Semestrální práce ke kurzu 4IT421 Zlepšování procesů budování IS	
Semestr	LS 2014/2015
Autoři	Barbora Nagyová, xnagb00 Pavel Strnad, xstrp47
Téma	Mezinárodní norma ISO/IEC 15504 - bezpečnostní rozšíření
Datum odevzdání	15.3.2015

Obsah

Úvod

Problematika normování podnikových procesů a jejich certifikace je v současné době stále velmi zajímavou a často projednávanou otázkou. Proces normování přináší podnikům mnohé benefity, které není radno přehlížet. Zároveň ale i tento proces představuje obrovské množství lidské práce, které se za ním skrývá. Společně s lidskou prací je proces implementace normovaných podnikových procesů a bezpečnostních opatření velmi nákladnou procedurou, která se může za nepříhodné situace velmi prodražit a mít na podnik neblahé následky.

Z tohoto důvodu vznikla tato práce s cílem přiblížení účelu Bezpečnostní rozšíření normy ISO/IEC 15504. Bezpečnostní rozšíření ISO/IEC 15504 vzniklo jako smyšlený most, který propojuje normu ISO/IEC 15504 zaměřenou na posuzování podnikových procesů současně s normou ISO/IEC 27002, která se věnuje zavádění bezpečnostních opatření v podnicích s cílem získat bezpečnostní certifikace definované na základě normy ISO/IEC 27001. Tímto pomáhá ulehčit implementaci norem ISO/IEC 15504 a ISO/IEC 27002 a současně snížit náklady, které tento proces přináší.

Tato práce pojednává zejména o Bezpečnostním rozšíření normy ISO/IEC 15504. V rámci tohoto tématu však budou představeny i další normy jako je rodina norem ISO/IEC 27000, norma ISO/IEC 15504 a něco málo bude řečeno i o normě ISO/IEC 12207. Všechny tyto normy totiž spolu úzce souvisí a svým způsobem charakterizují vlastní důvod vzniku Bezpečnostního rozšíření normy ISO/IEC 15504 a jeho použití.

Cílem této semestrální práce je tedy analyzovat Bezpečnostní rozšíření mezinárodní normy ISO/IEC 15504, porovnat jej a rozlišit od norem ISO/IEC 27000, ISO/IEC 27001 a ISO/IEC 27002. Dále se bude tato práce věnovat přiblížení podstaty využití těchto norem a současně bude vyzdvihovat přidanou hodnotu, kterou přináší Bezpečnostní rozšíření normy ISO/IEC 15504. Konkrétně se tedy tato práce bude zaměřovat na popis výše uvedených norem a jejich vzájemné kompatibility. V rámci tohoto popisu budou zmíněny jejich přínosy pro podniky. Následně bude také popsáno jejich začlenění v procesu implementace norem v podniku a způsoby, kterými tato implementace probíhá.

Norma ISO/IEC 15504 a její bezpečnostní rozšíření

ISO norma 15504, taktéž známá pod zkratkou SPICE (Software Process Improvement and Capability Determination) je mezinárodní normou, na jejímž základě se posuzuje kvalita procesů v oblasti vývoje, správy a nákupu software. Norma stanovuje minimální požadavky na realizaci a posuzování procesů.

Tato norma úzce souvisí s ISO normou 12207, která obsahuje referenční model SW procesu, původně definovaný v normě 15504, nicméně v roce 2004 se referenční model od normy 15504 oddělil a díky tomu se model normy 15504 soustředí pouze na realizaci posouzení kvality procesu.

Obsah normy

Norma se skládá z těchto devíti částí:

- 1. Pojmy a slovník (Concepts and vocabulary)
- 2. Realizace posouzení (Performing an assessment)
- 3. Návod na realizaci posouzení (Guidance on performing an assessment)
- 4. Návod na zlepšování procesu a určování způsobilosti procesu (Guidance on use for process improvement and process capability determination)
- 5. Vzor modelu posuzování procesu (An exemplar software life cycle process assessment model)

Zbylé části nebyly do českého jazyka nikdy přeloženy, nicméně jejich překlad zní přibližně takto:

- 6. Příklad životního cyklu modelu posouzení systémového procesu (An exemplar system life cycle process assessment model)
- 7. Posouzení organizační vyspělosti (Assessment of organizational maturity)
- 9. Zaměření procesních profilů (Target process profiles)
- 10. Bezpečnostní rozšíření (Safety extension)

V současnosti se připravuje další část normy s názvem: 8. Příklad posouzení procesního modelu pro řízení IT služeb – technický report (An exemplar process assessment model for IT service management [Technical report]). [11]

Jak již bylo řečeno, tato norma se zabývá posuzováním procesů. Samotný model posuzování procesů je definován ve 2. části normy, nazývané též jako ISO/IEC 15504-2 (Realizace posouzení). Model je dvoudimenzionální, první je dimenze procesní, ve které jsou procesy charakterizovány a klasifikovány do příslušných kategorií. Druhá dimenze definuje rozsah způsobilosti na základě modelu CMMI. Model CMMI definuje 6 úrovní zralosti procesů:

0 – Neúplné – tuto nejnižší úroveň zralosti mají procesy, které jsou chaotické a nejsou realizovány v plném rozsahu.
1 – Vykonávané - procesy jsou vykonávané a mohou splnit svůj účel díky identifikovaným pracovním produktům.
2 – Řízené – procesy jsou řízené podle definovaných postupů.
3 – Zavedené – je zavedena dokumentace procesů a procesy probíhají podle toho, jak jsou nadefinované.

4 – Předvídatelné – lze dopředu předvídat a efektivně řídit náročnost procesů, neboť jsou kvantitativně řízené.
5 – Optimalizované – Nejvyšší úroveň zralosti dosahují ty procesy, které optimalizované tak, aby byly pro podnik co nejefektivnější a splňovaly jak současné, tak budoucí požadavky podniku. [5]

ISO/IEC 15504 – Bezpečnostní rozšíření (Security extension)

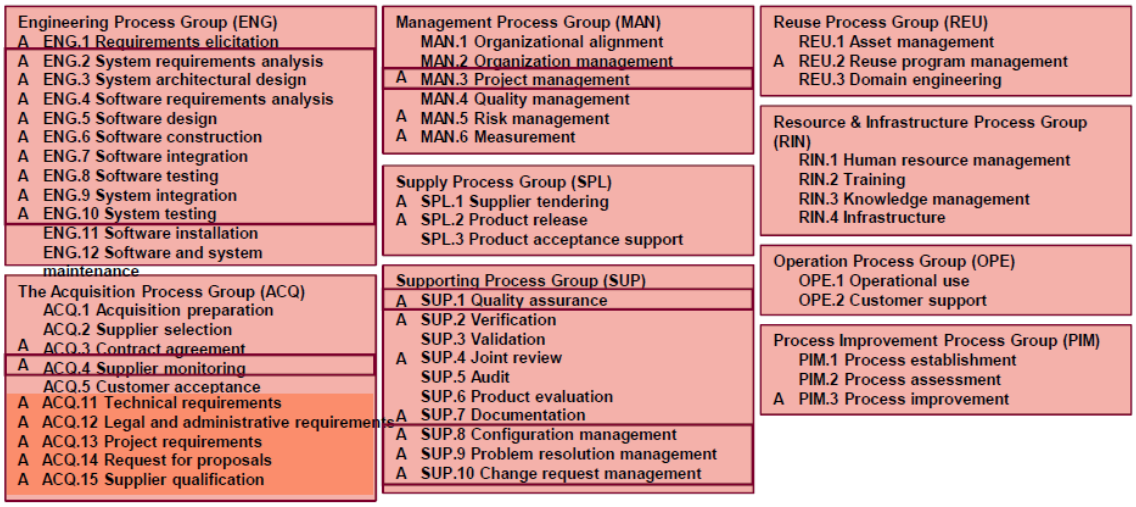
K normě 15504 existuje i rozšíření, které pokrývá oblast bezpečnosti. Jedná se v podstatě o rozšíření části 15504-5. Bezpečnostní rozšíření má dva následující cíle:

1. Usnadnění implementace normy ISO/IEC 27001 v softwarových organizacích, které byly zahrnuty do programu SPI (Software proces improvement – Zlepšení sw procesů) v souladu s normou 15504.

2. Usnadnění simultánní implementace ISO/IEC 27001 a ISO/IEC 15504 standardů tak, aby se předešlo opakování stejných částí, vyskytujících se v obou standardech, a aby se tak snížilo úsilí, vyžadované organizací.

Pro naplnění těchto cílů musí organizace v obou případech nejprve vybrat z normy ISO/IEC 27002 všechna aplikovatelná opatření v závislosti na druhu organizace a jejích hlavních aktivit. Ve druhém kroku vybere procesy z normy ISO/IEC 15504-5, které pokrývají opatření zvolená v prvním kroku.

Příklad: Podnik zvažuje implementaci opatření, převzaté z normy ISO/IEC 27002 s názvem Poučení se z vyskytnutých událostí, týkající se informační bezpečnosti (Learning from information security incidents), které je definováno jako: „Mechanismus, který umožňuje kvantifikaci a monitorování typů, objemů a nákladů incidentů informační bezpečnosti. Informace, získané z vyhodnocení incidentů informační bezpečnosti, by měly být použity k identifikaci opakující se incidenty nebo ty s vysokým dopadem. Vyhodnocení incidentů může naznačit potřebu zlepšení, nebo přidání dalších kontrol pro omezení frekvence, škod a nákladů na budoucí výskyt.“ Aby mohlo dojít ke splnění požadavků z výše definovaného opatření, je potřeba vybrat veškeré procesy, pokrývající danou oblast. [1] Následuje tabulka těchto procesů:



[12]

Procesy, které pokrývají oblast daného opatření, jsou: SUP.9, MAN.5 a RIN.3.

Proces SUP.9 (Management řešení problémů) musí zajistit, že incidenty bezpečnosti informací jsou definované, analyzované, řízené a kontrolované v souladu s bezpečnostní politikou.

Proces MAN.5 (Management rizik) musí zajistit, že incidenty jsou neustále identifikovány, analyzovány, kvantifikovány, vyšetřovány a monitorovány.

Proces RIN. 3 (Znalostní management) vyžaduje záznam informací, získaných z ohodnocení incidentů. [1]

Normy řady 27000

Veškeré normy z řady 27000 se zabývají oblastí informační bezpečnosti. Definic pro bezpečnost informací existuje mnoho, nicméně všechny se shodují v tom, že bezpečnost informací se snaží o zajištění tří věcí: důvěrnosti, integrity a dostupnosti informace. Znamená to tedy, že informace je zpřístupněna pouze tomu, kdo k ní má oprávnění, že je tato informace správná a úplná a je přístupná ve správnou dobu, kdy jí uživatel potřebuje. [4] Bezpečnost informací je v dnešní době velmi důležitá, neboť informace neustále nabývají na hodnotě a je to nejcennější aktivum jak pro lidi, tak pro celé firmy.

Do řady 27000 patří celá řada norem, pokrývající oblast bezpečnosti informací. Tyto normy bývají poměrně často aktualizované, a jelikož bezpečnost informací je neustále se vyvíjející obor, každou chvíli vznikne nová norma. V současnosti se připravuje norem hned několik, patří mezi ně například norma ISO 27017, která poskytuje doporučení pro zabezpečení cloud computingu, dále norma ISO 27040, která obsahuje doporučení pro bezpečné ukládání dat, nebo norma ISO 27041, která obsahuje doporučení pro zajištění důkazů pro digitální metody vyšetřování. [6]

Mezi ty nejznámější normy řady 27000 patří v současnosti norma ISO 27000, ISO 27001 a ISO 27002, které přímo souvisejí s normou ISO 15504 a jsou dále charakterizovány.

Norma ISO/IEC 27000

První norma ISO/IEC 27000, celým názvem „Information technology - Security techniques - Information security management systems - Overview and vocabulary“ patří do skupiny norem 27000 - Information Security Management System (ISMS). Vznikla v roce 2009 a její poslední aktualizace proběhla v roce 2014. Obsahem této normy je seznam veškerých důležitých pojmů z oblasti bezpečnosti informací a jejich přesná definice, a terminologický slovník. Pojmy, definované v této normě jsou pak používané v charakteristice ostatních norem řady 27000.

Tato norma vznikla proto, že ostatní normy, spadající do řady 27000 nejsou napsané pouze jedním člověkem, na jejich tvorbě se podílí mnoho lidí. Vzhledem k tomu, že každý autor při tvorbě a úpravě norem by mohl používat rozdílné pojmy, které by mohly vést k mnohým nedorozuměním, bylo potřeba tyto pojmy standardizovat a exaktně definovat jejich význam. [6]

Mezi definované pojmy patří například:

Hrozba – potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace
Risk – účinek nejistoty na cíle
Útok – pokus o zničení, odhalení, změnu, ukradení nebo získání neautorizovaného přístupu nebo neoprávněné používání aktiva
Následek – Výsledek události, která negativně ovlivní vytyčené cíle.
[9]

Norma ISO/IEC 27001

Obsah normy

Další normou z řady 27000 je norma 27001. Tato norma nahradila svou předchozí verzi BS7799-2:2002 v roce 2005 a naposledy byla aktualizovaná v roce 2013. Její název zní Information technology – Security techniques – Information security management systems – Requirements, neboli požadavky na bezpečnost informací. [7]

Tato norma slouží k tomu, aby usnadnila aplikaci normy 27002. Obsahuje seznam doporučení, které by podniky měly dodržet proto, aby získaly certifikaci o bezpečnosti informací. Norma popisuje, jak by měl vypadat vhodný systém řízení, struktura a procesy pro řízení informační bezpečnosti. Podnik však nemusí nutně získat certifikaci, pokrývající veškeré části organizace, systém bezpečnosti může být zaveden pouze do některých částí. Doporučení, která tato norma obsahuje, jsou v souladu s opatřeními, která jsou definovaná v normě 27002. [4]

Norma vychází z modelu PDCA (Plan-Do-Check-Act):

Plan - ustanovení ISMS, kde se vytváří například bezpečnostní plány a cíle, definuje se politika a vymezí rozsah řízení bezpečnosti informací, identifikují, analyzují a vyhodnocují se rizika. Výsledky musí být v souladu s cíli organizace.

Do – Zavádění a provozování ISMS, kde probíhá řízení provozu a zdrojů ISMS, formuluje se a implementuje se zde plán zvládání rizik, určují se postupy pro měření účinnosti zavedení těchto opatření, a další.

Check – Monitorování a přezkoumání ISMS, kde se například měří účinnost zavedených opatření, identifikují se možná zlepšení systému, probíhají monitorovací procedury, interní audit ISMS, a jeho pravidelná analýza a řízení.

Act – Udržování a zlepšování ISMS – kde probíhá implementace identifikovaných zlepšení ISMS z předchozího kroku, provedení nápravných a preventivních akcí a další. [7]

Co podniku přinese dodržení požadavků na bezpečnost informací?

Pro podniky je dodržení požadavků nezbytné, pokud chtějí získat certifikaci systému řízení bezpečnosti informací uvnitř podniku. Díky této certifikaci podniky mohou získat konkurenční výhodu nad podniky, které tuto certifikaci nemají. Zároveň mohou lépe jednat se svými obchodními partnery, protože mají „záruku“, že data, která si vzájemně vyměňují, jsou zabezpečená a riziko jejich zneužití je velmi nízké.

Na druhou stranu zavedení systému řízení bezpečnosti informací je poměrně nákladné a malé firmy si jej často nemohou dovolit, proto bývá tento systém častěji zavedený ve větších podnicích. [4]

Norma ISO/IEC 27002

Norma ISO/IEC 27002 je další normou z řady 27000. Původně se jmenovala ISO/IEC 17799:2005, avšak v roce 2007 byla zařazena do souboru norem 27000 a byla přejmenována na svůj současný název. Její obsah byl zachován. Tato norma se naposledy dočkala aktualizace v roce 2013. Její celý název zní „Information technology - Security techniques - Code of practice for information security management“, neboli sada nejlepších praktik v oblasti řízení bezpečnosti informací. [8]

Tato norma v podstatě definuje seznam všech doporučených opatření, založených na „best practice“, které by podniky měly dodržet pro zajištění bezpečnosti jejich informací. Jedná se však pouze o doporučení, což znamená, že nejsou závazná a každá společnost si může zvolit vlastní způsob ke splnění bezpečnostních požadavků, které jsou definované v normě 27001.

Podniky nejprve zhodnotí a analyzují bezpečnostní rizika. Na základě analýzy bezpečnostních rizik pak v dalším kroku vyberou vhodná doporučení, které jsou v souladu s riziky a také s požadavky. Doporučení se primárně snaží pokrýt oblasti, kde se vyskytují důležité a pro firmy klíčové informace, které mají vysoké riziko, že by mohly být jakýmkoliv způsobem zneužity. Protože předmět podnikání, politika a procesy jsou u každé firmy trochu rozdílné, doporučená opatření v této normě si společnosti mohou do jisté míry přeformulovat a přizpůsobit podle svých potřeb. Cílem tedy není bezpodmínečně aplikovat veškerá opatření, definovaná v této normě, ale spíše naimplementovat ta opatření, která jsou pro podnik možné aplikovat. [4]

Obsah normy

Norma definuje 35 cílů opatření pro větší ochranu informací, aby nemohlo dojít k porušení jejich bezpečnosti (důvěrnosti, dostupnosti a integrity). Cíle opatření obsahují funkční požadavky na architekturu konceptu bezpečnosti informací.

Dále obsahuje více než 100 specifických opatření, které společnost musí vzít v úvahu pro zajištění kontrolních cílů. Některá opatření vychází z legislativních požadavků, jedná se například o ochranu osobních údajů, ochranu duševního vlastnictví, či ochranu důležité dokumentace organizace (účetní záznamy a pod.). Ostatní opatření pro zajištění bezpečnosti vychází z best practices, zde se jedná například o dokument bezpečnostní politiky informací, přidělení odpovědnosti v oblasti bezpečnosti informací, vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací, zvládání bezpečnostních incidentů a jejich kroky k nápravě. [10]

Oblasti, kterých se opatření týkají, jsou: Hodnocení a zvládání rizik, bezpečnostní politika, organizace bezpečnosti informací, řízení aktiv, bezpečnost lidských zdrojů, fyzická bezpečnost, řízení provozu ICT, řízení přístupu uživatelů, pořízení a vývoj systémů, zvládání incidentů, řízení kontinuity činností a soulad s požadavky. [10]

Porovnání norem

Tato část semestrální práce se bude věnovat obecnému shrnutí a vysvětlení vztahů mezi výše uvedenými normami tak, aby čtenář měl jasno v této problematice.

Nejdříve si tedy povíme proč je pro podniky lukrativní se touto problematikou zabývat. Veškerá otázka bezpečnosti se točí právě kolem normy ISO/IEC 27001. Tato norma, jak bylo již dříve řečeno, umožňuje firmám získat certifikaci v dané oblasti bezpečnosti informací. Podniky nemusejí získávat certifikaci na veškeré procesy, ale pouze jen na ty, které si zvolí jako nejvíce ceněné. V této fázi je důležité správně vybírat, jelikož certifikace a úpravy procesů dle požadavků bezpečnosti informací jsou poměrně nákladná činnost. Na druhou stranu přináší tato certifikace také podnikům konkurenční výhodu, která jim může v budoucnu přinést velmi zajímavé projekty. Je samozřejmě jisté, že při výběru dodavatele informačního systému, ve kterém se i v omezené míře pracuje s citlivými informacemi, zvolí každý odběratel raději mezinárodními normami certifikovanou firmu, než kohokoliv jiného.

Teď, když už známe důvod, proč mají firmy zájem o tuto problematiku, ukažme si, co dalšího lze v této chvíli pro podnik dále udělat. Jakmile podnik začne uvažovat o získání certifikace bezpečnosti informací ať už v jakémkoliv měřítku, musí nejprve definovat svá rizika, která mohou při práci s těmito citlivými daty nastat a na základě této analýzy zvolit bezpečnostní opatření. Právě této problematice se věnuje norma ISO/IEC 27002, která může podniku přinést světovou komunitou uznávané „best practices“ v této oblasti. Na základě těchto doporučení si podnik může, ale také nemusí vytvořit opatření pro snížení těchto rizik. Jak jsem již zmínil, tato opatření nejsou podmínkou při certifikaci, každý podnik může zvolit svou cestu, kterou se vydá při řešení tohoto problému. Najde se ale jen málo případů, kdy je lepší poslechnout vlastní rozum, než si nechat poradit od normalizačních autorit.

Další důležitou normou je norma ISO/IEC 15504. Tato norma obsahuje také své vlastní bezpečností rozšíření, kolem kterého se celá tato semestrální práce točí. Norma ISO/IEC 15504 se konkrétně zabývá výhradně posuzováním kvality procesů. Tento proces hodnocení je tvořen ze dvou částí. Nejdříve je nutné dané procesy charakterizovat a následně v druhém kroku je klasifikovat. Klasifikace probíhá dle známého modelu zralosti CMMI.

Je však otázkou jak do tohoto ale zapadá bezpečnostní rozšíření normy ISO/IEC 15504. V obecném pojetí jde o imaginární most, který spojuje současnou implementaci normy ISO/IEC 27001 a 15504 v podniku. Toto rozšíření zajišťuje, aby při této snaze v podniku nedocházelo k zbytečným duplicitním akcím a tím i úspěšně snižuje dobu implementace a náklady na zlepšení procesů budování IS.

Řízení bezpečnosti a praktické užití bezpečnostního rozšíření normy ISO/IEC 15504

Tato kapitola pojednává o praktickém nasazení opatření bezpečnosti informací z normy ISO/IEC 27002 v podniku, kde jsou již zavedeny a klasifikovány procesy pokryté normou ISO/IEC 15504.

Typy adaptace procesů normy ISO/IEC 15504 pro splnění opatření z ISO/IEC 27001

Při zavádění bezpečnostních opatření v podniku je nutné počítat s právě zavedenými a fungujícími podnikovými procesy. Tyto procesy mohou být různého typu a také různým způsobem mohou zasahovat do nasazení bezpečnostních opatření popsaných v normě ISO/IEC 27002. Z tohoto důvodu jsou přímo definovány čtyři akce, které popisují jak je nutné s těmito procesy zacházet při zavádění daných opatření.

Čtyři nejčastější akce spojené se zaváděním bezpečnostních opatření

Nejlepší případ pojednává o částečném, nebo plnohodnotném využití daných procesů pro docílení požadavků daných opatření bez jakýchkoliv úprav podnikových procesů.

V dalším případě se může jednat pouze o rozšíření základních charakteristik jednoho nebo více procesů za účelem uspokojení nároků na bezpečnost, což ještě neznamená velké úsilí.

Často ale může docházet k nutnosti přidání nových charakteristik procesů s cílem dosáhnutí bezpečnostních požadavků tak, aby došlo k změně již zaběhlých procesů.

A posledním opatřením je úplné změnění, či rozšíření daných procesů a jejich cílů, tak aby vedly k dodržení bezpečnostních opatření uvedených v normě ISO/IEC 27002.

Příklady adaptace procesů normy ISO/IEC 15504 při zavádění bezpečnostních opatření normy ISO/IEC 27002

Tato část semestrální práce se věnuje ukázkám praktických případů, kdy je nutné pracovat současně s normou ISO/IEC 15504-5 a ISO/IEC 27002 za účelem dosažení požadovaných bezpečnostních opatření pro získání certifikace.

Praktický příklad jednotných charakteristik procesů při nasazování bezpečnostních opatření

Je důležité zmínit, že některé podnikové procesy s vnitřními charakteristikami, které se shodují s normou ISO/IEC 15504-5 není nutné nijak měnit k dosažení bezpečnostních opatření

uvedených v normě ISO/IEC 27002. Příkladem může být přímé propojení mezi odstavcem 10.1.1 normy ISO/IEC 27002 a částí SUP. 7 z normy ISO/IEC 15504-5 , kde obě tyto normy vykládají způsob dokumentace procesu, jehož činností je vytvářet a spravovat záznamy tvořené jinými procesy. Výklad obou těchto norem je naprosto totožný a není nutný žádný další zásah při jejich implementaci ať už společné, nebo jen částečné.

Praktický příklad rozšíření vnitřních charakteristik procesů při nasazování bezpečnostních opatření

V některých případech může docházet k nutnosti rozšíření vnitřních charakteristik procesů uvedených v normě ISO/IEC 15504-5 za účelem pokrytí všech aspektů bezpečnostních opatření. Jedním případem této situace může být vztah mezi odstavcem 8.2.2 normy ISO/IEC 27002, který se věnuje uvědomělosti bezpečnosti informací, vzdělání a jejich tréningu. Je zde pojednáno o tom, jakým způsobem by měli být všichni důležití zaměstnanci, zákazníci a účastníci třetích strach poučeni a instruováni o bezpečnostních opatřeních a procedurách týkajících se jejich zaměstnání. S tímto nařízením nepřímo souvisí RIN.2.BP2 „Identifikace potřeb k zaškolení“ z normy ISO/IEC 15504-5, která pojednává o zjištění a porovnávání zkušeností a znalostí získaných při školeních. V tomto případě je možné jednoduše rozšířit tyto požadavky o bezpečnostní nároky, odpovědnosti a podniková opatření tak, aby bylo vyhověno bezpečnostním požadavkům dané normy.

Praktický příklad přidání vnitřních charakteristik procesů při nasazování bezpečnostních opatření

V dalším případě je popsán způsob, jakým se přidává, nebo rozšiřuje vnitřní charakteristika procesu popsaného normou ISO/IEC 15504-5 za účelem pokrytí nároků na bezpečnost. Jednoduchým případem může být odstavec 12.4.2 normy ISO/IEC 27002, který se věnuje ochraně testovacích dat systému. Pojednává o tom, jakým způsobem by testovací data měla být vybírána, chráněna a spravována. Například když je zaměstnanec danou situací donucen použít citlivá data někoho ze zákazníků pro testování nového software, je nutné, aby nejprve došlo k nevratnému poškození těchto dat tak, aby nemohla být následně zneužita třetí stranou. Právě v tomto případě bylo nutné přidat novou vnitřní charakteristiku k procesu ENG.8.BP0 „Ochrana testovacích dat“ normovaného v ISO/IEC 15504-5, která splňuje tyto požadavky.

Praktický příklad změny účelů procesů při nasazování bezpečnostních opatření

Poslední možností je adaptace účelu procesů normy ISO/IEC 15504. V tomto případě byla shoda identifikována pouze na základě porovnání popisu bezpečnostního opatření s účelem daného procesu a daná situace žádá změnu, nebo rozšíření tohoto účelu za cílem pokrytí všech popsaných bezpečnostních požadavků. Ilustrovat nám to může případ odstavce 10.7.4 „Řízení bezpečnosti systémové dokumentace“ normy ISO/IEC 27002, která pojednává o ochraně proti neoprávněnému přístupu právě k těmto souborům dokumentace. Dle popisu byl definován proces SUP.7 normy ISO/IEC 15504 „Proces dokumentace“. Pro dosažení daných bezpečnostních požadavků bylo nutné

účel tohoto procesu rozšířit tak, aby nejen vytvářel a spravoval danou dokumentaci, ale také aby se věnoval určování přístupu a zabezpečoval tak dokumentaci proti neoprávněnému užití.

Praktické užití bezpečnostního rozšíření normy ISO/IEC 15504

Jak již bylo zmíněno, právě bezpečnostní rozšíření normy ISO/IEC 15504 bylo stvořeno tak, aby celý tento proces adaptace co nejvíce zjednodušil. Nejlépe tuto situaci můžeme demonstrovat na konkrétním případu popsaném v dříve zmíněné kapitole věnované přímo tomuto rozšíření, kde při snaze dosáhnout uspokojení bezpečnostních požadavků pomohlo právě bezpečnostní rozšíření k vyvolání akcí u třech různých ISO/IEC 1504-5 procesů a jejich vzájemné spojení tak, aby bylo dosaženo společného cíle v co nejkratším čase a s minimem pracnosti.

Závěr

V této práci bylo představeno Bezpečnostní rozšíření normy ISO/IEC 15504 a současně i další normy, na které se toto rozšíření vztahuje. Zároveň byly také představeny důvody, které vedou zejména softwarové společnosti k zavedení těchto norem do podniku a jejich použití v praxi. Důležitou částí této práce byla také kapitola věnovaná praktickým ukázkám adaptace podnikových procesů při zavádění bezpečnostních opatření uvedených v normě ISO/IEC 27002. V této části byly uvedeny čtyři různé varianty situací, které mohou při těchto změnách nastat a také jejich dopady na podnikové procesy. U každého příkladu byl uveden praktický případ, který může reálně nastat při zavádění bezpečnostních opatření za účelem získání bezpečnostní certifikace. Na daném případu bylo konkrétně vysvětleno jakým způsobem je nutné podnikové procesy upravovat tak, aby splňovaly podmínky pro získání bezpečnostní certifikace uvedené v normě ISO/IEC 27001. Tímto bylo současně představeno i praktické využití Bezpečnostního rozšíření normy ISO/IEC 15504, které usnadňuje právě činnosti této adaptace a přináší podnikům úspory lidské práce a finančních nákladů.

V práci bylo také uvedeno, že Bezpečnostní rozšíření normy ISO/IEC15504 není použitelné v každé situaci. V některých případech přistupují podniky k zavádění vlastních bezpečnostních opatření, které splňují požadavky normy ISO/IEC 27001, ale neshodují se s opatřeními uvedenými v normě ISO/IEC 27002. V tomto případě je Bezpečnostní rozšíření ISO/IEC15504 zcela nepoužitelné. Podnik sice z jednoho úhlu pohledu může dodržovat normování procesů v rámci ISO/IEC15504, ale nebere ohledy na normu ISO/IEC27002, tedy přebírá veškerou odpovědnost za náklady spojené s implementací plně na sebe.

Jistě existují případy, kdy se toto jednání některým jedincům vyplácí. Obecně však, pokud se podnik rozhodne certifikovat větší množství podnikových procesů s ohledem na bezpečnost, je výhodné držet se uvedených doporučení v normě ISO/IEC27002 a za pomoci Bezpečnostního rozšíření normy ISO/IEC15504 podle nich následně adaptovat stávající podnikové procesy. Tímto postupem může podnik dosáhnout zamýšlených cílů v co nejkratším čase a s poměrně nízkými náklady.

Seznam zdrojů

[1] *Software process improvement and capability determination: 11th International Conference, SPICE 2011, Dublin, Ireland, May 30 - June 1, 2011. proceedings*. 1st ed. New York: Springer, 2011, s. 64-72. ISBN 3642212328.

[2] *SPOLEČNOST RISK ANALYSIS CONSULTANTS. Český překlad normy ČSN ISO/IEC 27001:2005. 1. vyd.* Praha: Společnost Risk Analysis Consultants, 2006.

[3] *SPOLEČNOST RISK ANALYSIS CONSULTANTS. Český překlad normy ČSN ISO/IEC 27001:2005. 1. vyd.* Praha: Společnost Risk Analysis Consultants, 2006

[4] *Komparace současných přístupů k řízení bezpečnosti informací*. Praha, 2013. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Tomáš Klíma.

[5] *Hodnocení vyspělosti procesů IT*. Praha, 2014. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Vlasta Svatá.

[6] *SPOLEČNOST RISK ANALYSIS CONSULTANTS. ISO/IEC 27000:2014* [online]. [cit. 2015-05-15]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27000

[7] *SPOLEČNOST RISK ANALYSIS CONSULTANTS. ISO/IEC 27001:2013* [online]. [cit. 2015-05-15]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27001

[8] *SPOLEČNOST RISK ANALYSIS CONSULTANTS. ISO/IEC 27002:2013* [online]. [cit. 2015-05-15]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27002

[9] Online Browsing Platform (OBP). ISO/IEC 27000:2014(en) [online]. [cit. 2015-05-15]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

[10] BS ISO/IEC 27002:2005: Information Security Management[online]. [cit. 2015-05-15]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27002/$FILE/BS_ISO_IEC_27002_obsah.pdf

[11] *Online Browsing Platform (OBP): ISO/IEC 15504-5:2012(en)* [online]. [cit. 2015-05-15].Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27002/$FILE/BS_ISO_IEC_27002_obsah.pdf

[12] PETRY, Erwin. *Automotive SPICE® & ISO/CD 26262: Their Mutual Relationship* [online]. [cit. 2015-05-15]. Dostupné také z: http://www.automotive-spin.it/uploads/5/Petry_5W.pdf