně zavádět administrativní a personální opatření i za cenu vyšších požadavků lidské zdrojů, úskalím však bývají finanční náklady na pořízení složitých technologických opatření. U velkých společností lze tyto preference vysledovat obráceně, neboť pro ně bývá snazší pružně zavést nové technologické opatření, než jej nahradit administrativními či organizačními změnami. V případě preferencí středně velkých firem je stav logicky někde uprostřed. Záleží na pružnosti řízení, technologické úrovni a znalostech pracovníků firmy, k jakým typům opatření se budou přiklánět více.

Zavedení opatření DRP a IRH

Poslední důležitou oblastí opatření při zavádění a provozu ISMS je tvorba a údržba *Havarijních plánů* (DRP – Disaster Recovery Planning) a *Postupů řešení bezpečnostních incidentů* (IRH – Incident Response Handling). Stejně jako v případě ostatních formálních postupů i zde platí, že pro malé organizace je neefektivní vypracovávat a udržovat podrobné formální havarijní plány. Pro obnovu systémů jim plně postačí vytvoření **stručného univerzálního havarijního "checklistu"** pro všechny možné případy havárie, který bude obsahovat postup bezpečného vypnutí a restartu technického vybavení a serverů, jednoduchý záznam výsledné konfigurace technologií a aplikací, postup obnovení dat ze záložních médií a seznam kontaktů na interní a externí osoby, které mohou pomoci při výskytu havárie nebo závažného bezpečnostního incidentu. Tyto havarijní postupy by měly být alespoň jednorázově otestovány a poté postačí testy opakovat až při zásadní změně používaných technologií a služeb.

U středně velkých organizací je doporučeno rozšířit zmíněný havarijní „checklist" i o popis kroků instalace jednotlivých částí informačního systému a obnovy dat a aplikací ze záložních médií. U komplikovanějších informačních systémů je třeba rozlišit obnovu klíčových aktiv od ostatních a tomu přizpůsobit priority v havarijním plánování. Pro výběr strategie způsobu obnovy a nastavení priorit je nejlépe realizovat **analýzu dopadů na činnosti organizace** (BIA – Business Impact Analysis). Pokud byla správně realizována analýza rizik, lze informace o negativních dopadech nedostupnosti jednotlivých aktiv nalézt tam. Na základě těchto výsledků je vypracován strukturovaný havarijní plán obnovy, obsahující varianty postupu dle specifikovaných typů havarijních stavů. Takovýto plán je nezbytné pravidelně testovat a aktualizovat a na základě výsledků testů (v porovnání s cíly obnovy) vylepšovat.

Závěr 2.dílu

Nebylo možné v rámci vymezeného prostoru prodiskutovat veškeré činnosti, realizované v rámci etapy „Dělej ISMS". Důležité je v závěru upozornit na fakt, že při implementaci a provozu opatření, zvolených v předchozí fázi Plánuj (Plan) se nezavádí a neprovozují pouze primárně účinná technická a organizační opatření typu: „nastav autentizační mechanizmus" nebo „eviduj pohyb osob v serverovně" ale spolu s nimi je třeba myslet na stejně důležitá sekundární řídící opatření, která mají za cíl potřebnou úroveň bezpečnosti dlouhodobě udržovat a komplexně rozvíjet.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
P L A N	**Plán / projekt bezpečnosti**			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
D O	**Způsob implementace opatření**	Okamžitě, rychle, efektivně, bez zbytečné administrativy	Podle významu protiopatření formou projektů nebo direktivním nařízením	Formou projektů
	Metody prosazení bezpečnosti	Direktivní – Osobní - Neformální Stručné pokyny (email, Intranet) a verbální působení na všechny zaměstnance	Direktivní – Neosobní - Formální Kombinace verbálních pokynů vedoucích a písemných organizačních. Závazné a formální seznámení s nařízeními	Direktivní – Neosobní – Důsledně formální Písemné organizační pokyny Závazné a formální seznámení s nařízeními
	Bezpečnostní dokumentace	Bezpečnostní politika, některé směrnice, občas konkrétní postupy	Bezpečnostní politika a další dokumentace včetně směrnic, postupů, návodů apod.	Kompletní řízená bezpečnostní dokumentace a její průběžná (plánovaná) revize
	Program zvyšování bezpečnostního povědomí	Jednorázové informace dle potřeby. Bezpečnostní minimum součástí úvodního zaškolení.	Nepravidelné pokyny a nařízení Bezpečnostní minimum součástí úvodního zaškolení. Specializovaná školení pro vybrané zaměstnance.	Strukturovaný kontinuální vzdělávací program. Pravidelná specializovaná školení všech zaměstnanců.
	Způsob zvládání rizik za provozu	Neformální proces, bez speciálních postupů a pravomocí. Pokrytí a kontrola bezprostředně po identifikaci.	Formální proces s rámcově stanoveným postupem a odpovědnostmi. Revize zvládání rizik nepravidelná, dle potřeby.	Formálně řízený proces s předem stanovenými postupy a pravomocemi. Pravidelné analýzy a kontroly zvládání rizik.
	Nároky na provoz opatření a zajištění bezpečnosti	Krátkodobé plánování. Není separátní rozpočet. Externí spolupráce není obvyklá.	Krátkodobé a střednědobé plánování Rozpočet v rámci IT/IS Prosazuje se outsourcing	Dlouhodobé plánování Individuální rozpočet Běžné využití outsourcingu
	Zavedení opatření DRP a IRH **(Havarijní plány)**	Zpravidla řada neformálních havarijních postupů pro jednotlivá aktiva.	Formální univerzální havarijní plán Postupy zvládání bezpečnostních incidentů	Provedena analýza dopadů (BIA) Strukturované havarijní plány Formální postupy zvládání bezpečnostních incidentů
C H E C K	**Monitoring IS a testování funkčnosti opatření**			
	Kontrola a audit bezpečnostních opatření			
	Revize adekvátnosti a efektivnosti ISMS			
A C T	**Vyhodnocení fáze CHECK, identifikace a analýza neshod**			
	Nápravná a preventivní opatření			

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

Příklady typických úrovní implementace řízení bezpečnosti informací (ISM) v organizacích

Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky norem. Příklady rozsahu bezpečnostní dokumentace pro typické kvalitativní úrovně řízení bezpečnosti v organizacích, tak jak se s nimi nejčastěji setkáváme v praxi, jsou uvedeny v následující tabulce.

Poznámka: Rozsah bezpečnostní dokumentace, uvedený u příslušné úrovně zavedeného ISM, obsahuje zároveň i veškerou dokumentaci, popsanou u nižších úrovní řízení ISM.

	Typická úroveň řízení ISM	Stav implementace a provozu ISM (dle dosažené úrovně řízení)	Rozsah bezpečnostní dokumentace (dle dosažené úrovně řízení ISM)*
Kvalitativní úrovně implementace a provozu řízení bezpečnosti informací (ISM) v organizacích	**Re-certifikovaný ISMS** (bezpečnost informací je prokazatelně dlouhodobě řízena dle BS 7799-2:2002)	Organizace opakovaně provádí re-certifikaci provozovaného ISMS dle standardu BS 7799-2:2002. Aktualizuje stav opatření a dokumentace ISMS dle změn v podnikatelských cílech, prostředí a procesech organizace a dle aktualizovaných výsledků analýzy rizik .	Aktualizace rozsahu ISMS a výsledků analýzy rizik. Pravidelná revize Bezpečnostní politiky informací. Aktualizace návrhu opatření, prohlášení o aplikovatelnosti a implementačního plánu opatření a procesů ISMS. Pravidelná revize a aktualizace bezpečnostní dokumentace opatření a procesů ISMS.
	Certifikovaný ISMS (bezpečnost informací je prokazatelně zavedena a řízena dle BS 7799-2:2002)	Organizace se rozhodla certifikovat ISMS a realizovala kontrolní pre-certifikační audit, na základě jehož výsledků zavedla chybějící opatření a dopracovala procesy a dokumentaci dle požadavků BS 7799-2. Poté přistoupila k certifikaci ISMS.	Zpráva o výsledcích pre-certifikačního auditu ISMS. Plán řízení zdrojů ISMS. Kompletní provozní dokumentace opatření ISMS. Kompletní řídící a kontrolní dokumentace ISMS. Zpráva o certifikaci ISMS. Certifikát ISMS dle BS 7799-2:2002.
	Implementovaný ISMS v souladu s normou (bezpečnost informací je systematicky řízena a zlepšována, rizika jsou řízena a zvládána)	V organizaci je implementován a provozován ISMS v souladu s normou ISO/IEC 17799:2000. Rozsah ISMS, jeho řízení, procesy a odpovědnosti jsou definovány. Jsou identifikována a zvládána všechna rizika a zavedena opatření schválená k implementaci. Bezpečnostní dokumentace pokrývá všechny oblasti ISMS, nicméně nemusí být zcela dle požadavků certifikace (revize, aktualizace)	Působnost (rozsah) ISMS. Plán zvládání rizik . Prohlášeni o aplikovatelnosti opatření. Strategie BCP + DRP a IRH dokumenty a postupy. Základní provozní a řídící dokumentace opatření ISMS. Záznamy o provozu, využívání a zlepšování ISMS. Evidence bezpečnostních incidentů a následných reakcí a opatření. Výsledky auditu a evidence nalezených neshod, nápravných a preventivních opatření.
	Částečně implementovaný ISMS (koncepce bezpečnosti a plán zavedení ISMS je neúplná, nebo teprve postupně realizována)	Je přijata koncepce bezpečnosti managementem. Byla provedena analýza rizik a návrh opatření. Zavedena pouze vybraná opatření (priorita, zdroje). ISMS není řádně zdokumentován, nejsou realizovány veškeré řídící procesy (zejména kontrolní a nápravné) a řízeny zdroje ISMS. Není prováděn audit ISMS.	Zpráva o aktivech a dopadech. Zpráva o analýze rizik. Návrh opatření a implementační plán, případně Prohlášení o aplikovatelnosti opatření. Částečná provozní a řídící dokumentace procesů ISMS. Nekompletní záznamy o provozu , fungování řídících procesů ISMS a evidence bezpečnostních incidentů. Dílčí projekty/plány implementace prioritních opatření.
	Plánovaný ISMS (zavedení systému řízení bezpečnosti a zvládání rizik ve fázi přípravy a plánování)	Je přijata koncepce řízení bezpečnosti managementem na základě cíle zvládání rizik . Je vytvořen rámcový plán/projekt ISMS a případně delegován rozpočet na bezpečnost. Je vytvářeno bezpečnostní povědomí v organizaci.	Strategie bezpečnosti. Bezpečnostní politika informací. Program zvyšování bezpečnostního povědomí. Výsledky přehledové (případně detailní) analýzy rizik. Rámcový projekt bezpečnosti informací. Plán implementace ISMS a zvládání rizik.
	Ad-hoc ISM (řízení bezpečnosti informací bez znalosti a systematického zvládání bezpečnostních rizik)	Neexistuje systematická koncepce bezpečnosti, ISM „je řízena přes neznalost rizik“. Částečné bezpečnostní povědomí některých pracovníků. Zavedeny vybrané dílčí opatření a procesy ISM spolu s technickými opatřeními.	Neexistuje řízená systematická bezpečnostní dokumentace. Pouze dílčí interní dokumentace pokrývající určité oblasti nebo systémy. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.
	Nezavedený ISM (neprobíhá řízení bezpečnosti informací)	Neexistuje žádné bezpečnostní povědomí, řízení ani koncepce. Realizovány jsou pouze dílčí technické opatření, bez potřebných ISM procesů a dokumentace.	Interní bezpečnostní dokumentace v oblasti bezpečnosti informací neexistuje. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

3.díl Check - Kontroluj

Žádný proces, opatření nebo činnost sledující cíl a plnící určitou funkci v systému není možné udržet, řídit a zlepšovat v čase, pokud se neprovádí periodická kontrola jejich funkčnosti, efektivity a souladu s požadovaným stavem. Nejinak je tomu i v procesu zavádění a provozování systému řízení bezpečnosti informací (ISMS) dle normy ISO/IEC 27001:2005. Jak efektivně provádět kontrolu ISMS v prostředí malých a středních organizací popisuje tento 3.díl seriálu.

Kontrola ISMS

Jak již bylo uvedeno v předchozích dílech tohoto seriálu, ISMS (Information Security Management System) slouží k vybudování, provozování, sledování, řízení a zlepšování bezpečnosti informací v organizacích. Jedná se o systematický a konzistentní proces v čase, který je realizován dle periodického procesního modelu PDCA (Plan-Do-Check-Act). Hlavní kroky a opatření v etapách Plánuj (Plan) a Dělej (Do) byly předmětem 1. a 2. dílu seriálu. Tento 3. díl se zabývá náplní etapy Kontroluj (Check), která slouží jako **zpětná vazba**, podávající vedení organizace i dalším odpovědným osobám informace o tom do jaké míry byly naplněny zásady a cíle bezpečnostní politiky informací, zda byla zavedena všechna bezpečnostní opatření uvedená v Prohlášení o aplikovatelnosti opatření a zda fungují dostatečně spolehlivě a efektivně.

Ono nechvalně známé rčení „důvěřuj ale prověřuj" je v oblasti bezpečnosti informací nanejvýš namístě a s trochou nadsázky lze dodat, že pokud „Opakování je matkou moudrosti", pak „Prověřování je otcem bezpečnosti" a jejich společným potomkem je právě tato etapa „Kontroluj".

Protože během budování ISMS jsou v organizaci zaváděna jednak funkční bezpečnostní opatření, zvolená z ISO 17799dle výsledků analýzy rizik a dále opatření (proces) pro jejich řízení a zlepšování v čase dle ISO 27001, je třeba se při kontrole ISMS zaměřit na obě tyto skupiny opatření. K tomu slouží řada technik a postupů, jejichž popis s přihlédnutím k prostředí malých a středních firem je obsahem tohoto článku. Na konci tohoto dílu je uveden seznam procesů, obsahující hlavní kroky ISMS s detailem na etapu Kontroluj (Check) procesu PDCA.

Monitoring provozu

Monitoring provozu klíčových prvků IS a ochranných opatření je základním zdrojem informací pro kontrolu jejich funkčnosti a spolehlivosti. Pokud organizace zavádějící ISMS plánuje v budoucnu i jeho certifikaci, musí **vytvářet a shromažďovat záznamy** o fungování alespoň těch opatření, která jsou uvedena v Prohlášení o aplikovatelnosti (ty budou předmětem auditu). Bohužel ne všechny typy opatření samy automaticky generují záznamy o činnosti a tak je nezbytné přistoupit i v prostředí malých a středních firem k nepopulárnímu **ručnímu generování záznamů** u takových opatření, která tuto vlastnost nemají (především organizační a administrativní). Nemusí se přitom zdaleka jednat o únavnou administrativu, protože rozsah a složitost opatření, zvláště u malých a středních firem, nebývá nijak velký. Příkladem toho, co postačí pro audit funkčnosti opatření „bezpečnostní školení uživatelů IS" (viz. předcházející díl seriálu), jsou seznamy účastníků školení a datum a předmět školení. Zodpovědná a systematická asistentka si je stejně pořídí a pokud tak učiní do připravené tabulky, kterou bude dle potřeby aktualizovat a iniciativně nesmaže, je povinnost vůči auditu ISMS splněna. Pochopitelně pouze za jedno opatření - školení pracovníků, nicméně časová náročnost se pohybuje v rámci jednotek minut.

Pro monitoring ICT postačí u malých organizacích výchozí nastavení logování dle standardní instalace většiny produktů a jejich ruční **namátková kontrola** pracovníkem, pověřeným na půl úvazku základními bezpečnostními povinnostmi. U středních organizací, je již vzhledem ke komplikovanosti IS infrastruktury nedostatečné spolehnout se pouze na namátkové ruční kontroly log souborů a je třeba využít **automatických nástrojů** pro jejich filtrování a vyhodnocování nestandardních událostí např. pomocí skriptů nebo dodatečných produktů. Podrobnější bezpečnostní monitoring se vyplatí aktivovat pouze krátkodobě, při podezření na výskyt bezpečnostního incidentu (což při pozdní reakci může skončit příslovím „s křížkem po funuse").

Testování funkčnosti opatření

Abychom při provozu IS pomyslnému funusu předešli, je třeba uvedené pasivní metody kontroly doplnit i o aktivní a preventivní způsoby, jakými jsou např. aplikační kontroly chyb výpočtů a zpracování dat nebo testování zranitelností, případně penetrační testování systémů. Zatímco komplikovanější a časově i finančně náročnější penetračního testování má za cíl simulaci reálných útoků ze zvoleného prostředí a identifikaci možných negativních dopadů na IS, bezesporu jednodušším, rychlejším a levnějším způsobem testování odolnosti vůči útokům je vyhledání a testování zranitelností provozovaných ICT produktů.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

3.díl Check - Kontroluj

Oba způsoby mohou být prováděny z interní sítě, nebo častěji z externího prostředí – zpravidla Internetu nebo bezdrátových sítí, což by měly být v případě malých a středních firem hlavní oblasti prevence proti útokům na IS. Protože se v případě penetračního testování jedná o vysoce specializovanou činnost, vyžadující detailní znalosti o technikách a nástrojích hackingu, stejně jako o bezpečnostních slabinách jednotlivých ICT produktů a komunikačních protokolů, bývá tento úkol svěřován specializovaným externím firmám, které mají dostatečné profesní zázemí pro jejich kvalifikovanou realizaci. Naproti tomu testování zranitelností je proces, který si mnohdy mohou počítačově gramotní uživatelé udělat sami, pomocí dostupných programů nebo využít **specializovaných webových služeb** (např. QualysGuard®).

Pro malé organizace lze testování zranitelností doporučit, pokud využívají permanentní připojení k externím sítím nebo provozují bezdrátovou LAN v husté zástavbě. V případě vybalení a zapojení „chytrého" VLAN přístupového bodu se Vám totiž může stát, že až se po několika minutách budete chtít k tomuto zařízení připojit na administrátorskou konzolí, bude Vám hlásit že administrátorské připojení již využívá jiný počítač a Váš to rozhodně nebude! Pro střední organizace by **testování zranitelností klíčových serverů a služeb IS mělo být samozřejmostí**, alespoň po implementaci bezpečnostních opatření a před rutinním provozem komunikačních spojů. Pokud střední organizace provozují citlivá data a aplikace na Internetu, mohou zvážit realizaci penetračního testování nebo podrobný technický bezpečnostní audit konfigurace klíčových prvků IS a bezpečnostních opatření jako např. Firewallu, DNS nebo Internetového aplikačního nebo databázového serveru či routeru na rozhraní LAN/WAN.

Audit a kontrola bezpečnostních opatření

Spolu s monitorováním provozu, testováním zranitelností a technicky zaměřeným auditem konfigurace ICT, je další metodou kontroly implementace a provozu IS / ISMS realizace Auditu a kontrol bezpečnosti IS. Obecně lze říci, že audit opatření musí být prováděn v každém typu a velikosti organizace, která provozuje systém řízení nad opatřeními, jinak by neexistovala zpětná vazba o stavu reality vůči plánu a návrhu požadovaného cílového stavu. Každý typ auditu by se měl řídit pravidly ISO 19011:2002 a měl by probíhat dle schváleného ročního i operativního plánu.Je zřejmé, že takovéto formální „harakiri" malé a střední organizace dobrovolně nepodstoupí a že přichází v úvahu pouze v případě potřeby certifikace systému řízení.

V případě ISMS by měl audit zahrnovat kontrolu funkčních bezpečnostních i řídících opatření ISMS, která jsou deklarována v Prohlášení o aplikovatelnosti a popsána v bezpečnostní dokumentaci. Audit by měl ověřit jak jsou realizována v praxi.

U malých organizací není třeba vytvářet samostatná oddělení nebo pracovní funkce **interního auditora**, ale je nutné i v malé organizaci funkci interního auditora dedikovat, alespoň jako přidruženou pracovní náplň nějakému zaměstnanci. Jednou ročně je nezbytné projednání zjištěných výsledků plánovaných auditů i namátkových kontrol s majitelem / ředitelem organizace a následně se všemi zaměstnanci.

V případě středně velké organizace se již doporučuje zvážit existenci samostatné funkce interního auditora, kterému připadne i funkce **bezpečnostního auditora**. I v tomto případě má za úkol provádění plánovaných i namátkových kontrol dle ročního i operativního plánu auditu, který je sestavován s přihlédnutím k největším rizikům a nálezům předchozích auditů. Pro dosažení vyšší odborné úrovně a komplexnosti výsledků kontroly je doporučeno realizovat alespoň jednou ročně přehledový srovnávací audit stavu ISMS, vzhledem k požadavkům ISO 27001, s účastí jednoho externího odborného konzultanta.

Revize adekvátnosti a efektivnosti ISMS

Kromě ověření funkčnosti, spolehlivosti a úplnosti funkčních i řídících opatření je třeba přibližně jednou ročně zrevidovat rozsah, adekvátnost a efektivnost celého ISMS ve vztahu k potřebám, cílům a prostředí organizace. Výsledek této celkové revize ISMS by měl být stejně jako souhrnné výsledky auditů opatření **projednán s vedením organizace** a pořízeny záznamy o přijatých závěrech.

Jelikož se jedná o činnost vyžadující široký přehled a značné zkušenosti z oblasti bezpečnosti informací a implementace ISMS v organizacích, musejí se malé i střední organizace spolehnout na pomoc externích specialistů, stejně jako v případě analýzy informačních rizik v etapě Plánuj.

Závěr 3.dílu

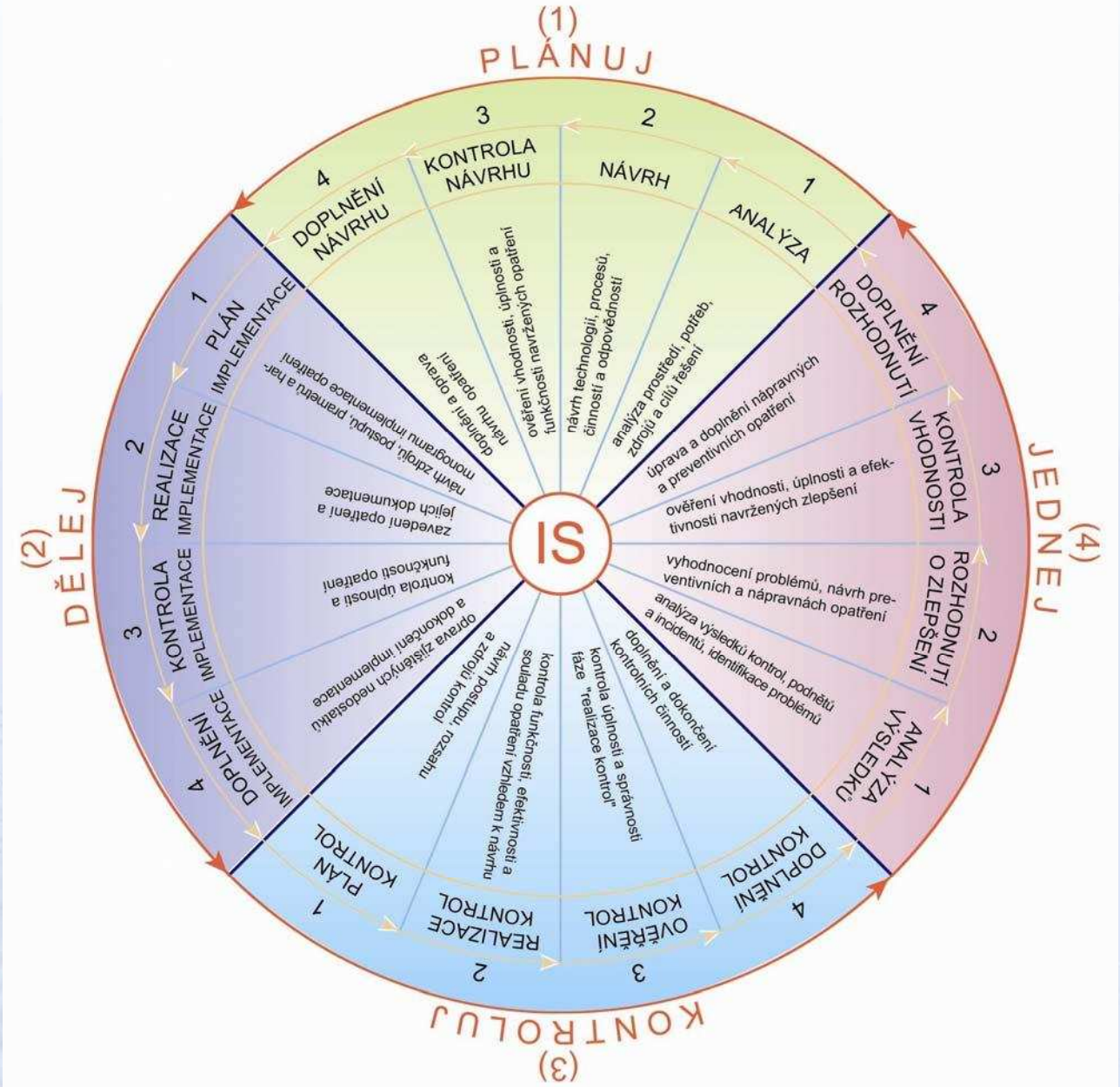
Dlouhodobé zajištění bezpečnosti informací, stejně jako udržení a zlepšování kvality produktů a služeb či stavu životního prostředí, je kontinuální a konzistentní proces v čase, pro jehož systematické řízení byl zaveden normami řízení (ISO 27001, ISO 9001, ISO 14001) shodný periodický procesní model PDCA. Ten je možné aplikovat na celkový proces řízení stejně jako na každé opatření a činnosti, které jsou v rámci systému řízení zavedeny a prováděny.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

3.díl Check - Kontroluj



PDCA není přísně lineární proces, ale nekonečný proud navzájem vnořených PDCA smyček na různých úrovních detailu pohledu, které jsou realizovány v rámci jednotlivých činností a opatření každé etapy PDCA.

Nejlépe je to vidět na příkladu etapy Kontroluj (Check) celého procesu řízení bezpečnosti informací, která je realizována i v průběhu etap plánování (testování vhodnosti opatření při jejich výběru), zavádění opatření do provozu a jejich využívání (kontrola funkčnosti a nastavení), v průběhu kontroly ISMS (audit souladu s interní/externí dokumentací) a v průběhu zlepšování (výběr a testování nápravných a preventivních opatření).

Právě poslední etapa Jednej (Act) představuje ve své podstatě pouze rozhodovací krok, který spouští další paralelní obrátky PDCA procesů využívání a zlepšování ISMS. O této etapě a o významu certifikace ISMS pro malé a střední firmy pojednává následující díl tohoto seriálu.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

3.díl Check - Kontroluj

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	Plán / projekt bezpečnosti			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
DO	Způsob implementace opatření			
	Metody prosazení bezpečnosti			
	Bezpečnostní dokumentace			
	Program zvyšování bezpečnostního povědomí			
	Způsob zvládání rizik za provozu			
	Nároky na provoz opatření a zajištění bezpečnosti			
	Zavedení opatření DRP a IRH Havarijní plány)			
CHECK	Monitoring IS a testování funkčnosti opatření	Namátkový monitoring provozu IS a vyhodnocování logů a záznamů událostí (v papírové i el. podobě). Otestování zranitelností u systémů připojených k Internetu.	Pravidelný monitoring a vyhodnocování logů a záznamů událostí (v papírové i elektronické podobě). Otestování zranitelností u systémů připojeným k externím subjektům (třetím stranám).	Centralizovaný a automatizovaný monitoring provozu ICT a vyhodnocování logů a záznamů událostí. Pravidelné testování zranitelností doplněné o penetrační testování (simulaci „hacker" útoků). Bezpečnostní analýza klíčových prvků systému.
	Audit a kontrola bezpečnostních opatření	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Iniciuje ředitel, provádí vybraný pracovník jako rozšíření standardní pracovní náplně. Namátková interní kontrola stavu opatření.	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Bezpečnostní technický audit nastavení klíčových ICT systémů. Namátková interní kontrola stavu opatření.	Pravidelná interní kontrola a audit bezpečnostních a ISMS opatření, dle interních směrnic a politik (vyhrazený interní auditor). Průběžný bezpečnostní technický audit konfigurace ICT a bezpečnostních záplat.
	Revize adekvátnosti a efektivnosti ISMS	Rámcová revize procesu ISMS a vyhodnocení aktuálnosti, efektivnosti a adekvátnosti opatření. 1 denní workshop s využitím externího konzultanta.	Roční podrobná revize procesu ISMS a stavu opatření s využitím externího konzultanta. Porovnávání stávajících opatření s novými trendy a vývojem hrozeb a zranitelností.	Srovnávací audit stavu ISMS s normou. Průběžné přehodnocování míry zbytkových a akceptovaných rizik vůči cílům organizace. Revize podnětů na zlepšení efektivnosti.
ACT	Vyhodnocení fáze CHECK, identifikace a analýza neshod			
	Nápravná a preventivní opatření			
ISMS	Doporučení zavést ISMS	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

Je bezpečnost informací problematikou spíše technologickou nebo manažerskou? Jak zajistit její dlouhodobou stabilitu a konzistentnost v čase, navzdory měnícím se vnitřním i vnějším podmínkám a prostředí organizace? Co je hlavním motorem procesu zavádění, údržby a zlepšování bezpečnosti informací, kde začíná a kde vlastně končí? Lze bezpečnost informací měřit a má smysl její certifikace? O těchto otázkách pojednává závěrečný 4.díl seriálu ISMS v malých a středních firmách.

Zlepšování ISMS

V předchozích částech byly popsány nejobsáhlejší a zdánlivě i nejdůležitější kroky procesu zavádění a využívání systému řízení bezpečnosti informací (ISMS) podle procesního diagramu PDCA normy ISO/IEC 27001:2005. V každém z dílů byly postupně nastíněny hlavní činnosti jednotlivých fází: Plánuj (PLAN), Dělej (DO) a Kontroluj (CHECK), s přihlédnutím na specifické prostředí malých a středních firem. Logickou náplní tohoto závěrečného dílu je tedy popis poslední (nikoliv však významem) čtvrté fáze Jednej (ACT), představující nejdůležitější rozhodovací krok celého procesu. Součástí tohoto dílu je i celkové zhodnocení významu ISMS a jeho certifikace pro prostředí malých a středních firem. Přehled všech hlavních kroků ISMS procesu s detailem na fázi Jednej (ACT) je uveden, jako v každém díle, na konci v tabulce.

V úvodu jsem pro první tři fáze PDCA procesu záměrně použil spojení „zdánlivě nejdůležitější“ což nyní uvedu na pravou míru: Aby bylo možné ve fázi Dělej (DO) implementovat a provozovat IS, aplikaci, bezpečnostní opatření nebo systém řízení, je vhodné realizovat nejdříve analýzu prostředí a potřeb a následně vybrat řešení a naplánovat jeho implementaci, neboli zrealizovat fázi Plánuj (PLAN). Pokud záleží na funkčnosti a spolehlivosti objektu, který byl ve fázi Dělej (DO) implementován a je provozován a všichni pořád dokola „otravují s tou bezpečností“, je nanejvýš vhodné realizovat kontrolu úplnosti a správnosti implementace zvoleného řešení (naplánovaného ve fázi Plánuj) a ověřit také splnění požadovaných parametrů. Jinými slovy realizovat fázi Kontroluj (CHECK). Tím jsou nastíněny hlavní principy závislostí prvních třech fází, ale bez přidání klíčové čtvrté fáze by se stal cyklus PDCA pouze jednorázovým procesem, díky němuž by se zabezpečení informací stalo statickou a velmi rychle zastaralou událostí v historii.

Klíčovým významem 4. fáze Jednej (ACT) je tedy **vyhodnotit výsledky auditu a kontrol funkčnosti** bezpečnostních opatření i ISMS procesu samotného a nastartovat další cyklus PDCA, ve kterém budou naplánovány, zavedeny, zkontrolovány a opět vyhodnoceny nápravná a preventivní opatření k zajištění požadovaného a konzistentního stavu bezpečnosti v čase.

Provedení každé fáze PDCA cyklu je vhodné také naplánovat, zrealizovat, poté zkontrolovat a doplnit. Proto v sobě obsahují další vnořené PDCA cykly, které se samostatně roztáčejí pro realizaci každého kroku, které byly pro danou fázi popsány v tomto seriálu. Princip vnořených PDCA fází uvnitř základního PDCA procesu ISMS znázorňuje obrázek na předchozí straně.

Popisem hlavních činností nejdůležitější rozhodovací fáze Jednej (ACT) procesu ISMS v prostředí malých a středních firem se zabývají následující kapitoly.

Vyhodnocení fáze Kontroluj

Základním předpokladem pro správné rozhodnutí „co a jak dál“ by vždy měly být co nejpřesnější a nejúplnější informace o aktuálním stavu a cílech organizace. Informace o aktuálním stavu týkající se monitoringu provozu, evidence chyb a bezpečnostních incidentů, výsledků testování funkčnosti a spolehlivosti implementovaných opatření, výsledků testování zranitelností a výsledky interních i externích auditů poskytuje předcházející fáze Kontroluj (CHECK). **Vyhodnocení** těchto informací **provádí v malých firmách pracovník pověřený činností bezpečnostního managera** na částečný úvazek, jako přidruženou činnost ke své pracovní náplni. Výsledky svého šetření by měl minimálně jednou ročně předložit majiteli, případně řediteli organizace a společně provést jejich analýzu a vyhodnocení.

U středních a velkých organizací se již vyplatí přidat do tohoto kroku také revizi návrhů a možných zlepšení bezpečnosti informací i procesu ISMS, jejichž evidenci zajišťuje **fórum pro bezpečnost** informací, složené ze zástupců uživatelů, dodavatelů a odborných rolí delegovaných pro oblast bezpečnosti informací v organizaci. V rámci procesu řízení rizik je prováděno také pravidelné přehodnocování úrovně zbytkových a přenesených rizik, s ohledem na změny v organizaci, technologiích, podnikatelských cílech a vnějších událostech a hrozbách.

Identifikace a analýza neshod

I když byla revize výsledků auditu zahrnuta již do předcházejícího kroku, je vhodné tuto činnost popsat podrobněji. Identifikace a analýza neshod má za úkol rozebrat výsledky interního i případného externího

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

auditu a posoudit, které z nalezených neshod jsou skutečné, které pouze potenciální a vyřadit nesprávně identifikované neshody. Toto rozhodnutí je opět vhodné zaevidovat formou tabulky. Nakonec je pro odstranění skutečně identifikovaných neshod třeba navrhnout nápravná opatření a pro zabránění opakovaného výskytu skutečných i potencionálních neshod v budoucnu je třeba navrhnout preventivní opatření. Jejich výběr, implementace a ověření funkčnosti je již náplní dalších paralelních PDCA procesů (koleček), které jsou spuštěny pro každé nově navržené opatření.

U malých organizací provede tuto **analýzu neshod** majitel, případně ředitel organizace, ve spolupráci s pracovníkem pověřeným funkcí bezpečnostního managera. S výsledným rozhodnutím je vhodné seznámit všechny zaměstnance. Implementace těchto rozhodnutí bývá velmi rychlá a flexibilní. Pokud malá firma usiluje o certifikaci ISMS, je vhodné obrátit se pro pomoc na externího konzultanta, případně zrealizovat **srovnávací audit procesu ISMS vzhledem k ISO 27001** externí specializovanou firmou a s její pomocí navrhnout potřebná nápravná opatření pro dosažení souladu.

U středních firem bude interpretace výsledků auditů i návrh nápravných a preventivních opatření komplikovanější a formální proces, řízený pracovníky interního auditu ve spolupráci s dalšími zainteresovanými odbornými pracovníky organizace. Při přípravě na certifikaci ISMS se i zde doporučuje sáhnou pro pomoc externích odborníků, pokud takoví nejsou ve vlastních řadách.

Nápravná a preventivní opatření

Nápravná opatření slouží k odstranění skutečně nalezených nedostatků a chyb, spojených s implementací a provozem ISMS a k zabránění jejich dalšímu trvání (opakování). Jedná se například o neúplnou implementaci opatření zvolených v Prohlášení o aplikovatelnosti opatření, o chybějící dokumentaci těchto opatření, o nedostatečné proškolení pracovníků zainteresovaných v procesu ISMS apod.

Preventivní opatření jsou vybírána s cílem **zabránit výskytu potencionálních neshod** v budoucnu, tedy za účelem eliminace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody může být například nedodržení oddělení rolí u některých činností a opatření ISMS nebo nedůsledné provádění potřebných monitorovacích a kontrolních činností.

Pro malé organizace je typická rychlá praktická změna bez byrokratických průtahů a příklon především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější.

Pro střední organizace, stejně jako ve fázi Dělej (popis nároků na provoz opatření), není již hledisko nákladů na pořízení a zavedení opatření tak palčivé jako pro malé organizace a bude při jejich výběru více rozhodovat jeho účinnost a pokrytí nalezených nedostatků.

Zavést ISMS?

Uvedeným přehledem byly popsány všechny hlavní kroky tvořící pilíře procesu ISMS, tak jak jsou definovány normou ISO 27001, která se v roce 2006 stane také součástí soustavy norem ČSN.

Existuje jednoznačná odpověď na otázku zda zavádět ISMS proces v prostředí malých a středních firem? Pokud existence, poslání nebo strategické cíle těchto firem závisejí na zajištění některého z „parametrů“ bezpečnosti informací – tj. na dostupnosti, důvěrnosti nebo integritě informací a dat, je odpověď **jednoznačně ANO**. Zavedení systému řícení samo o sobě nezaručuje kvalitativní nárůst některého z parametrů bezpečnosti informací, ale představuje odzkoušený a celosvětově uznávaný postup, jak dosáhnout bezpečnosti informací adekvátní požadavkům a cílům organizace a jak jí udržovat a efektivně zlepšovat v čase, za pomocí ochranných opatření, odpovědností, činností a řídících a kontrolních procesů. Vzhledem ke své formalizaci tak poskytuje zdokumentovanou inventuru činností a odpovědností, které se ve velké míře stejně v organizacích provádějí, většinou ale nesystematicky a nedůsledně, což v praxi způsobuje vážná rizika a bezpečnostní incidenty.

Certifikovat ISMS?

Odpověď zda certifikovat ISMS prozatím tak jednoznačná není. Zavedení ISMS má prokazatelně pozitivní efekt. Vzhledem k narůstající závislosti firem na informačních systémech, jejich propojování a sdílení informací v rámci B2B a B2C aplikací a vzhledem k požadavkům platné národní a nadnárodní legislativy na zabezpečení informací a dat je správně zavedený a provozovaný ISMS chápán jako vysoký stupeň záruky adekvátní ochrany dat. Zvyšující se počty projektů implementace ISMS i v České republice jsou toho důkazem.

Lze ale míru (stupeň) zabezpečení informací v IS organizace objektivně měřit? Celková bezpečnost informací v organizacích je zajišťována kombinací technologických opatření, fyzických, personálních a administrativních, které by měly být implementovány

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

v rozsahu a kvalitě odpovídající prostředí a potřebám každé jednotlivé organizace. Jednou z možností jak hodnotit míru bezpečnosti informací je posouzení kvality procesu řízení bezpečnosti informací ISMS, vyhodnocením míry souladu s požadavky na tento proces dle normy ISO 27001.

Pro malé a střední firmy představuje proces přípravy a samotné certifikace akreditovanou certifikační autoritou nemalou investici, kterou je třeba manažersky a ekonomicky zvážit. Pokud firma podniká v sektoru, kde je důvěryhodnost vysoce ceněným faktorem a podmínkou úspěšných obchodních vztahů, může být pro takovou firmu užitečné realizovat certifikaci bezpečnosti informací **jako další důkaz kvality řízení** k certifikátu QMS nebo EMS (dle ISO 9001:2000 a ISO 14001:1996). Certifikace ISMS do prostředí firem, kde je již certifikován jiný systém řízení, je méně náročnou variantou. Vzhledem k harmonizovanému PDCA modelu ISMS, QMS a EMS je řada procesů a odpovědností již nastavena.

Ve světě existují již téměř dva tisíce (stav k 11/2005) certifikátů ISMS dle normy BS 7799:2000, která je předchůdcem ISO/IEC 27001:2005. Podle ISMS International User Group – Certificate Register (*http://www.xisec.com*) bylo nejvíce certifikátů bylo dosud uděleno ve Velké Británii a Japonsku. V České Republice má v rámci integrovaného systému řízení certifikovaný ISMS zatím pouze společnost Eurotel (více informací viz. Aktuality DSM 5/2004). Stojí za zmínku, že zkušenosti získané v rámci implementace ISMS a přípravy této organizace na certifikaci přispěly ke vzniku tohoto seriálu. Vlna certifikací ISMS je teprve před námi a jeví se velice pravděpodobné, že se prosadí ve stejné míře jako dnes certifikace QMS a EMS.

Závěr

Touto prognózou končí seriál ISMS v malých a středních firmách, který si kladl za cíl prakticky popsat hlavní kroky procesu implementace a využívání ISMS, s přihlédnutím k podmínkám malých a středních firem. Při jeho tvorbě jsme se setkali s kritickými i pozitivními ohlasy na ISMS. Ty kritické zpochybňovaly aplikovatelnost a efektivnost principů ISMS pro prostředí těchto firem a zatracovaly ISMS jako zbytečnou byrokracii. Naopak pozitivní, kterých bylo mnohem více, zdůrazňovaly **univerzálnost PDCA modelu řízení a jeho využitelnost pro bezpečnost informací nejen malých a středních firem**.

Je třeba přiznat, že zavedení a provoz ISMS přináší zaměstnancům i vedení firem nárůst režijních kapacit. To ale zejména proto, že donutí odpovědné osoby vykonávat činnosti, které bývají v běžné praxi opomíjeny a nebo v horších případech nejsou vůbec delegovány.

Zbývá odpovědět na první otázku z perexu tohoto dílu: Bezpečnost informací v organizacích JE problematikou technologickou stejně jako manažerskou. Jedna část nemůže účinně a efektivně fungovat bez druhé. Správná konfigurace ICT produktů a bezpečnostních opatření poskytuje většinou dobrou úroveň ochrany informací. Bez zajištění ISMS řídícího procesu jsou však časem znehodnoceny na úroveň zapomenuté zrezlé závory s utrženou cedulí „Zákaz vstupu“, kolem které vede vyšlapaná stezka do zakázaného prostoru. Známe to přeci z praxe všichni.

Využité zdroje a další informace:

- www.ISO27000.cz
- ISO/IEC 17799:2005 IT - Security techniques - Code of practice for information security management
- ISO/IEC 27001:2005 IT - Security techniques - Information security management systems - Requirements
- BS 7799-2:2002 ISMS - Specification with guidance for use
- ISO 9001:2000 QMS – Requirements
- ISO 14001:1996 EMS - Specification with guidance for use
- ISO 19011:2002 - Guidance for management systems auditing
- PD 3002:2002 Guide to BS 7799 Risk Assessment
- PD 3004:2002 Guide to the implementation and auditing of BS 7799 controls
- PD 3005:2002 Guide on the selection of BS 7799 controls
- ISMS International User Group – Certificate Register (*http://www.xisec.com*)

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	Plán / projekt bezpečnosti			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
DO	Způsob implementace opatření			
	Metody prosazení bezpečnosti			
	Bezpečnostní dokumentace			
	Program zvyšování bezpečnostního povědomí			
	Způsob zvládání rizik za provozu			
	Nároky na provoz opatření a zajištění bezpečnosti			
	Zavedení opatření DRP a IRH Havarijní plány)			
CHECK	Monitoring IS a testování funkčnosti opatření			
	Kontrola a audit bezpečnostních opatření			
	Revize adekvátnosti a efektivnosti ISMS			
ACT	Vyhodnocení fáze Kontroluj	Revize zejména bezpečnostních incidentů, chyb a průběhu jejich řešení (dle potřeby). Revize penetračního a zkušebního testování, pokud bylo realizováno. Revize výsledků ročního auditu.	Pravidelná revize incidentů, chyb a průběhu jejich řešení. Revize penetračních a dalších typů testů. Revize výsledků auditu. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.	Proces průběžné revize výsledků monitoringu provozu, IDS systémů, incidentů, chyb a průběhu jejich řešení. Revize penetračních testů a technických auditů konfigurace systémů. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.
	Identifikace a analýza neshod	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace a okamžitý návrh opatření ředitelem / majitelem.	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace výsledků kontrol interním auditem s využitím externích odborníků. Jednoduchý projekt pro návrh opatření.	Identifikace a řízená evidence možností zlepšování, neshod a potenciálních problémů. Vícestupňový proces analýzy neshod bezp. auditem a jejich interpretace bezp ředitelem. Kompletní projekt pro návrh a testování opatření
	Nápravná a preventivní opatření	Přednostní výběr jednoduchých organizačních a personálních opatření, bez nutnosti investic. Rychlé zavedení dostupných opatření do praxe.	Výběr organizačních opatření podpořených technologiemi a nástroji. Testování opatření před uvedením do praxe. Aktualizace bezpečnostní dokumentace.	Výběr a implementace opatření formou projektu Primárně výběr robustních a automatizovaných opatření s podrobným testování a sledováním účinnosti a přizpůsobení organizaci. Řízená aktualizace bezpečnostní dokumentace.
ISMS	Doporučení zavést ISMS	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

Management Summary

Plánuj

Způsob zavádění ISMS ve smyslu ISO/IEC 17799:2005 a ISO/IEC 27001:2005 je rozdílný pro organizace s ohledem na jejich velikost. První se čtyř dílů článku popisuje rozdíly v procesu plánování ISMS v malých a středních firmách. Zaměřuje se na strategii bezpečnosti, bezpečnostní politiku, organizační strukturu bezpečnosti, způsoby provádění analýzy rizik a výběr vhodných protiopatření. Další díly popisují zbývající činnosti zavádění a využívání ISMS podle modelu PDCA.

Dělej

Základní opatření ISMS a činnosti při jeho zavádění a využívání v malých a středních organizacích jsou rámcově shodné jako v prostředí velkých organizací. Liší se však ve způsobu, rozsahu a hloubce jejich aplikování, přizpůsobeným na míru konkrétním organizacím. Tento článek popisuje příklady náplní hlavních činností kroku Dělej (Do) a jejich specifika v prostředí malých a středních firem.

Kontroluj

Pro kvalifikované řízení každé činnosti nebo procesu v čase je třeba periodicky získávat informace o její funkčnosti, spolehlivosti a efektivnosti. Pokud jsou stanoveny cíle a deklarovány opatření k jejich naplnění, je možné kontrolovat i míru dosažení shody s požadovaným stavem. Etapa Kontroluj (Check) využívá všech těchto kontrolních kroků a opatření k dosažení konzistentní bezpečnosti informací, deklarované v bezpečnostní dokumentaci.

Jednej

Závěrečný díl seriálu ISMS popisuje hlavní kroky fáze „Jednej" (ACT), která představuje rozhodovací krok ke zlepšování úrovně bezpečnosti informací na základě vyhodnocení výsledků kontrolních činností a návrhu nápravných a preventivních opatření. V závěru článku jsou zhodnoceny přínosy zavedení a certifikace ISMS pro sektor M&S firem.

Plan

The method of ISMS implementation as described in IEC 17799:2005 and ISO/IEC 27001:2005 is different for organizations of various sizes. This is the first part of a series of four articles and describes differences in the ISMS planning process in small and medium enterprises. It focuses on security strategy, policy, security infrastructure, risk analysis methods and selection of appropriate countermeasures. The next articles in the series will deal with the remaining activities related to implementation and use of ISMS according to the PDCA model.

Do

The main controls and processes for ISMS implementation and operation are basically the same for small and medium enterprises as for large enterprises. The main difference is in the method, range and depth of their application, which are adapted to the requirements of the individual organization. This article describes examples of the "Do" stage controls and processes, adapted for small and medium enterprise areas.

Check

Periodic information about functionality, reliability and efficiency is necessary for the proper management of any activity or process. Compliance with a desired status can be checked only if the objectives are declared and the measures to achieve the objectives are defined. The "Check" stage uses all these controls to attain consistent information security described in the security documentation.

Act

Last in the series of articles describing the main activities is the "Act" stage that represents a decision-making step towards improving the information security level based on the evaluation of control activity results and suggested corrective and preventive measures. The article concludes with an evaluation of the benefits of implementation and certification of ISMS for small and medium enterprises.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

PŘÍLOHA P III: UŽIVATELSKÝ MANUTÁL APLIKACE RANIT

Uživatelský manuál

Aplikace RANIT

10. září 2009

Předkládá: Pro IT, a. s.

ID Dokumentu	Uzivatelsky_manual_RANIT	**Verze**	
Zodpovídá	Jakub Chovanec	**Stav**	Definitivní
Stupeň utajení	Pro interní použití	**Určeno pro**	Interní
Počet výtisků	-	**Výtisk číslo**	-

Obsah

1. Základní popis

RANIT je softwarová aplikace vytvořená pro podporu provádění rizikových analýz především v oblasti bezpečnosti informací založených na metodice RANIT. Specifikace metodiky RANIT je předmětem dokumentu „Metodika RANIT“). RANIT slouží jako pomůcka pro ukládání a vyhodnocování údajů získaných pohovory s vlastníky procesů, aktiv a komponent. Program umožňuje spravovat data pro větší množství projektů analýzy rizik.

Program RANIT je vícejazyčný, v současnosti je možno zvolit český nebo anglický jazyk. Další jazykové verze lze na zakázku vytvořit.

Tento manuál popisuje a vysvětluje základy práce s aplikací RANIT.

Pro technické informace o běhovém prostředí a instalaci aplikace nahlédněte do dokumentu Administrátorská dokumentace.

2. Projekty a jejich správa

Při práci v aplikaci RANIT je ústředím termínem projekt, který zpracovává pohled na námi modelovaný systém. Pro produkt MALÉ ORGANIZACE nelze vytvářet projekty. Otvírá se automaticky předvolený prázdný projekt.

2.1. Licence

Produkt RANIT MALÉ ORGANIZACE je možno zakoupit jen s jednou licencí a proto není potřeba provádět změny uživatelů.

Obrazovku pro zadání licence najdeme: Info -> Licence

Zobrazí se kontaktní informace a box pro zadání licenčního klíče, který byl dodán s programem.

V případě, že nebyl kód zadán, anebo nebyl přijat, poběží po dobu 30 dní Demo programu. Toto demo je plně funkční a představuje produkt RANIT EXPERT. Nedostupnou položkou jsou exporty a vyhodnocení

Pro aktivaci aplikace je třeba přístup k internetu.

3. Základní popis modelování

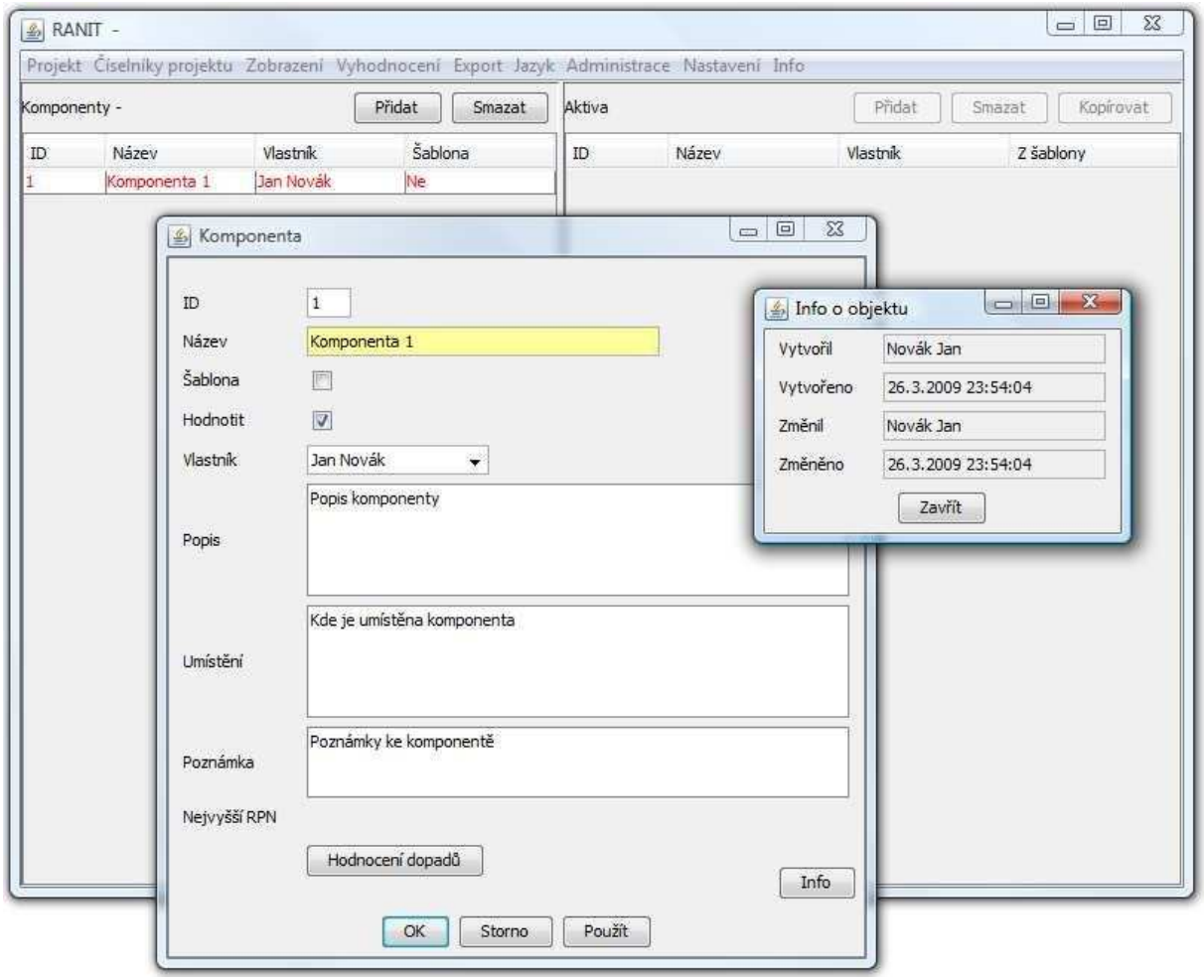
Modelování procesu nebo jiné reality (v našem případě systému IS/IT), např. toku informace v procesu, je postup, kterým převádíme vlastnosti takového reálného objektu na formální (virtuální) popis. Takovéto modely poté poskytují různé pohledy na systém a vytváří se na různých úrovních abstrakce.

3.1. Model systému

3.1.1. Komponenty

Prostředí informačních a komunikačních technologií a informačních systémů (dále též jen informační systém, nebo zkráceně IS) je na základě stanovení hranic revize pro účely analýzy rizik rozděleno na komponenty. Komponenty jsou zobrazeny v levé polovině hlavního okna.

Komponenty vytváříme prostřednictvím tlačítka „Přidat“.



Obrázek č. 4 – Vytvoření komponenty a informace o objektu

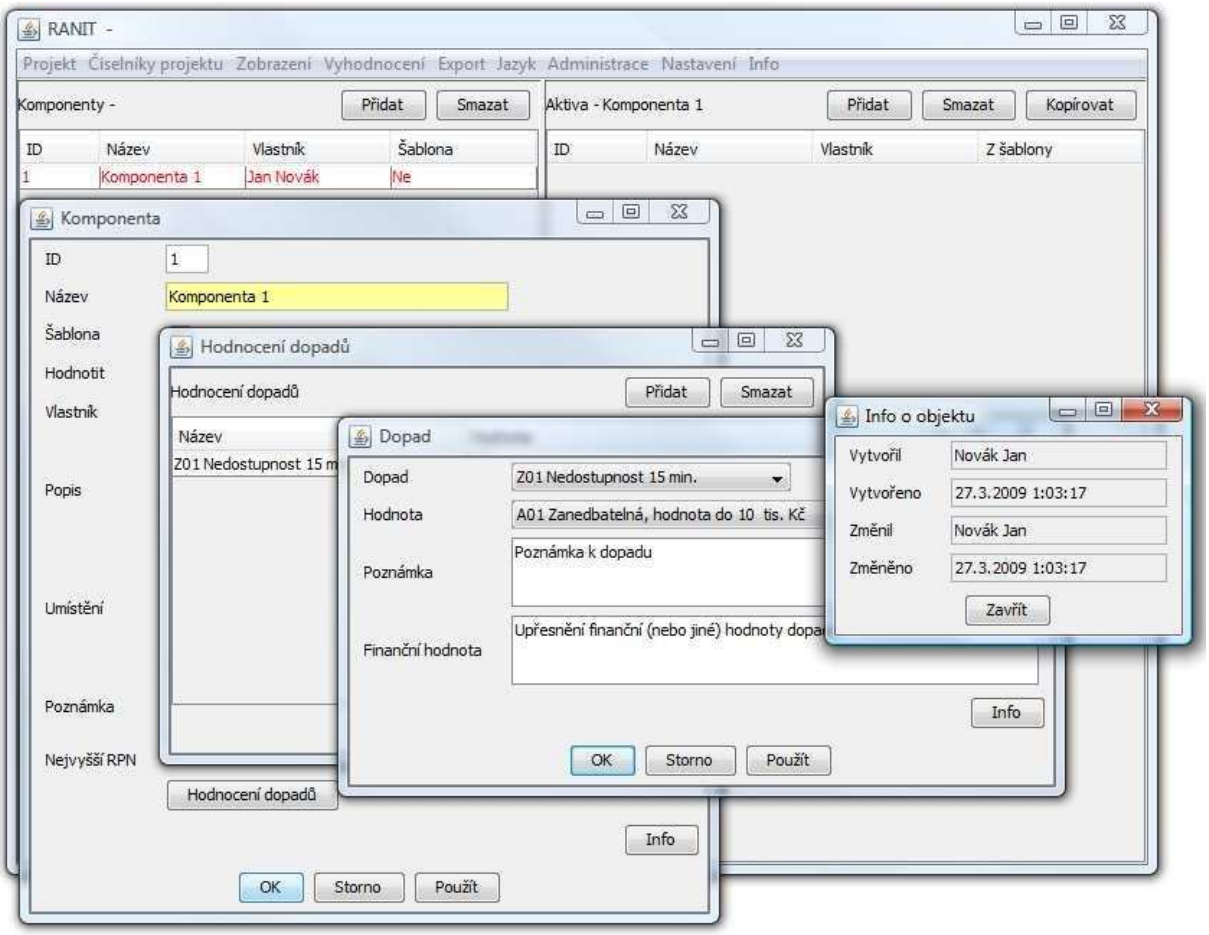
Po stisknutí tohoto tlačítka se zobrazí karta komponenta pro vytvoření a popis komponenty. Jako povinné je označeno pole „Název“. Přiřazení vlastníka (popř.

vytvoření nového), vyplnění polí Popis, Umístění, Poznámka je nepovinné, avšak doporučené. Označení komponenty jako šablony, což znamená, že v případě vytvoření kopie aktiva této komponenty do jiných komponent není vytvořena samostatná kopie aktiva (s vlastními atributy), ale kopie aktiva, která je z hlediska svých atributů provázána s originálem (atributy kopie nelze upravovat samostatně, upravovat lze pouze originál, ze kterého byla kopie vytvořena). Komponent může být v jednom projektu libovolný počet.

Komponentu lze v procesu Analýzy rizik kdykoli upravovat (tj. upravovat všechny výše zmíněné hodnoty – editaci komponenty otevřete jednoduše „dvojklikem“ na položku komponenty v hlavním okně aplikace). Na kartě komponenty je dostupné tlačítko „Info“ po jehož stisknutí dojde k zobrazení informací o vytvoření a změně komponenty.

Dokud není komponenta naplněna jen aktivy, označenými atributem „Dokončeno“, je komponenta (podobně jako „nedokončená“ aktiva) označena červenou barvou pro lepší orientaci v rozpracovaném projektu.

Volitelná je rovněž tzv. Bussines Impact Analýza, jejíž vstupní parametry lze zadat/upravit v kartě komponenty pod nabídkou „Hodnocení dopadů“. Jednotlivé aspekty jsou zadávány pomocí parametrů: Aspekt hodnocení, jeho hodnota a volitelně Poznámka a upřesnění finanční hodnoty dopadu (viz obrázek č. 5).



Obrázek č. 5 – Dopad a informace o objektu

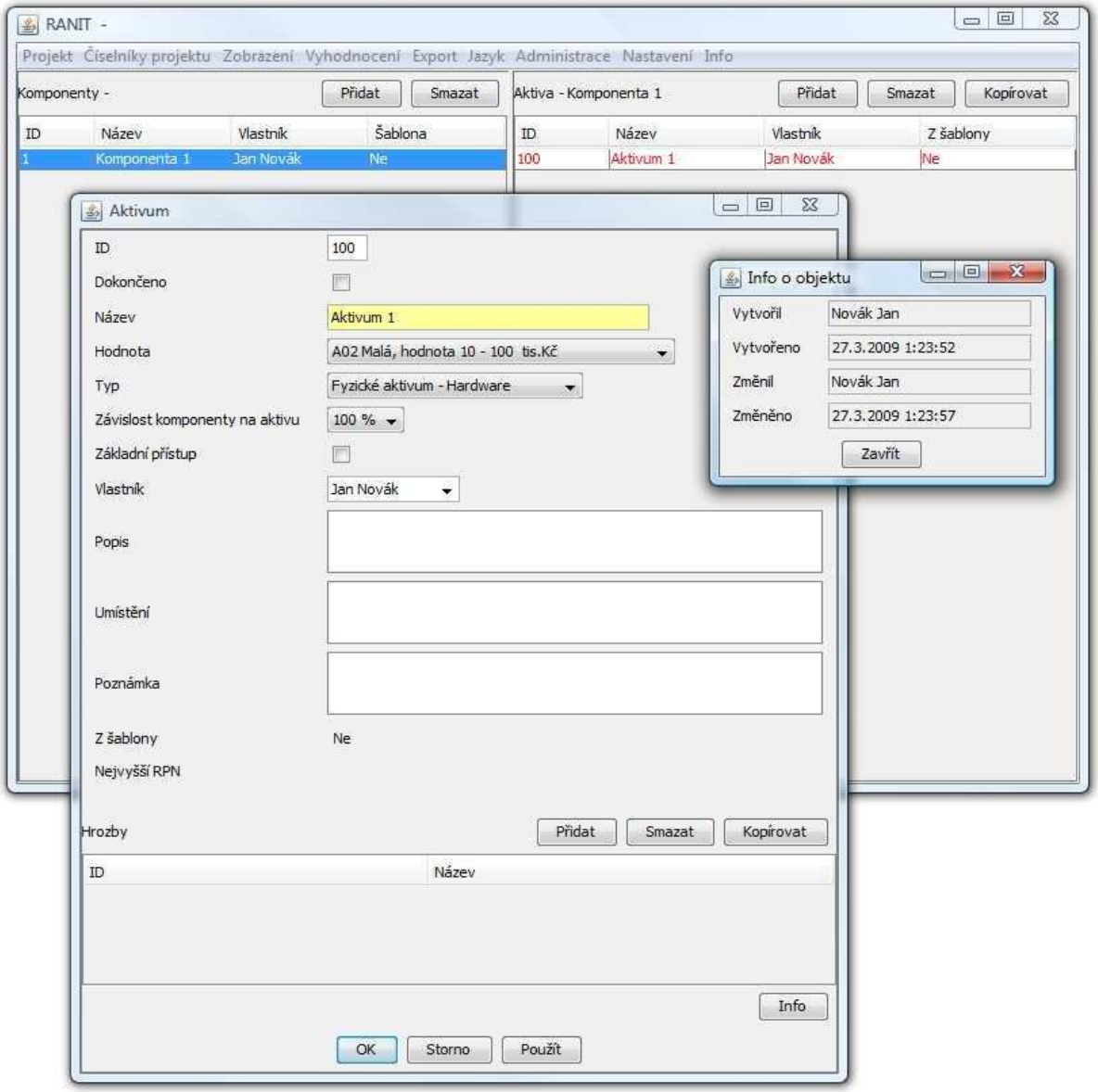
3.1.2. Aktiva

Aktivum je část celkového systému, které organizace přímo přiřazuje hodnotu a pro kterou tudíž organizace požaduje ochranu. Při identifikaci aktiv by mělo být vzato v úvahu, že informační systém netvoří jen hardware a software.

Všechna aktiva uvnitř stanovených hranic revize musí být identifikována.

Identifikovaná aktiva jsou poté přiřazena jednotlivým komponentám. Seznam vytvořených aktiv je zobrazený na pravé straně hlavního okna. Zobrazená aktiva jsou vždy aktiva vztažená k vybrané komponentě (pozn. Komponentu vyberete kliknutím na její záznam v levé části hlavního okna).

Založení aktiva je vztaženo tedy vždy ke konkrétní komponentě.



Obrázek č. 6 - Vytvoření aktiva a informace o objektu

Aktiv může být v jednom procesu/komponentě libovolný počet. Aktiva vytváříme prostřednictvím tlačítka „Přidat“ v horní části pravé poloviny hlavního okna.

Po stisknutí tohoto tlačítka se zobrazí karta aktiva pro vytvoření aktiva. Jako povinná jsou označena pole „Název“, „Hodnota“, „Typ“ a „závislost komponenty na aktivu“. Přiřazení typu aktiva, vlastníka (popř. vytvoření nového), hodnoty aktiva a závislosti komponenty na tomto aktivu (procentuální vyjádření), volitelně vyplnění polí Popis, Umístění, Poznámka a seznam hrozeb přiřazených aktivu. Zároveň je u aktiva volba „Dokončeno“ označující ukončení identifikace aktiva a všech jeho atributů. Dalším atributem aktiva je volba „Základní přístup“ (viz dále – kapitola 3.1.3. Přiřazení hrozeb aktivům).

Aktivum lze v procesu Analýzy rizik kdykoli upravovat (tj. upravovat všechny výše zmíněné atributy – editaci aktiva otevřete jednoduše „dvojklikem“ na položku aktiva v hlavním okně aplikace). Na kartě aktiva je dostupné tlačítko „Info“ po jehož stisknutí dojde k zobrazení informací o vytvoření a změně aktiva.

Dokud není aktivum označeno jako dokončené (viz výše) je aktivum (a komponenta, ke které toto aktivum přísluší) označena červenou barvou pro lepší orientaci v rozpracovaném projektu.

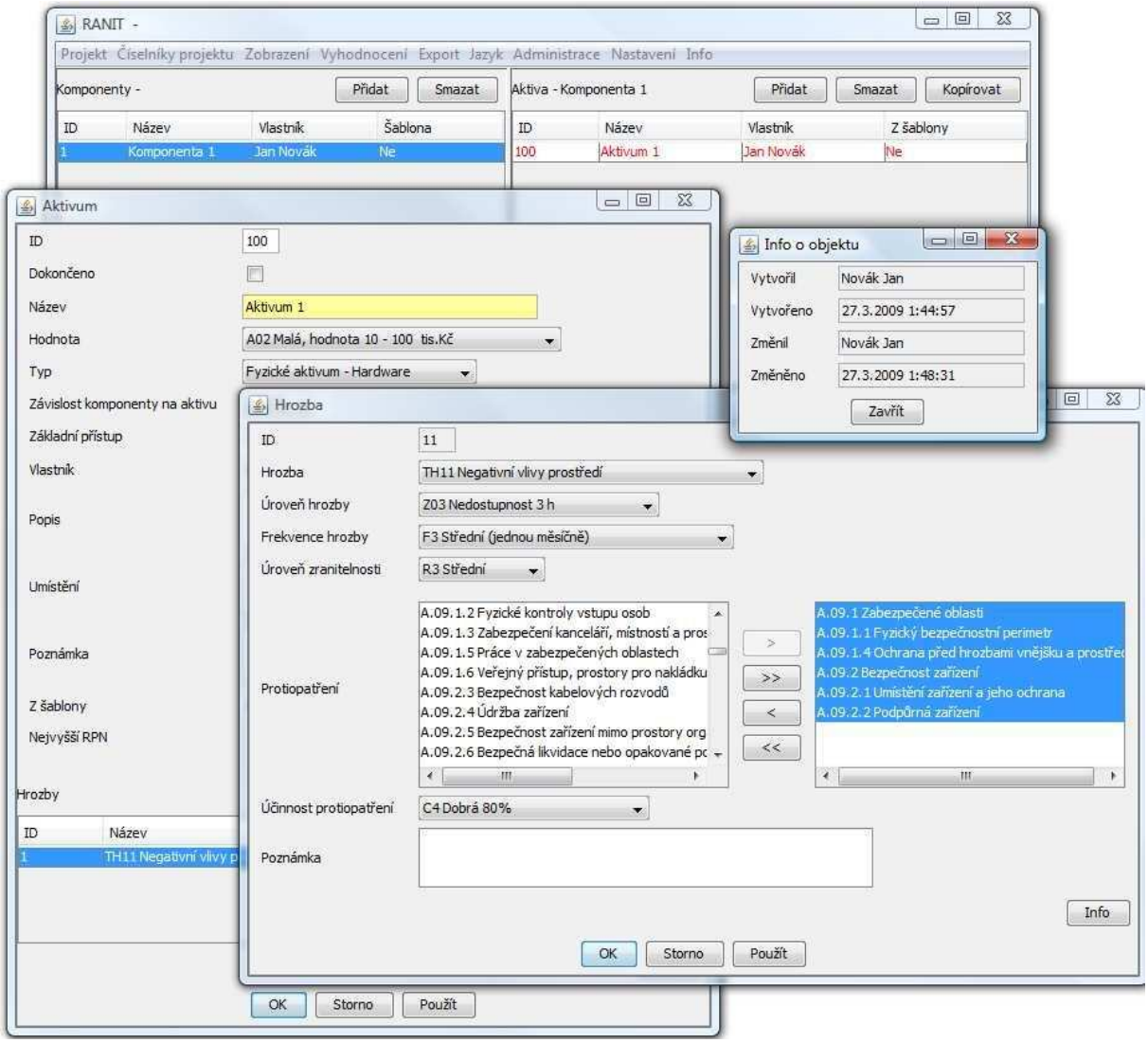
Každému typu aktiva lze z číselníku (viz dále) hrozeb přiřadit hrozby, které jsou pro tento typ aktiva relevantní a budou nabízeny k výběru. Tento seznam je zároveň vodítkem při řízeném pohovoru s vlastníkem komponenty či aktiva.

Na rozdíl od komponent, je možné vytvořená aktiva kopírovat a poté tyto kopie upravovat, čímž si uživatel značně ulehčí vytváření podobných aktiv.

Pokud je aktivum součástí komponenty, která je označená atributem „Šablona“ (viz kapitola 3.1.1 Komponenty), pak v případě vytvoření kopie aktiva této komponenty (volba „Kopírovat“) do jiných komponent není vytvořena samostatná kopie aktiva (s vlastními atributy), ale kopie aktiva, která je z hlediska svých atributů provázána s originálem (atributy kopie nelze samostatně upravovat, upravovat lze pouze originál, ze kterého byla kopie vytvořena).

3.1.3. Přiřazení hrozeb k aktivům

Založení hrozby vztahující se k aktivu: Při zaškrtnutí volby „Základní přístup“ v předchozí nabídce (při vytvoření/úpravě aktiva) není možné zakládat hrozby vztahující se k aktivu. V opačném případě jsou hrozby nabízeny k výběru z tabulky hrozeb v závislosti na typu aktiva. Dále přiřazení úrovně hrozby výběrem z tabulky úrovní hrozeb, přiřazení frekvence hrozby výběrem z tabulky frekvencí hrozby, přiřazení úrovně zranitelnosti z tabulky úrovní zranitelnosti, přiřazení jednoho nebo více protiopatření výběrem z tabulky protiopatření a přiřazení účinnosti protiopatření z tabulky účinnosti protiopatření (viz obrázek č. 7).



Obrázek č. 7 – Vytvoření hrozby, přiřazení protiopatření a informace o objektu

Hrozeb může být přiřazeno k jednomu aktivu libovolný počet. Pro sledování trendů je volitelně možné vybrat z tabulky protiopatření uvažovaná opatření a přiřadit účinnost uvažovaných protiopatření z tabulky účinnosti protiopatření.

3.1.4. Rizika

Aplikace RANIT na základě vložených údajů stanoví hodnotu míry rizika pro každou hrozbu/aktivum/komponentu. Hodnota míry rizika je stanovena ve třech variantách: aktuální míra rizika (Riziko), míra rizika po aplikaci uvažovaných protiopatření (Riziko (Uvažovaná protiopatření)) a jako míra rizika hrubá tedy bez aplikace protiopatření (Riziko (Bez protiopatření)). Pozn.: Hodnocení dopadů ovlivňují stanovenou míru rizika.

4. Vyhodnocení

Kdykoliv v průběhu vkládání dat lze zobrazovat výsledky v přehledu, kde jsou stanovené hodnoty míry rizika již také rozděleny do skupin a barevně zvýrazněny. Rovněž lze kdykoliv vytvořit textový soubor ve formátu RTF, obsahující podrobný výpis a vyhodnocení všech získaných údajů, setříděný dle komponent a aktiv, nebo podle stanovené míry rizika. Textový výstup lze vytvořit ze všech údajů nebo jen z údajů o komponentách a aktivech jednoho vlastníka. Taktéž samotné zobrazení aktiv a komponent lze kdykoli zobrazit pouze pro jednotlivé vlastníky.

PŘÍLOHA P IV: PROJEKTOVÝ MANAGEMENT

Vzhledem k tomu, že zavádění bezpečnostní politiky, je potřeba důkladně rozplánovat a její realizaci systémově řídit, je v této části práce zařazena kapitola o projektovém managementu, který by měl tento proces usnadnit.

Projekty zaměřené na bezpečnost by měly být kvantifikovány pomocí těchto parametrů [10]:

- *popis cíle a účelu,*
- *priorita řešení,*
- *popis výstupů,*
- *popis projektových etap,*
- *návaznost na další projekty,*
- *předpoklady a rizika,*
- *odhad ceny a časové náročnosti.*

Dále by neměl chybět harmonogram zavádění, který zachycuje návaznosti a možnosti řešení více projektů paralelně. [10]

PDCA

Metoda PDCA (plan – do – check – act) se využívá pro řešení každodenních problémů v nejrůznějších sférách podnikové činnosti.

Metodika byla vytvořena tak, aby umožňovala efektivní řešení a zlepšování výrobních procesů a systémů. Často je také využíván při zavádění změn a řešení problémů. PDCA cyklus je využíván zejména v oblastech řízení kvality a zajišťování bezpečnosti.

Celá metoda se stává ze čtyř kroků:

1. **Plan (plánuj)** – tato fáze zahrnuje zjišťování informací a popis řešeného problému, ze kterých je následně vytvořen plán, obsahující činnosti, které je třeba udělat k odstranění řešeného problému.
2. **Do (dělej) –** postupné zavádění činností naplánovaných v předchozím kroku.
3. **Check (kontroluj)** – následující krok obsahuje sledování dosažených výsledků a jejich srovnávání s nastaveným plánem a postupné plnění a kontrolu nastaveného plánu.

4. **Act (jednej)** – jestliže, v průběhu realizace není plán plněn dle očekávání a problém není řešen, dle očekávání, je třeba stanovit nový plán, ve kterém se zaměříme na odstranění příčiny. Pak lze potřebné změny implementovat a uplatňovat při každodenních činnostech.

PŘÍLOHA P V: RODINA ISO 27000