Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnostní politika firem v oblasti řízení přístupových oprávnění k informačním systémům

Bc. Ivona Fúziková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Ivona Fúziková

Podnikání a administrativa

Název práce

Bezpečnostní politika firem v oblasti řízení přístupových oprávnění k informačním systémům

Název anglicky

Security policy of companies in the area of information systems´ access rights management

---

Cíle práce

Práce si klade za cíl vytvoření návrhu interní směrnice pojednávající o řízení přístupových oprávnění k informačním systémům v podnicích, který je v souladu s legislativou a respektuje poznatky tzv. „best practice“. Na závěr práce bude vytvořen odhad finančního a personálního zatížení na zavádění navrhnuté interní směrnice.

Metodika

V teoretické části diplomové práce bude identifikována legislativa týkající se problematiky řízení práv. S danou legislativou bude pracováno metodou výkladu práva. V teoretické části budou dále analyzovány poznatky „best practice“ a bude provedena jejich vzájemná komparace. Výsledkem bude specifikace nejvýznamnějších poznatků „best practice“. Na závěr teoretické části bude provedena syntéza legislativních a „best practice“ požadavků k identifikaci stěžejních kritérií interní směrnice.

V praktické části práce budou analyzovány přístupy k řízení přístupových práv pro dva odlišné modelové podniky s rozdílnou velikostí a různým předmětem podnikání. Jednotlivé přístupy budou zkoumány z pohledu legislativních požadavků a srovnávány s identifikovanými zásadami „best practice“. Metodou syntézy budou všechny požadavky, označené jako vyhovující z obou pohledů, následně agregovány do návrhu interní směrnice.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Bezpečnostní politika, řízení přístupů, COBIT, ITIL, oddělení povinností, směrnice, informační systémy

---

Doporučené zdroje informací

BUCHALCEVOVÁ, A. *Metodiky vývoje a údržby informačních systémů : kategorizace, agilní metodiky, vzory pro návrh metodiky.* Praha: Grada, 2005. ISBN 80-247-1075-7.

GRAMLING, Audrey A. Addressing problems with the segregation of duties in smaller companies. The CPA Journal, 2010, 80 (7), s. 30-34. ISSN 0749-8284

HENDRAWIRAWAN, David. ERP security and segregation of duties audit: A framework for building an automated solution. Information Systems Control Journal, 2007. ISSN 1526-7407

LIGHTLE, Susan S. a VALLARIO, Cynthia W. Segregation of duties in ERP: an automated assessment tool enables internal auditors at MeadWestvaco to enhance their SOD control reviews throughout the enterprise. Internal Auditor, 2003. ISSN 0020-5745

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

SANDHU, Ravi S. Role-based access control models. Computer, 1996. ISSN 0018-9162

SANDHU, Ravi S.; Samarati, Pierangela. Access control: principle and practice. IEEE communications magazine, 1994. ISSN 0163-6804

Segregation of Duties. ISACA Information Systems Audit and Control Association – COBIT Control Objective PO4.11

VOŘÍŠEK, J. Principy a modely řízení podnikové informatiky. Praha: Ekonomica, 2010. ISBN 978-80-245-1440-6

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci Bezpečnostní politika firem v oblasti řízení přístupových oprávnění k informačním systémům jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.3.2019 Bc. Ivona Fúziková _____

Poděkování

Ráda bych touto cestou poděkovala mému vedoucímu panu Ing. Mgr. Vladimíru Očenáškovi, Ph.D. za cenné rady a svojí rodině za podporu.

Bezpečnostní politika firem v oblasti řízení přístupových oprávnění k informačním systémům

Abstrakt

Tato práce se zabývá vytvořením návrhu interní směrnice pojednávající o řízení přístupových oprávnění k informačním systémům v podnicích, který je v souladu s legislativou a respektuje poznatky tzv. „best practice“. V teoretické části práce se nachází výčet legislativy dotýkající se problematiky přístupových práv a popsán vliv této legislativy na obsah interní směrnice. Dále jsou stanoveny významné zásady „best practice“ týkající se přístupových oprávnění. V praktické části je provedeno hodnocení zkoumaných interních směrnic deseti různých podniků z pohledu stanovené legislativy a „best practice“. Na základě tohoto hodnocení a legislativních a „best practice“ požadavků je vytvořen návrh interní směrnice o řízení přístupových oprávnění. Závěrem je vytvořen odhad finančního a personálního zatížení na zavádění navrhnuté interní směrnice.

Klíčová slova: bezpečnostní politika, řízení přístupů, COBIT, ITIL, oddělení povinností, zákon o kybernetické bezpečnosti, GDPR, směrnice, informační systémy

Security policy of companies in the area of information systems´ access rights management

Abstract

This thesis deals with the creation of a draft of an internal guideline dealing with the management of access rights to information systems in companies, which is in compliance with the legislation and respects the knowledge of so-called "best practice". In the theoretical part of the thesis there is a list of legislation related to the issue of access rights and described the impact of this legislation on the content of the internal guideline. In addition, significant “best practice” policies on access privileges are set out. In the practical part there is an evaluation of examined internal guidelines of ten different companies from the point of view of set legislation and "best practice". Based on this assessment and legislative and "best practice" requirements, a draft internal directive on access control is created. Finally, an estimate of the financial and personnel burden on the implementation of the proposed internal guideline is made.

Keywords: security policy, access control, COBIT, ITIL, segregation of duties, law on cyber security, GDPR, guidelines, information systems

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Jedním z významných faktorů, které ovlivňují fungování a bezpečnost informačních systémů je tzv. lidský faktor. Samotní uživatelé systému představují jednu z jeho největších hrozeb. Jak tuto hrozbu minimalizovat řeší manažeři informační bezpečnosti ve všech podnicích. Důraz je kladen především na vzdělanost uživatelů. Cílem procesů kybernetické bezpečnosti v oblasti vzdělávání uživatelů je bezpochyby uvědomělý uživatel, který zná interní pravidla stanovená organizací a dokáže rozpoznat pokusy o vnitřní narušení například v podobě phishingu a dalších podvodných taktik.

Lidský faktor však není možné posuzovat pouze jako slabý článek v obraně proti vnějším útokům. Uživatelé se mohou sami uvnitř bezpečné interní sítě nebo informačního systému stát narušiteli. Důvodů může být hned několik – jedním z nejčastějších je prostá chyba. Systém musí být připravený na chybování uživatele, avšak důležité je chybám předcházet, před omyly uživatele varovat, ale především mu k omylům nedávat prostor. Do druhé pomyslné kategorie narušitelů můžeme zařadit ty uživatele, kteří systému škodí záměrně a úmyslně porušují stanovená interní pravidla nebo dokonce páchají trestnou činnost.

S příchodem zákonu o kybernetické bezpečnosti a také nařízení GDPR se zvýšil důraz na omezování přístupů k datům. Je nutné si však uvědomit, že omezování přístupu uživatelů k určitým částem systémů je také významným nástrojem právě v boji za snížení rizik interního lidského faktoru. Pokud zaměstnanec nemá oprávnění přistupovat k datům, která nutně nepotřebuje k výkonu svojí práce, je tím eliminovaná jeho chybovost právě na těchto zamezených datech. Zamezení používání určitých práv, především těch privilegovaných, v systémech je taktéž dobrým nástrojem předcházení páchání trestné činnosti nebo porušování interních pravidel.

2 Cíl práce a metodika

2.1 Cíl práce

Práce si klade za cíl vytvoření návrhu interní směrnice pojednávající o řízení přístupových oprávnění k informačním systémům v podnicích, který je v souladu s legislativou a respektuje poznatky tzv. „best practice“. V teoretické části práce bude proveden výčet legislativy dotýkající se problematiky přístupových práv a popsán vliv této legislativy na obsah interní směrnice. Následně budou stanoveny významné zásady „best practice“ týkající se přístupových oprávnění. V praktické části bude provedeno studium interních směrnic několika různých organizací. Na základě hodnocení zkoumaných interních směrnic z pohledu stanovené legislativy a „best practice“ z teoretické části práce bude vytvořen vlastní návrh interní směrnice. Na závěr práce bude vytvořen odhad finančního a personálního zatížení na zavádění navrhnuté interní směrnice.

2.2 Metodika

V teoretické části diplomové práce bude identifikována legislativa týkající se problematiky řízení práv. S danou legislativou bude pracováno metodou výkladu práva. V teoretické části budou dále analyzovány poznatky „best practice“ a bude provedena jejich vzájemná komparace. Výsledkem bude specifikace nejvýznamnějších poznatků „best practice“. Na závěr teoretické části bude provedena syntéza legislativních a „best practice“ požadavků k identifikaci stěžejních kritérií interní směrnice.

V praktické části práce budou analyzovány přístupy k řízení přístupových práv z praxe na příkladu anonymizovaných firem. Bude provedeno studium interních směrnic několika různých podniků. Jednotlivé přístupy budou zkoumány z pohledu legislativních požadavků a srovnávány s identifikovanými zásadami „best practice“. Metodou syntézy budou procesy z praxe, označené jako vyhovující z obou pohledů, následně agregovány do návrhu interní směrnice.

3 Teoretická východiska

Tvorba bezpečnostních směrnic, které stanovují pokyny pro řízení provozu informačních systémů, by měla být velmi významnou součástí implementace IS. Jak ovšem zdůrazňuje Vrana a Richta (2005), ve fázi implementace se tvorba bezpečnostních směrnic často zanedbá. Autoři vyzdvihují důležitost ochrany informačního systému hned od prvního dne provozu, čehož může být dosaženo jedině v případě, že uživatelé IS znají řídící pokyny a jsou seznámeni s metodickými směrnicemi.

Bezpečnostní studie, která předchází tvorbě bezpečnostní směrnice, sestává z analýzy dostupnosti informací a dokumentů. Nelze však provádět takovou analýzu bez znalosti rolí koncových uživatelů IS. Role uživatelů mohou být rámcově charakterizovány již v úvodní studii k informačnímu systému, musí ale být v průběhu implementace detailně popsány. Od stanovených rolí se následně odvíjí způsob přiřazování přístupových práv stanovený v bezpečnostní směrnici. (Vrana a Richta, 2005)

I Buchalcevová (2005) při srovnání různých metodik budování IS podtrhuje významnost včasného a správného definování uživatelských rolí. Všechny metody, které Buchalcevová hodnotí (např. Metodika OPEN, metodika RUP, agilní metodika DSDM a další), dokazují, že uživatelské role a z nich plynoucí přístupová oprávnění jsou klíčovým procesem implementace systému, neboť všechny s touto problematikou pracují hned v úvodních procesech a definicích a prvotních studiích.

Agilní metodiky vyzdvihují vliv lidského chování a vlastností lidského charakteru na vývoj softwaru obecně. Mezi nejvýraznější lidské charakteristiky, na které je nutno brát zřetel, patří především:

- jednání člověka je ovlivněno výší odměny,
- lidem jen s obtížemi dodržují stanovené postupy a pravidla,
- lidé chybují,
- lidé konají na základě vlastní iniciativy. (Cockburn, 1995)

Cockburn sice uvedené charakteristiky pak využíval pro stanovení optimálních pracovních postupů vývojářských týmu, bezpochyby je však lze využít i pro demonstraci

chování koncových uživatelů systému. Již charakteristiky samy napovídají, že může velmi snadno dojít k závažným a rozsáhlým problémům, pokud přístup uživatelů do systému a jejich oprávnění vně systému nejsou nijak omezena ani regulována.

Lze tedy konstatovat, že jedním z hlavních důvodů, proč uživatele rozdělovat do různých skupin a přiřazovat jim uživatelské role, je ochrana systému a informací v něm před lidskými chybami a omyly. Existuje však významnější důvod, který motivuje především velké organizace k tomu, aby dbali na správné přiřazování uživatelských rolí. Jak uvádí Gramling (2010), oním důvodem je segregace povinností. Dle této autorky je pro velké organizace klíčové, aby povinnosti vztahující se k jednomu procesu byly mezi zaměstnance rozděleny. Díky tomu lze zabránit zneužití procesu k osobnímu prospěchu a jiným nestandartním praktikám.

Co lze snadno zavést ve velkých organizacích, které jsou často byrokratické a mají jasně stanovené postupy a pravidla, bývá velmi obtížné u malých podniků. I přesto, že povinnosti budou formálně segregovány, v praxi může v malých podnicích snadno dojít k porušování stanovených oprávnění. Důvodem je nejčastěji nízký počet zaměstnanců a z toho plynoucí obtížná zastupitelnost a časté střety vzájemně neslučitelných rolí. (Gramling, 2010)

Clark a Wilson již v roce 1987 uvedli první definici pojmu segregace povinností. Uvedli, že největším úskalím informačních systémů je nutnost, aby uživatelé kontrolovali, zda informace obsažené v systému korespondují s realitou a díky tomu IS co nejvěrněji odrážel skutečnost.

Dle Clarka a Wilsona (1987) by měli být povinnosti segregované tak, že daný uživatel může mít přístup pouze k určitým programům, funkčnostem, transakcím nebo dokumentům. K těm ostatním mu nemá být přístup povolen za žádných standartních okolností.

S tímto tvrzením zcela ostře nesouhlasí Nash a Poland (1990). Domnívají se, že omezení by se neměla vztahovat na funkčnosti či snad celé části programu, ale měla by se vztahovat na procesy. Pokud tedy bude daný dokument součástí procesu, k němuž uživatel

má přidělené své povinnosti, měl by k němu mít přístup bez ohledu na jeho umístění v programu. Revoluční je však jejich druhý přístup k segregaci práv. Dle něj lze povolit uživateli přístup k datům, ačkoliv nejsou součástí žádného procesu, ke kterému se vztahují uživatelovi povinnosti. Jedinou podmínkou je, aby uživatel na datech již neprovedl žádné další úkony v průběhu celého procesu zpracování těchto dat.

Přístupy k segregaci povinností lze tedy obecně rozdělit na dva různé přístupy – statické rozdělení povinností zastávané Clarkem a Wilsonem a dynamické rozdělení povinností zastávané Nashe a Polandem. (Nash a Poland, 1990)

Na obě teorie navázalo několik autorů a dále podrobněji rozváděli, způsoby, kterými by měly být oba způsoby uváděni v praxi. Jeden z nejvýznamnějších byl Lee (1989), který stanovil, že kontroly autorizace a povinností by měli být stanoveny dle rolí, které uživatel v systému má. Jeho metodika pracovala čistě se statickým rozdělením, neboť každému uživateli má být přiřazen jakýsi štítek (label). Na jeho základě je pak snadné rozčlenit všechny uživatele do kategorií, které v sobě integrují vždy jednu úroveň schvalování a kontroly dat. Každá kategorie zároveň odpovídá jednomu stupni v organizační struktuře podniku.

Chybu v této teorii objevil velmi záhy Shockley (1991). Metodika štítků má totiž za následek, že určitý okruh zaměstnanců bude zcela odříznut od některé části systému nebo nebude mít vůbec přístup k některým programovým funkčnostem. Shockleyho přístup byl v kontrastu s Leeho dynamický. Doporučoval definovat role, jež se vzájemně vylučují, jelikož jsou ve vzájemném konfliktu. Kontrolní mechanismus tak nebude zabraňovat uživateli v přístupu, ale ve vykonání určité akce v závislosti na tom, zda je či není v konfliktu s jinou uživatelovou povinností.

Definováním vzájemně se vylučujících rolí, akcí a povinností vznikne matice známá pod anglickým pojmem Segregation of Duties matrix – zkráceně jen SoD, tedy matice oddělených povinností/úkolů. SoD je tedy schéma rolí, které prvky uvnitř matice vyjadřují, zda dvě určité role mohou být vykonávány současně či jsou ve vzájemném konfliktu. Odvětvím, kde se s SoD začalo pracovat nejdříve a je v současnosti nejvíce využívané, je bankovnictví a účetnictví. (Behr a Coleman, 2017)

Obdobnou definici lze nalézt i v glosáři ISACA (Information systems audit and control association) – nezisková mezinárodní asociace v poskytující odborné vzdělání pro profesionály z oblastí auditu a IT. ISACA definuje SoD jako základní interní kontrolu, která zabraňuje nebo dokonce odhaluje pochybení a abnormality tím, že samostatným jedincům přiřazuje odpovědnosti za transakce. (ISACA journal, 2017)

Nejjednodušší a nejlépe názorný příklad SoD je proces zpracování přijaté faktury. Ve zjednodušeném modelu tohoto procesu existují tři zaměstnanci - uživatelé informačního systému. První uživatel je úředník back office, který přijímá fakturu ve fyzické papírové podobě a nahrává ji do informačního systému. Dalším uživatelem je pracovník účtárny, který kontroluje (ať už s pomocí automatizované kontroly v systému nebo ručně), zda faktura v systému souhlasí s objednávkou, výdejkou, dodacím listem a dalšími zásadními dokumenty. Posledním uživatelem završujícím celý proces je nadřízený či vedoucí oddělení, který schválí proplacení přijaté faktury zadané pracovníkem účtárny.

Dle výše zmíněných metodik a definic je tedy nutné zabránit tomu, aby všechny tři části zmíněného procesu provedla jedna jediná osoba. Všichni tři uživatelé totiž vykonávají v rámci procesu role, které nejsou vzájemně slučitelné. Nelze nechat zaměstnance schválit svůj vlastní úkon. V extrémním případě by totiž procesem mohla projít faktura, která by byla ve všech fázích schvalována jedinou osobou, která by tak mohla nechat proplatit podvodnou fakturu, neboť by zde neexistovala žádná kontrola.

Dalším významným odvětvím kromě bankovnictví a účetnictvím, ve kterém se SoD hojně využívá, je v oblasti informačních technologií, především ve velkých organizacích. Zde je za největší potenciální riziko považováno nasazení kódu, který je podvodný nebo má za cíl úmyslně škodit. (ISACA journal, 2017)

Největší pozornost SoD je však stále věnována v bankovnictví. V tomto odvětví se totiž vyskytuje nejvíce procesů a transakcí, které je nutné oddělit a definovat vzájemně konfliktní role. Tato potřeba nevychází pouze ze snahy zamezit podvodům a nekalým jednání, ale také z požadavků interního auditu a externího auditu.

Interní audit potřebuje efektivní nástroj, díky němuž může provádět kontroly toho, zda nedochází k překračování přidělených oprávnění a nevzniká někde v procesu prostor pro potenciální podvod. Zároveň externí audit potřebuje důkaz o tom, že role jsou rozděleny a existuje kontrolní mechanismus. Ani interní a ani externí audit nemůže kontrolovat každou jednu transakci (či náhodné vzorky) ručně a proto potřebují jednoznačný vzor, dle kterého lze jasně a rychle kontrolu provést. Největší potenciál se pak skrývá v automatizaci dozoru nad SoD. (Lightle a Vallario, 2003)

Zájem interních i externích auditorů na dodržování správně definovaného SoD vychází především z legislativních požadavků. Momentálně nejaktuálnější z nich je Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které je zpopularizováno pod zkratkou anglického názvů tohoto nařízení General Data Protection Regulation – GDPR. Od května 2018 musí být podniky, na které se GDPR vztahuje, v souladu s požadavky tohoto nařízení. Jedním ze základních kamenů GDPR je přístup k osobním datům, respektive kontrola a omezení těchto přístupů.

V článku 49 zmiňovaného nařízení GDPR se mluví o tom, že informační systémy musí být připraveny na to, aby dokázaly „odolávat na dané úrovni spolehlivosti, náhodným událostem nebo protiprávnímu či zlovolnému jednání ohrožujícímu dostupnost, pravost, správnost a důvěrnost uložených či předávaných osobních údajů“ (GDPR, 2016). Článek také říká, že v ohrožení nemusí být jen samotná data, ale také služby, které jsou poskytovány těmito informačními systémy. Služby souvisí s činnostmi prováděnými „orgány veřejné moci, skupiny pro reakci na počítačové hrozby (CERT), skupiny pro reakci na incidenty v oblasti počítačové bezpečnosti (CSIRT), poskytovatelé elektronických komunikačních sítí a služeb a poskytovatelé bezpečnostních technologií a služeb“ (GDPR, 2016).

Nejvýznamnější bod z celého článku 49 je však konstatování o oprávněném zájmu. Přesněji, že zajištění odolnosti IS proti událostem, které nařízení popisuje, a zajištění bezpečnosti služeb, které jsou v něm vyjmenované, „představuje oprávněný zájem dotčeného správce údajů“ (GDPR, 2016). GDPR udává i příklad onoho oprávněného zájmu:

„Oprávněný zájem by například mohl spočívat v zabránění neoprávněnému přístupu k sítím elektronických komunikací a šíření škodlivých kódů a zamezení útokům, jejichž důsledkem je odepření služby, a škodám na počítačových systémech a systémech elektronických komunikací.“ (GDPR, 2016).

Z článku 49 tedy jasně vyplývá, že pokud chce být zpracovatel osobních údajů v souladu s GDPR a chce vyhovět jeho nárokům, musí zajistit, aby jeho informační systémy byly schopné čelit a odolat možným protiprávním jednáním. SoD a udělování přístupových práv je pro zajištění této odolnosti výborným podpůrným nástrojem, jak se domnívá Nilsson (2018). Nejlepším prostředkem, jak zabránit protiprávnímu jednání spáchanému na firemním informačním systému, je nedat osobám – potenciálním škoditelům systému – vůbec přístup k němu či datům v něm ukrytých. Správně definovaná, funkční a pravidelně kontrolovaná přístupová oprávnění podle něj dokáže zabránit úmyslnému poškození systému nebo dat. Nilsson navrhuje tři kroky, díky nimž přístupová práva ochrání systém před hrozbami:

- důkladně zkontrolovat administrátorská oprávnění a přiřazené role v SoD,
- zrychlit proces poskytnutí přístupových práv a zařazení zaměstnance do skupiny v SoD matici a především zrychlit proces odebírání těchto práv pro zabránění přístupu bývalých zaměstnanců do systému,
- posílit proces autentizace uživatele, například silnější politikou hesel. (Nilsson, 2018)

3.1 Legislativa ČR dotýkající se problematiky řízení přístupových práv

Bezpečnostní politika je pojem, který může nabývat mnoha významů v závislosti na tom, v jaké oblasti lidské činnosti je použit. Pojetí bezpečnostní politiky lze chápat jako velmi širokou a komplexní oblast bezpečnosti státu, obrany státní suverenity, zachování míru nebo stanovení postupů při krizi či ohrožení konfliktem. Do této velké skupiny vztahující se k bezpečnosti země je možno zařadit také oblasti jaderné, energetické nebo kybernetické bezpečnosti.

Kybernetická bezpečnost bude bezpochyby předmětem zkoumání této diplomové práce, avšak ne z pohledu mezinárodních organizací či vnitřní politiky státu, nýbrž z pohledu vnitřních metodik podniku, které se promítají do vnitropodnikových směrnic.

Jelikož je téma bezpečnostní politiky natolik multidisciplinárním předmětem, je nutné na samotném začátku uvést význam některých základních pojmů. Jejich vymezení je nezbytné pro zakotvení těchto pojmů do kontextu vnitropodnikových směrnic.

Prvním a nejvíce obecným termínem je bezpečnost. Zeman (2002) definuje bezpečnost jako stav, ve kterém jsou rizika ohrožující daný objekt eliminována na nejnižší možnou úroveň. Definice je dále rozváděna a upřesňuje, že hrozby nemusí působit pouze na konkrétní objekt, ale i na jeho zájmy. Stavu bezpečnosti lze dosáhnout jedině za předpokladu, že je objekt efektivně vybavený k odstranění hrozeb nejen těch bezprostředně hrozících, ale i těch potenciálních.

Zeman (2002) dále rozlišuje bezpečnost na základě toho, kde vznikají hrozby působící na objekt – zdali uvnitř či vně objektu. Pokud hrozba, kterou je nutno potlačit, vzniká vně objektu, jedná se o bezpečnost vnější. Pokud hrozba vzniká uvnitř objektu, mluví se o bezpečnosti vnitřní. Předmětem práce je zkoumání přístupových práv do systémů podniku. Přístupová práva jsou udělována subjektům (zaměstnancům) nacházejících se uvnitř podniku. Zaměstnanci přistupují do systému z vnitřního prostředí podniku, proto

můžeme tvrdit, že zkoumaná problematika se řadí do kategorie vnitřní bezpečnosti. Při zmínce prostředí podniku je vhodné jej definovat i s rozlišením vnějšího a vnitřního prostoru.

Jeden z nejrozšířenějších a nejvíce používaných konceptů, které formulují základní požadavky na bezpečnost nejen podnikových informačních systémů je takzvaná triáda „CIA“. Tento název je zkratkou skládající se ze tří anglických slov Confidentiality (důvěrnost), Integrity (integrita) a Availability (dostupnost). Jak vysvětluje například Bosworth (2002), první zásada Confidentiality (důvěrnost) znamená především zabránit přístupu k informačním systémům podniku (a potažmo k informacím, které obsahují) takovým osobám, které nejsou pověřeny či přímo autorizovány. Tuto první zásadu lze poměrně snadno ošetřit autentizací přístupů, která může navíc být spojená se šifrováním.

Druhá zásada, Integrity (integrita), je Bosworthem (2002) chápána jako neschopnost provést změnu v datech bez potřebné autorizace a pověření. Poslední zásada klade důraz na to, aby přes všechna opatření vztahující se k zabezpečení systému byla data autorizovaným osobám vždy přístupná. Bosworth (2002) však zdůrazňuje, že tyto tři zásady nejsou dostačující. Triáda „CIA“ podle něj chrání pouze počítačové systémy a podnikové síťové systémy, avšak nedostatečně ochraňuje samotné uplatnění a využití počítačů a počítačových sítí. Navrhuje rozšířit počet zásad na šest, které budou efektivně působit na ochranu informací. Bezpečnostními prvky jsou:

- availability (dostupnost),
- utility (užitek),
- integrity (integrita),
- authenticity (pravost),
- confidentiality (důvěrnost) a
- possession (vlastnictví).

Na základě těchto bezpečnostních prvků jasně vyplývá, že udělování, kontrola a důsledné odebírání přístupových práv osob do informačních systémů je jednou z nejdůležitějších činností v rámci informační bezpečnostní politiky. Neoprávněný přístup

do systému totiž může významně ohrozit všech šest uvedených prvků. Neautentizovaný přístup do systému může způsobit nedostupnost systému (například kompletní odstavení či porušení systému), zásahem do systémových dat či jejich změnou dojde nejen k poruše integrity, ale také k velmi pravděpodobnému znemožnění správného užití systému a tím k ohrožení prvku utility (užitek). Na změnu dat se samozřejmě váže i prvek pravosti. Samotným neautorizovaným přístupem do systému je ohrožením prvku důvěrnosti. V neposlední řadě jsou data ohrožena zcizením a tím je narušen poslední bezpečnostní prvek vlastnictví.

3.1.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti zařazuje Stupka (2018) do kategorie využití právní metody nazývané jako realistická (nebo také pragmatická). Realistickou metodu hodnotí pro využití u kybernetické bezpečnosti jako nejvhodnější, neboť pomocí této metody jsou tvořena pravidla, která svojí formulací bere v úvahu omezení, která na oblast působí. Limitem mohou být ekonomické, technické nebo komunikační faktory.

Výhodou využití této metody je stanovení závazných požadavků a především definování právní metodologie. Zároveň se při využití realistické metody počítá se spoluprací se soukromými subjekty. Cílem je regulace pouze těch částí informační infrastruktury, která je považována za bezpečnostně významnou. Stát tedy neodmítá svoji odpovědnost za kybernetický prostor, nýbrž zakládá procesy spolupráce s definičními autoritami, kterým zároveň ponechává rozsáhlý prostor k vlastnímu rozhodování a uznává je jako často nejschopnější v otázce řešení vlastních bezpečnostních incidentů. Mohou totiž nastat situace, kdy se povaha kybernetického útoku změní natolik dynamicky, že legislativa nebude schopna dostatečně rychle reagovat a nebude tak schopna poskytnout základ pro odpovídající reakci. V tomto případě pak bude velmi výhodná a nadmíru žádoucí spolupráce se soukromými subjekty, které budou moci reagovat odpovídajícím způsobem. (Stupka, 2018)

Jedním z prvních dokumentů, který si kladl za cíl zlepšení řízení informačních rizik, byl strategický dokument z roku 2005 vytvořený na základě zákona č. 365/2000 Sb. o informačních systémech veřejné správy, s názvem Národní strategie informační bezpečnosti České republiky. Mezi cíli, které si strategie stanovila, byly například následující body:

- zavést nejlepší praxi „best practice“ do systémů řízení informační bezpečnosti,
- soustavně monitorovat hrozby,
- realizovat systém včasného varování a reakce,
- monitorovat účinnost navržených protiopatření,
- zlepšit informační bezpečnosti orgánů veřejné správy,
- ochránit kritické informační infrastruktury státu,
- zvyšovat povědomí o informační bezpečnosti, bezpečnostních rizicích i u subjektů komerční sféry,
- zavést školicí a vzdělávací programy,
- podpořit celkový program národního povědomí o informační bezpečnosti,
- zvýšit efektivnost školicích programů a
- zvýšit povědomí uživatelů o důležitosti užívání bezpečnostně certifikovaných výrobků a služeb z oboru informačních a komunikačních technologií. (MIČR, 2005)

Bohužel mnoho z výše zmíněných cílů nebylo naplněno, a to především z důvodu nekoncepčnosti při jejich tvorbě a také z důvodu následného zániku Ministerstva informatiky v polovině roku 2007, což vedlo k nedodržení naplnění cílů.

Oblast týkající se kybernetiky byla následně převedena do správy Ministerstva vnitra České republiky. Ministerstvo vnitra ustanovilo Meziresortní radu pro oblast kybernetické bezpečnosti. Bohužel ani tato Rada nedokázala v problematice kybernetické bezpečnosti přijít s potřebnými kroky a naplnit tak stanovené cíle, které byly na začátku jejího fungování stanovený a v mnohém se podobaly cílům Národní strategie informační bezpečnosti České republiky. Otázky kybernetické bezpečnosti totiž byly krátce po ustanovení Rady převedeny pod správu Národního bezpečnostního úřadu. Toto se ukázalo jako zásadní milník ve tvorbě

legislativy, neboť v první polovině roku 2012 byl vytvořen návrh zákona o kybernetické bezpečnosti. (NÚKIB, 2012)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti platný od 29. srpna 2014 nabyl účinnosti 1. ledna 2015. Následně tento zákon upravili dvě novelizace. Aktuální znění zákona je účinné od 7. března 2018. (NÚKIB, 2018a)

Povinné osoby

Zákon o kybernetické bezpečnosti stanovuje, kdo jsou povinné osoby, na které jsou kladeny povinnosti vyplývající ze zákona. Povinnými osobami jsou:

- poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací,
- významné sítě,
- kritická informační infrastruktura (KII),
- významné informační systémy (VIS),
- provozovatelé základních služeb (PZS),
- poskytovatelé digitálních služeb. (NÚKIB, 2018a)

Vliv zákona na přístupová oprávnění

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti zmiňuje hned v úvodu, konkrétně v §5, bezpečnostní opatření, která musí povinné osoby splnit. Tato bezpečnostní opatření jsou rozdělena na dvě části – na část organizačních a část technických opatření. V §5 čl. 2 pojednávajícím o organizačních opatření je v písmenu i) zmíněna povinnost řídit přístup osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému. V §5 čl. 3, který stanovuje technická opatření, je v písmeně c) daná nutnost existence nástroje pro ověřování identity uživatele. S tímto písmenem pak zásadně souvisí i zmiňovaný bod z organizačních opatření a logicky tak ústí v požadavek zákonodárce v písmeně d). Zde je ustanovena povinnost organizace mít nástroje pro řízení přístupových oprávnění. Ustanovení

v §5 čl. 3 písm. d) tedy lze považovat za část zákona o kybernetické bezpečnosti, která má největší význam pro oblast řízení přístupových ustanovení. (Zákon č. 181/2014 Sb.)

3.1.2 Vyhláška o kybernetické bezpečnosti

K Zákonu o kybernetické bezpečnosti se bezpochyby neodmyslitelně pojí vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. Tato vyhláška vstoupila v platnost 27. května 2018 a novelizovala tak svoji předchůdkyni vyhlášku č. 316/2014 Sb., o kybernetické bezpečnosti z roku 2014. Vyhláška o kybernetické bezpečnosti v sobě reflektuje především tzv. směrnici NIS, tedy Směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Novelizace vyhlášky následně upřesnila některé nedostatečné body a především nastínila možnosti z praxe, jak eliminovat hrozby. Součástí vyhlášky je například i praktický vzor smlouvy s dodavatelem IT. (Vyhláška č. 82/2018 Sb.)

Ve vyhlášce je v §12 dále rozvedeno ustanovení v §5 čl. 3 písm. d Zákona o kybernetické bezpečnosti. V §12 se nachází výčet bodů, které do praxe stanovují praktické úlohy, díky nimž budou požadavky z §5 Zákona o kybernetické bezpečnosti splněny. Dle §12 povinné osobě ustanovuje následující:

a) řídí přístup na základě skupin a rolí,
b) přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor,
c) řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů,
d) zavádí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému,
e) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě,
f) omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,

g) omezí a kontroluje používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly,
h) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,
i) provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,
j) využívá nástroj pro správu a ověřování identity podle § 19 a nástroj pro řízení přístupových oprávnění podle § 20,
k) prosazuje, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy,
l) zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role,
m) zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a
n) dokumentuje přidělování a odebírání přístupových oprávnění. (Vyhláška č. 82/2018 Sb.)

V §20 je dále stanoveno, že pro řízení přístupových práv má povinná osoba používat centralizovaný nástroj.

K Vyhlášce o kybernetické bezpečnosti existuje několik podpůrných materiálů. Jedním z nich je Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. Tato pomůcka představuje tabulku ve formátu MS Office Excel, která má soužit jako checklist pro interního auditora. Po zkontrolování všech bodů v tabulce, které přesně kopírují jednotlivé požadavky předložené ve Vyhlášce, je tak zajištěno, že byly interním auditorem zkontrolovány všechny body, které vyplývají z Vyhlášky o kybernetické bezpečnosti. Z rozsáhlé tabulky, která má téměř 900 položek, je zde vybrán pouze zlomek, který se vztahuje k problematice přístupových práv.

#	Zdroj	§	Název §	úroveň členění				Text §	Relevantní pro		
				1	2	3	4		KII, ISZS	VIS	DSP
428	*VKB*	**§ 12**	**Řízení přístupu**	**1**				Povinná osoba na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu a komunikačnímu systému a přijímá opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení podle § 19 a 20, a která brání ve zneužití těchto údajů neoprávněnou osobou.	**v**	**v**	
429	*VKB*	**§ 12**	**Řízení přístupu**	**2**				Povinná osoba dále v rámci řízení přístupu k informačnímu a komunikačnímu systému	-	-	
430	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**a**			řídí přístup na základě skupin a rolí,	**v**	**v**	
431	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**b**			přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor,	**v**	**v**	
432	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**c**			řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů,	**v**	**v**	
433	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**d**			zavádí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému,	**v**	**v**	
434	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**e**			zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě,	**v**	**v**	

435	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**f**			omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,	**√**	**√**	
436	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**g**			omezí a kontroluje používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly,	**√**	**√**	
437	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**h**			přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,	**√**	**√**	
438	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**i**			provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,	**√**	**√**	
439	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**j**			využívá nástroj pro správu a ověřování identity podle § 19 a nástroj pro řízení přístupových oprávnění podle § 20,	**√**	**√**	
440	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**k**			prosazuje, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy,	**√**	**√**	
441	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**l**			zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role,	**√**	**√**	
442	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**m**			zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a	**√**	**√**	
443	*VKB*	**§ 12**	**Řízení přístupu**	**2**	**n**			dokumentuje přidělování a odebírání přístupových oprávnění.	**√**	**√**	

529	*VKB*	**§ 20**	**Řízení přístupových oprávnění**					Povinná osoba používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění	-	-	
530	*VKB*	**§ 20**	**Řízení přístupových oprávnění**	**a**				pro přístup k jednotlivým aktivům informačního a komunikačního systému a	**√**	**√**	
531	*VKB*	**§ 20**	**Řízení přístupových oprávnění**	**b**				pro čtení dat, zápis dat a změnu oprávnění.	**√**	**√**	

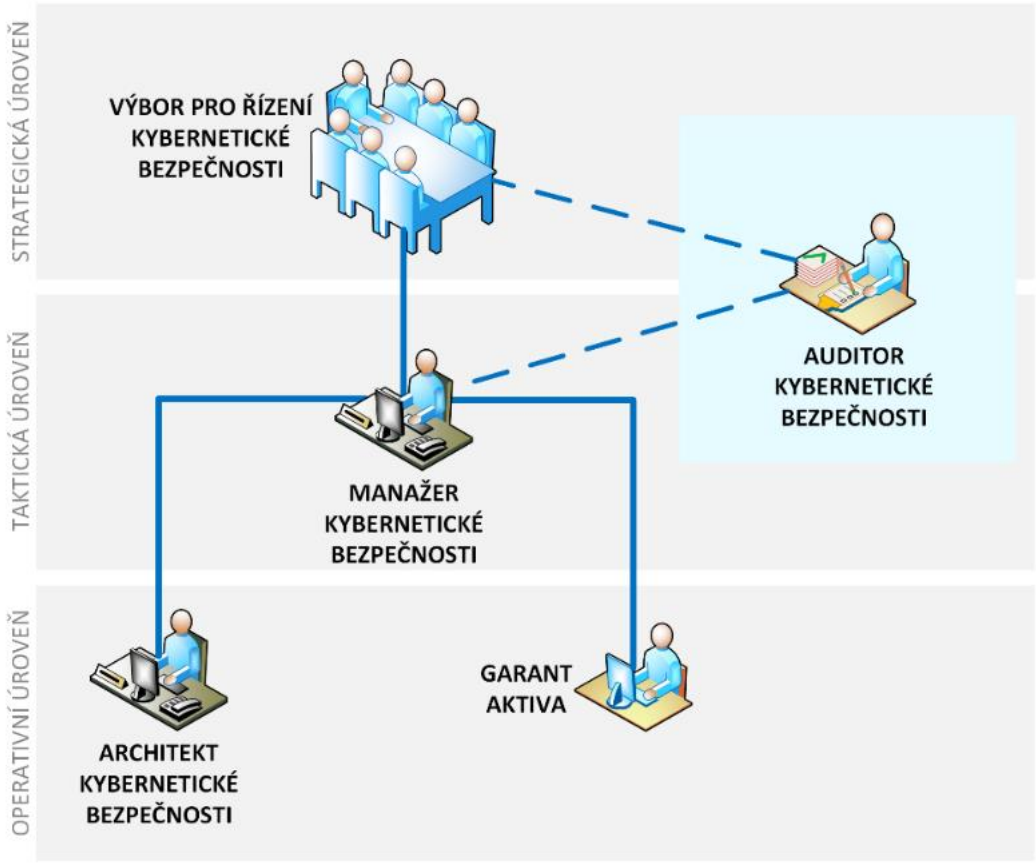
Tabulka 1 - Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.

Zdroj: NÚKIB,2018b

K Vyhlášce o kybernetické bezpečnosti byla Národním centrem pro kybernetickou bezpečnost vydaná pomocná metodika, která se zabývá bezpečnostními rolemi. Dokument především zdůrazňuje nutnost oddělení Výboru pro řízení kybernetické bezpečnosti (a obecně celého útvaru, zabývajícího se bezpečností ICT) od útvaru, který zajišťuje samotný chod a provoz ICT. Základními rolemi jsou:
manažer kybernetické bezpečnosti,

- architekt kybernetické bezpečnosti,
- auditor kybernetické bezpečnosti,
- garant aktiva a
- role ve výboru KB. (NÚKIB, 2018b)

Rozdělení bezpečnostních rolí přehledně ukazuje názorný obrázek hierarchie rolí.



Obrázek 1 - Hierarchie bezpečnostních rolí

Zdroj: NÚKIB, 2018b

Specifickou rolí z výše uvedených je role auditora, která se od ostatních odlišuje tím, že musí být zcela nezávislá. Role se mohou vzájemně překrývat nebo mohou dokonce splývat

v povinnostech jediné osoby, avšak role auditora je neslučitelná s jakoukoliv jinou rolí. Výše zmíněné role může vykonávat i externista.

V rámci zajištění kybernetické bezpečnosti jsou v metodice nastíněny základní procesy, které jsou vloženy do tabulky, ve které dochází k jejich propojení s bezpečnostními rolemi. Tím vzniká matice, která definuje vztah jednotlivých procesů a rolí. Tento vztah je popisován následujícími písmeny:

- R (Responsible) – fyzická zodpovědnost
- A (Accountable) – právní odpovědnost
- C (Consluted) – konzultační nebo spolupracující role
- I (Informed) – informovanost

Výsledná matice, která se dle názvů vzájemných vztahů nazývá RACI, má následující podobu:

Procesy:	Role:	Výbor KB	Manažer KB	Architekt KB	Auditor KB	Garant (vlastník) aktiva
Celkové řízení a rozvoj KB		A	R	R		C
Systém řízení bezpečnosti informací		A	R	C		C
Návrh bezpečnostních opatření		C	A	R		C
Implementace bezpečnostních opatření		C	A	R		C
Zajištění rozvoje, použití a bezpečnosti aktiva			A	C		R
Audit KB		I	C	C	A/R	C

Tabulka 2 - RACI matice

Zdroj: NÚKIB, 2018b

3.2 Legislativa EU a třetích zemí dotýkající se problematiky řízení přístupových práv

3.2.1 Obecné nařízení o ochraně osobních údajů

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) vešlo do obecného povědomí především pod názvem GDPR. Tato zkratka, která je i v českých odborných kruzích používána v anglické výslovnosti, vyplývá z anglického názvu nařízení General Data Protection Regulation.

Nařízení ovlivňuje zacházení s osobními údaji na území Evropské unie a posiluje práva osob na ochranu proti neoprávněnému zacházení s jejich osobními údaji. Důležitou součástí Nařízení je také právo osob být informován o zpracování svých osobních údajů a o důvodu tohoto zpracování. V Nařízení je také kladen důraz na vymahatelnost práv osob. Tu zajišťuje významnou částí celého Nařízení, kterou je stanovení povinností pro správce a zpracovatele osobních údajů.

Osobními údaji jsou takové informace, které se vztahují k identifikované nebo identifikovatelné fyzické osobě. V Nařízení nejsou taxativně uvedeno, jaké informace mohou vést k identifikaci nebo identifikovatelnosti, avšak mnoho autorů, jako například Škorničková (2018) výkladem Nařízení a především zkušeností z praxe uvádí následující:

- IP adresy,
- fotografické záznamy,
- genetické informace, analýzy biologických vzorků
- osobní údaje dětí,
- biometrické údaje,
- údaje o rasovém či etnickém původu,
- údaje o politických názorech,
- údaje o náboženském nebo filozofickém vyznání,
- členství v odborech,

- zdravotní stavu,
- sexuální orientace,
- trestních delikty nebo pravomocné odsouzení.

Z působnosti GDPR jsou však vyloučeny takové údaje, které jsou anonymizované – tedy nelze bez jedinečného identifikátoru přiřadit dané informace ke konkrétní osobě. Dále se vyloučení týká údajů zemřelých osob a v poslední řadě údajů, které jsou zpracovávané pro osobní potřebu v případě, že nebudou sdílené jiným osobám. (Škorničková, 2018)

Vliv nařízení na přístupová oprávnění

Nejvýznamnější částí Obecného nařízení o ochraně osobních údajů v souvislosti s přístupovými právy osob do systémů je oddíl 2 článek 32. V něm je uvedeno, že by měly být osobní údaje zpracovány takovým způsobem, aby byla zaručena jejich bezpečnost a důvěrnost. Článek 32 stanovuje, že má být zabráněno neoprávněnému přístupu k osobním údajům a také k zařízení, které je používáno pro jejich zpracování či neoprávněnému použití. (GDPR, 2018)

V článku 32 se také správci nebo zpracovateli osobních údajů ukládá povinnost posoudit rizika, která se pojí se zpracováním osobních údajů. Jedním z rizik, které je nutné posoudit, je i riziko neoprávněného přístupu či riziko zničení, ztráty nebo pozměnění osobních údajů. (GDPR, 2018)

3.2.2 ISO 29146:2016 – A Framework for access management

ISO 29146:2016 definuje a vytváří rámec pro řízení přístupu a bezpečnou správu procesu přístupu k informacím a zdrojům informačních a komunikačních technologií a v tomto kontextu dále spojeným s určitou zodpovědností subjektu.

Tato mezinárodní norma poskytuje koncepci, pojmy a definice, které mohou být použitelné pro techniky distribuovaného přístupu v prostředí sítě. Norma ISO 29146 (2016) také vysvětluje souvislosti mezi logickým a fyzickým přístupem, architekturu přístupového systému a jeho samotnou správu. Tato mezinárodní norma však nemá ve svém obsahu žádná pojednání o povaze nebo kvalitě fyzické kontroly přístupů.

Jedním z podstatných bodů normy je princip označovaný anglickým názvem „need-to-know“. Tento princip se zakládá na metodice, která stanovuje, že každý subjekt by měl mít přístup ke zdrojům dat pouze v takové míře, která je minimálně nezbytná pro vykonávání funkcí daného uživatele. (ISO 29146, 2016)

Norma také vysvětluje dva základní pojmy, kterými jsou oprávnění a role. Oprávnění je určeno rozsahem možných akcí, které může uživatel v systému provést. Oprávnění je nezbytnou, avšak ne dostatečnou podmínkou a předpokladem pro přístup. Přístup je totiž společně s oprávněním určován ještě rolí. Role je systémem úloh, které mohou být uživatelem vykonány. Tento systém úloh se skládá z jednotlivých oprávnění, proto jedině dohromady tvoří tyto dvě charakteristiky základní systém přístupového systému. (ISO 29146, 2016)

3.2.3 Bezpečnostní pokyny pro zařízení koncového uživatele

Ve Velké Británii vydalo Národní centrum kybernetické bezpečnosti (NCSC), které je součástí Vládního komunikačního ústředí Velké Británie (GCHQ), příručku Bezpečnostní pokyny pro zařízení koncového uživatele. Tato příručka se skládá z několika částí, z nichž nejvýznamnější část týkající se přístupových oprávnění, je oblast Řízení privilegovaných oprávnění. NCSC se zde zabývá možností, že může dojít k nedodržení zásady „need-to-know“ a uživatelé mají přidělena nadbytečná oprávnění. Všichni uživatelé by měli mít pouze minimální (avšak v rozsahu rozumné míry) oprávnění potřebné k jejich roli. Tento princip je nazýván rozšířeným anglickým pojmem „least privilege“. (End user devices security guidance, 2016)

V deseti bodech je v příručce uvedeno, jak zvládnout potenciální riziko, pokud není výše zmíněný princi „least privilege“ dodržen. Rizika lze snížit nebo jim předejít pokud organizace podnikne následující kroky:

- Vytvoření efektivních procesů správy účtů

  Uživatelské účty mají být spravovány od jejich vytvoření po celou dobu životnosti a případně odstranění, když zaměstnanec opustí nebo změní roli. Redundantní

účty, které mohou být poskytnuty dočasným zaměstnancům nebo testovány, by měly být odstraněny nebo pozastaveny, pokud již nejsou požadovány.

- Vytvoření zásad a standardů pro autentizaci uživatelů a kontrolu přístupu

  Měla by být vytvořena politika firemních hesel, která by usilovala o účinnou rovnováhu mezi bezpečností a použitelností. NCSC v příručce dále rozvádí pokyny pro bezpečné heslo. Pro některé účty pak může být vhodný další faktor ověřování (například token).

- Omezení uživatelských práv

  Uživatelům by měly být poskytnuty přiměřené minimální práva a oprávnění k systémům, službám a informacím, které potřebují k plnění své obchodní role v rámci principu „least privilege“.

- Omezení počtu a použití privilegovaných účtů

  Dle příručky je nutné přísně kontrolovat udělování vysoce privilegovaných systémových práv a pravidelně kontrolovat ty, kteří již taková práva mají udělena. Vysoce privilegované účty správců by neměly být používány pro vysoce rizikové nebo každodenní činnosti uživatelů, například prohlížení webu a e-mail. Administrátoři by měli používat standardní účty pro standardní obchodní účely.

- Monitorovat aktivitu uživatele

  Monitorována by měla být aktivita každého uživatele a zejména přístup k citlivým informacím a použití privilegovaných účtů. Pokud jsou aktivity mimo normální očekávané hranice, jako například přístup k velkému množství citlivých informací mimo standardní pracovní dobu, musí být provedeny odpovídající kroky.

- Omezení přístupu k auditorskému systému a protokolům o činnosti systému

Záznamy o činnosti na síťových zařízení by měly být zasílány do specializovaného systému účetnictví a auditu, který je oddělen od jádrové sítě. Přístup k auditorskému systému a protokolům by měl být přísně kontrolován, aby se zachovala integrita obsahu a zaznamenaný přístup všech uživatelských privilegií.

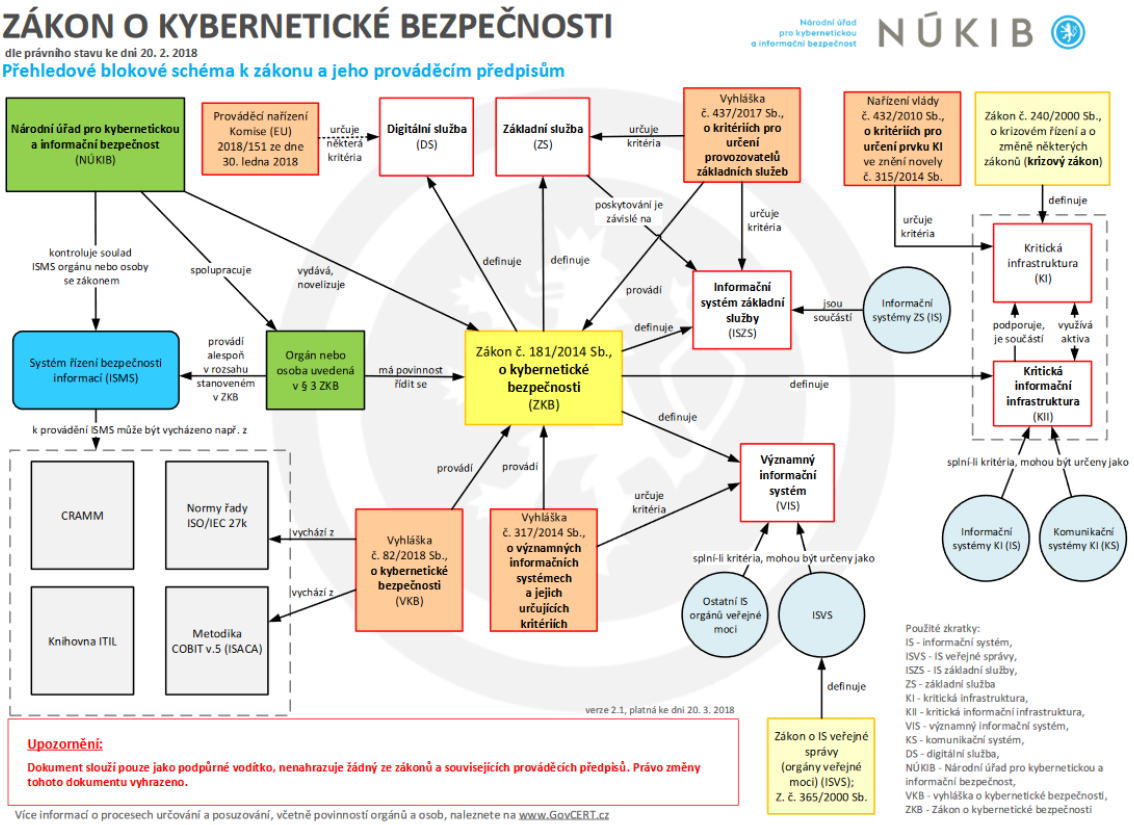
- Vzdělávání uživatelů

Všichni uživatelé by si měli být vědomi zásad ohledně přijatelného používání účtu a osobní odpovědnosti za dodržování zásad firemní bezpečnosti. Nutné je také jejich povědomí stále udržovat a zpřístupňovat uživatelům nové informace. (End user devices security guidance, 2016)

3.3 Best practice (COBIT, ITIL a další)

Jak lze vidět na schématu níže, zákon o kybernetické bezpečnosti není jediným zdrojem informací a metodiky v oblasti bezpečnosti ICT. Na schématu je dokonce vidět, že samotná Vyhláška o kybernetické bezpečnosti vychází ze dvou metodiky COBIT. Schéma tedy dokazuje, že COBIT i ITIL mají velký vliv na procesy informačních technologií

A jistě není třeba zdůrazňovat, že jejich využití přispívá k optimalizaci správy a řízení informačních a telekomunikačních technologií.



Obrázek 2 - Schéma k zákonu o kybernetické bezpečnosti

Zdroj: NÚKIB, 2018b

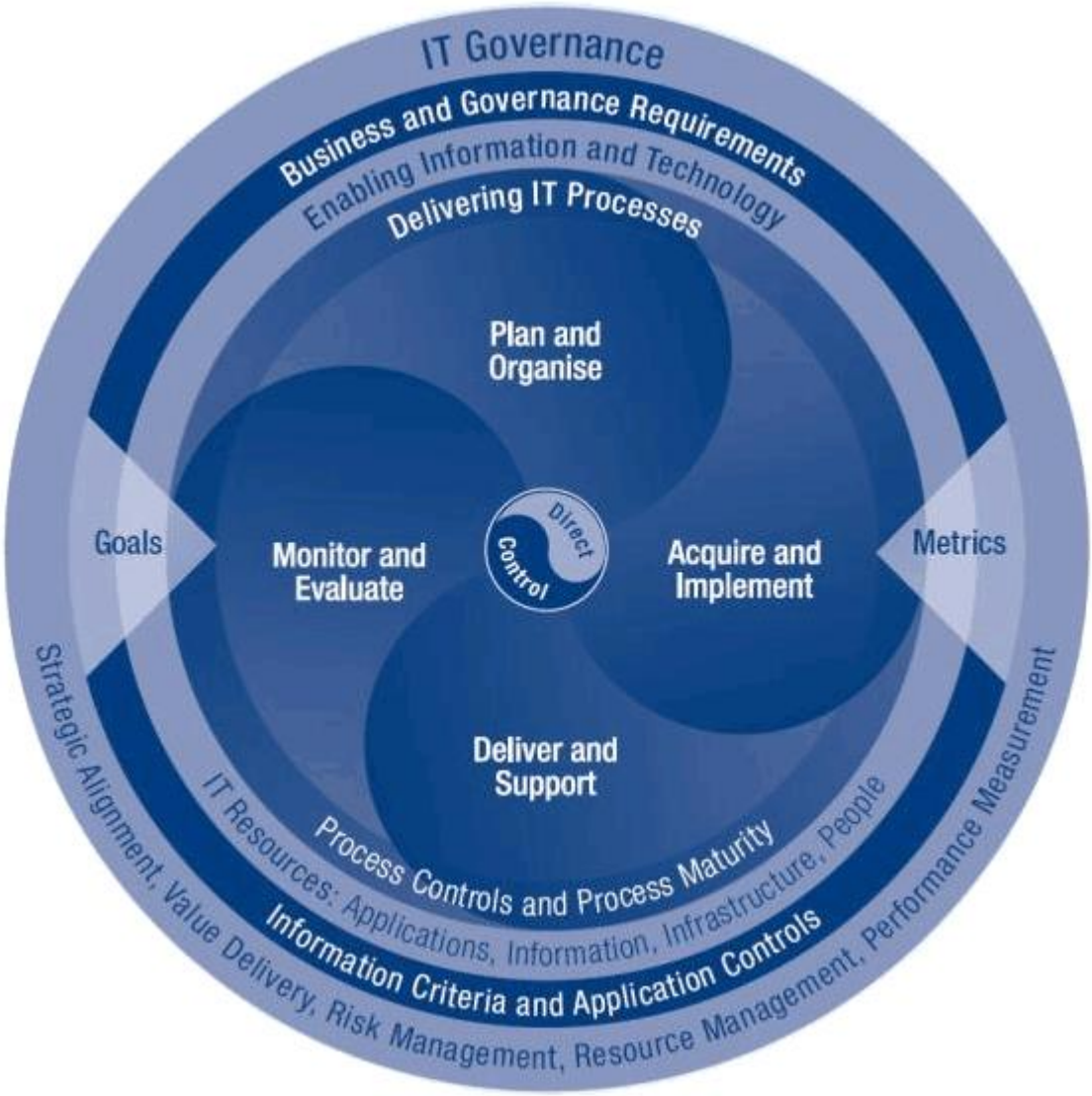
Aby využití obou metodologií mohlo být úspěšné, je třeba je správně implementovat na základě specifik konkrétního podniku a přizpůsobit jednotlivé body tak, aby mohly být úspěšně aplikovány na dané prostředí. Efektivní využití zásad ITIL a COBIT může vést k lepšímu využití stávajících technologií, zvýšení její spolehlivosti a z pohledu managementu také především k úsporám v provozu celého systému.

3.3.1 COBIT

COBIT (Control Objectives for Information and Related Technology), tedy Cíle řízení pro informační a s nimi spojené technologie, je souborem komplexních metrik, které se nejčastěji využívají pro IT audit, které vytváří americká asociace zabývající se IT Governance ISACA (Information Systems Audit and Control Association).

COBIT je velmi dobře využitelný při provádění auditů, neboť je schematický a jasně rozdělený do různých procesů, které jsou posuzovány na základě informačních kritérií a zdrojů. I bez hlubokých znalostí problematiky auditu tak lze podle metodiky COBIT rychle zhodnotit úroveň ICT v podniku. COBIT je zároveň nezávislý na technologiích, které jsou v podniku využívány, proto mohou být popsané metodiky snadno aplikovány plošně na podniky nejrůznějších velikostí. (ISACA, 2017)

Struktura procesů, které probíhají v rámci informačních technologií, vytváří jakousi COBIT "smyčku", která zároveň i odpovídá životnímu cyklu informačních systémů e jeho základním prvkům.



Obrázek 3 - Smyčka procesů COBIT

Zdroj: Ferroni, 2016

V jednom ze žurnálů ISACA uvádí Ferroni (2016) základní koncept segregace povinností, jehož základem je myšlenka, že žádný zaměstnanec nebo skupina by neměla být schopna spáchat a zakrývat chyby nebo podvody při běžném vykonávání svých povinností. Obecně pak platí, že hlavní neslučitelné povinnosti, které mají být odděleny, jsou:

- povolení nebo schvalování spolu souvisejících transakcí,
- úschova a opatrování majetku,
- zaznamenávání nebo hlášení souvisejících transakcí.

Do výčtu lez ještě zahrnout čtvrtou povinnost, která je potenciálně neslučitelná se zbývajícími třemi povinnostmi. Tato čtvrtá povinnost zahrnuje operace, které ověřují a kontrolují správnost operací provedených jinými jednotlivci, bez ohledu na to, zda se jedná o úschovu, zaznamenávání nebo povolování.

Subjekty, které vykonávají neslučitelní povinnosti je třeba rozdělit do samostatných entit. Každá entita má definované role, které se skládají z několika činností nebo celých procesů. Toto oddělení může být prováděno buď na úrovni jednotlivců nebo kolektivních skupin a tím vznikají rozdílné úrovně segregace v závislosti na organizačních omezeních, které se dělí na:

- SoD podle jednotlivců (individuální úroveň SoD)
  Tradiční a nejzákladnější úroveň segregace. Různé povinnosti jsou vykonávané různými jednotlivci, například účetní pověřeni manažerem provést platbu.
- SoD podle funkcí nebo organizačních jednotek (jednotková úroveň SoD)
  Různé funkce plní různé oddělené úkoly. Například obchodní oddělení může připravit nabídku, kterou pak uzavře a podepíše oddělení pro hodnocení operací nebo řízení rizik (případně vrcholový management).
- SoD podle společností (SoD na úrovni společnosti)
  Na této úrovni musí operace provádět různé právní subjekty. Například investice provedené dceřinou společností mohou vyžadovat povolení ze strany ovládající společnosti. Audity třetích stran mohou být také považovány za příklad firemního systému SoD. (Ferroni, 2016)

Kobelsky (2016) analyzoval a určil 6 základních povinností a jejich vzájemnou neslučitelnost. Nejčastěji používaný model SoD vyžaduje oddělení oprávnění (AUT – authorization), úschovy (CUS – custody), záznamu (REC – recording) a ověření (VER – verification). Z praxe však vyplývá zjednodušený přístup: rozdělení povinnosti ukládání záznamů od autorizačních povinností a zavádí třetí kategorii povinností: schválení přístupových oprávnění. V tomto modelu lze provádět operace spojené s různými povinnostmi na stejném majetku, pokud jsou povoleny druhou osobou. Typickým příkladem je úředník, který přijímá platby v hotovosti a zadává související údaje do počítačové aplikace.

Kromě výše uvedených povinností by měl model zahrnovat také povinnosti udělování nebo zrušení řádných práv a řízení povinnosti řízení a monitorování pravidel a postupů

společnosti SoD v souladu s řízením společností. Povinnosti udělování přístupových práv by měly bát zcela oddělení od ostatních povinností. (Kobelsky, 2016)

Z důvodu efektivity a nejčastěji z ekonomických důvodů může být účinné či dokonce nutné slevit z požadavků na oddělení provozních povinností, kterými jsou úschova a zaznamenávání v případě, že tyto dvě operace podléhají nezávislému oprávnění nebo ověření. V některých případech je jejich oddělení dokonce nemožné, například když záznamová operace vytvoří automatickou platbu (a tím vznikne povinnost k úschově).
Riziko oslabení SoD v tomto případě může být odstraněno zavedením kompenzační kontroly. Taková kontrola má za cíl snížit zranitelnost neefektivně oddělených funkcí, mezi něž patří riziko chyb, opomenutí, nesrovnalostí a nedostatků v kvalitě procesu. Nejčastěji se volí kontrola nezávislým auditem. (Ferroni, 2016)

Aby bylo možné řádně posoudit míru hrozby vzniku rizika vyplývající z konfliktních povinností, je zapotřebí řádného procesu posouzení rizik. Pro každý rizikový scénář, v němž je míra rizika považována za příliš vysokou, by měla být vhodná odpověď (implicitně nebo explicitně) zakotvena v pravidlech řízení společnosti SoD. Ferroni (2016) představil obecný rizikový scénář:

	CUS		AUT		VER		MGMT	
	Risk Category	Risk Scenario Examples	Risk Category	Risk Scenario Examples	Risk Category	Risk Scenario Examples	Risk Category	Risk Scenario Examples
REC	Material error	Undetected input of incorrect data	Embezzlement	A rogue authorizer enters forged data.	Fraud, embezzlement	Forged records go undetected.	Fraud, embezzlement	Recording grants are given to unauthorized people; privilege elevation.
	Fraud	Recorded data do not correspond to real money exchange.						
CUS			Embezzlement	A rogue authorizer diverts money to his/her advantage.	Fraud, embezzlement	Frauds related to the material handling of assets (e.g., money diversion) go undetected.	Fraud, embezzlement	Custody grants are given to unauthorized people; privilege elevation.
AUT					Fraud, embezzlement	Misuse of authorization grants goes undetected.	Fraud, embezzlement	Privilege elevation
VER							Fraud, embezzlement	Privilege elevation

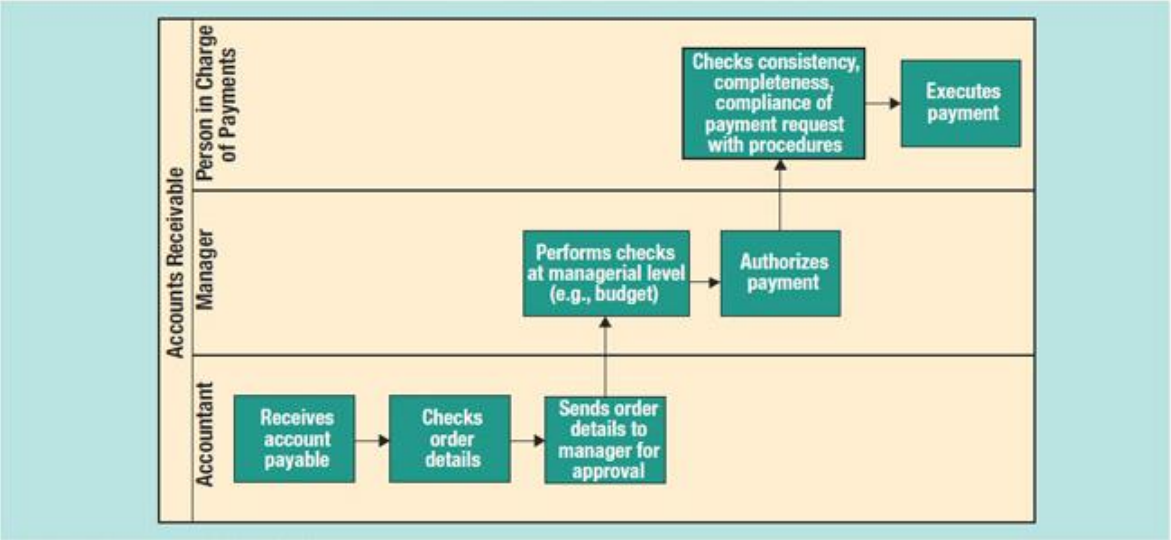
Obrázek 4 - Obecné scénáře rizik

Zdroj: Ferroni, 2016

Tabulka může být znázorněna i jako trojúhelníkový diagram, neboť prvky pod úhlopříčkou jsou shodné s těmi, které jsou nad nimi. Pokud c (X, Y) označuje povinnost X,

která je v rozporu s povinností Y, lze předpokládat, že c (X, Y) je ekvivalentní c (Y, X). Základem tabulky je také stanovení rozsahu povinností zahrnujících majetek. Povinnosti, které souvisejí s jedním a tímtéž aktivem by měly být odděleny. Jednotlivec může být odpovědný za různé povinnosti, pokud nezahrnují stejná aktiva. V některých případech je segregace účinná i tehdy, když je zdánlivě nějaký konflikt. Například dva zaměstnanci mohou být pověřeni záznamem a schvalováním transakcí na stejném souboru aktiv za předpokladu, že pro každý jednotlivý majetek jeden zaměstnanec zaznamená údaje transakce a druhý zaměstnanec povolí operaci. (Ferroni, 2016)

Ferroni (2016) představuje schéma, které představuje základní rozložení jednotlivých povinností a jejich oddělení procesu zpracování pohledávky. Schéma názorně zdůrazňuje, co je hlavním důvodem zavedení SoD – poskytuje konzistentní soubor kontrol a srovnání, které zajišťují, že všechny operace dodržují pravidla a jasné postupy, které lze zpětně kontrolovat.



Obrázek 5 - SoD pro proces zpracování pohledávky

Zdroj: Ferroni, 2016

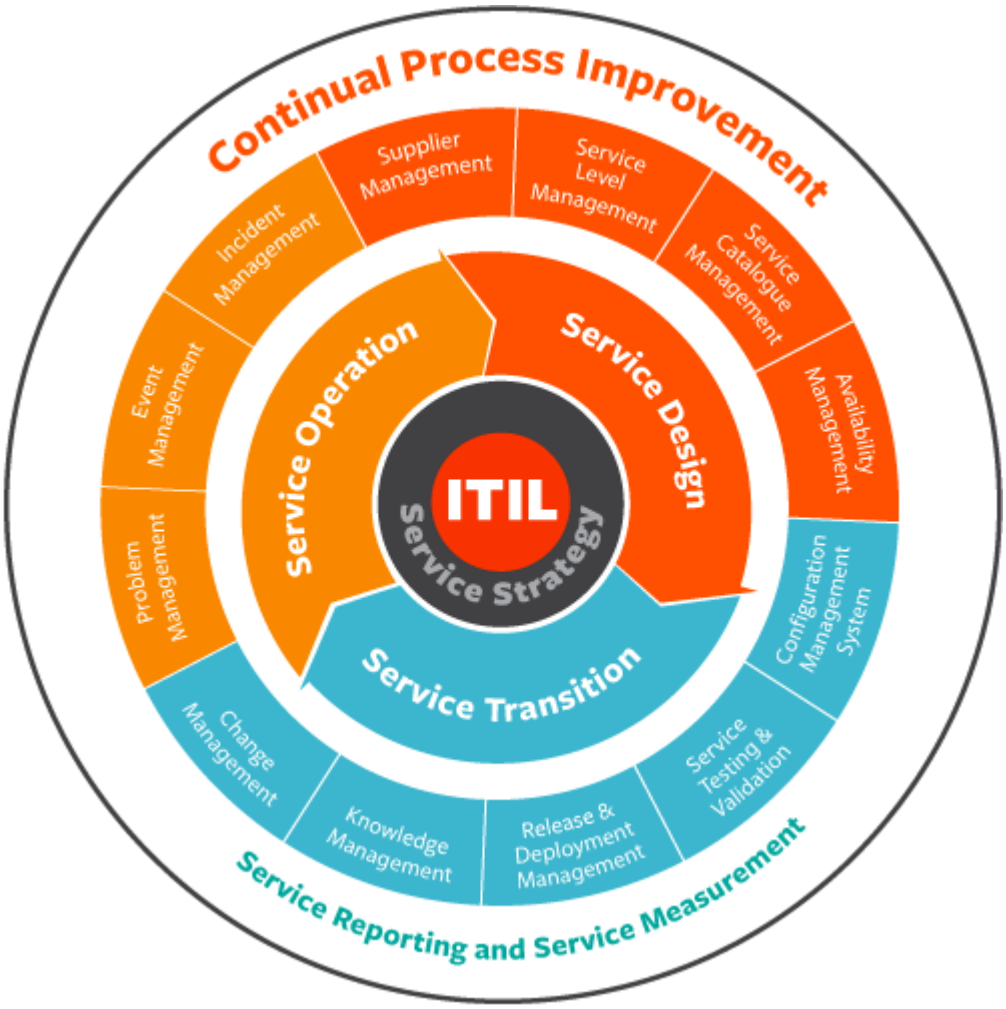
3.3.2 ITIL

ITIL (Information Technology Infrastructure Library), neboli Knihovna infrastruktury informačních technologií, je soubor dokumentů "best practices" pro řízení služeb. V těchto dokumentech lze nalézt postupy, které popisují jednotlivé kroky, které jsou využitelné v praxi. Dokumenty jsou ve formě praktických návodů, které však nejsou jediným zdrojem informací. ITIL nabízí i velký rozsah různých školení, profesionálních kvalifikací nebo dokonce softwarových prostředků. ITIL však funguje především jako návodná platforma pro výměnu zkušeností. Společnosti mohou získat znalosti a důležité podklady pro provoz efektivního a bezpečného ICT. Jednou z velkých výhod dokumentů ITIL je neustálý důraz na minimálních náklady, který je kontinuální ve všech oblastech, které ITIL zpracovává.

Jak zdůrazňují Basl a Novotný (2004), ITIL přijali a stále využívají velké společnosti z oblasti IT, jako je například Microsoft, Hewlett-Packard, IBM nebo Logica a implementovali návody ITIL do některých svých produktů.

Vývoj ITIL začal v osmdesátých letech minulého století a v současnosti má více než čtyřicet svazků, které vydala Central Computer and Telecommunications Agency (CCTA) ve Velké Británii. ITIL měl na svém počátku, kdy v polovině devadesátých let minulého století byl vydán první svazek, překotný úspěch, neboť dokázal spojit ověřené postupy řízení, (tedy tzv. „best practice“) a normy kvality ISO řady 9000. (Basl a Novotný, 2004)

Na rozdíl od metodiky COBIT neobsahuje návody určené pro audit. Všechny procesy, popisována dokumenty ITIL, nakonec tvoří uzavřený kruh neustálého procesu zlepšování úrovně ICT.



Obrázek 6 - Proces zlepšování ITIL

Zdroj: Bernard, 2012

Jednám ze základních kamenů filozofie řízení IT jsou tzv. 4P ITIL správy služeb. Mezi 4P patří:

- People (lidé),
- Products (produkty),
- Partners (partneři),
- Processes (procesy).

Fakt, že jako první ze 4P jsou lidi, dokazuje důležitost struktury a organizace lidí zapojených do poskytování IT služeb. Lidé jsou součástí zdrojů a kapacit potřebných pro poskytování kvalitních služeb IT uživatelům i zákazníkům. A protože kvalitní poskytování služeb se jedná pouze o jednání se zákazníky, uživateli a dodavateli, hodnota zavedení správných rolí a odpovědností v IT nemůže být podceňována. Správně řízené IT nebude nikdy fungovat bez lidí. (Ministr, 2013)

Role je soubor povinností, činností a orgánů udělených osobě nebo týmu. Role je definována v procesu nebo funkci. Jedna osoba nebo tým může mít několik rolí – například role manažera incidentů a správce problémů může provádět jedna osoba. Role jsou často zaměňovány s názvy pracovních pozic, ale je důležité si uvědomit, že nejsou stejné a často se neslučují. V každé organizaci je nutné definovat vhodné pracovní tituly a popisy práce, které vyhovují jejich potřebám. Jednotlivci, kteří mají tyto tituly, mohou vykonávat jednu nebo více z požadovaných rolí. (Ministr, 2013)

Neexistuje jediný nejlepší způsob organizace rolí, proto je třeba doporučené postupy popsané v ITIL přizpůsobit jednotlivým organizacím a situacím. Veškeré změny musí reflektovat omezení zdrojů, velikost, povahu a potřeby podniku. Výchozím bodem pro organizační návrh je jasná definice rolí a odpovědností potřebných pro uskutečnění procesů a činností. Strukturu rozložení rolí ovlivňuje vyzrálost, velikost, zeměpisné rozložení a míra využití technologií v podniku. Vzhledem k tomu, že organizace roste a dále se vyvíjí, je třeba provést změny rolí a vztahů a tím předejít možným problémům. (Ministr, 2013)

V malé organizaci mohou být různé role kombinovány pod jednou osobou. Ve větších organizacích může být každá z těchto rolí zastoupena mnoha různými lidmi, rozdělenými podle geografie, technologií nebo jiných kritérií. Pro zjednodušení lze chápat rozdělení malé a velké organizace na základě toho, zda je podnik povinen podrobit se auditu. Hlavní rozdíly mezi malou a velkou organizací popisuje následující tabulka:

MALÁ ORGANIZACE	**VELKÁ ORGANIZACE**
Role jsou kombinovány	Role jsou oddělené
Segregace povinností omezena	Segregace povinností byla maximalizována
Zobecňování dovedností	Specializace dovedností
Méně složitá struktura	Složitější struktura

Tabulka 3 - Rozdíly mezi malou a velkou organizací

Zdroj: http://bmc.lookbookhq.com/itil/476468.pdf

Mezi možná rizika v malé organizaci patří zneužití vlastnictví více služeb a procesů, v případě velké organizace se mezi největší rizika řadí složité vzájemné propojení rolí a tím vznikající nekontinuita toku pracovních činností. ITIL se proto opírá o morel RACI, který byl detailněji popisován v předešlých kapitolách. Každý vlastník specifické role by měl:

- mít znalost povinností, které se k roli váží,
- znát priority a podnikové cíle a jak k nim role přispívá,
- mít dovednosti, které je nutné mít pro vykonávání role,
- znát způsoby zvyšování a prohlubování kompetencí a znalostí role,
- porozumět a být schopen vykonávat osvědčené postupy. (ORR a BLOKKUM, 2016)

3.4 Náležitosti interních směrnic

3.4.1 Bezpečnostní dokumentace

Vyhláška 82/2018 Sb., resp. příloha vyhlášky č. 4 stanovuje doporučený obsah a strukturu bezpečnostní dokumentace a bezpečnostní politiky. Navrhovaná struktura je nezávazná. V příloze je specificky uvedeno, že záleží pouze na subjektu, jaký přístup k bezpečnostní dokumentaci zvolí.

Struktura bezpečnostní politiky je v příloze rozčleněna do kategorií dle oblastí, na které se má bezpečnostní dokumentace vztahovat. Nebude zde uváděno kompletní rozčlenění, avšak budou pouze zdůrazněny důležité body týkající se problematiky přístupových práv:

I. Struktura bezpečnostní politiky
   (1) Politika systému řízení bezpečnosti informací
   (2) Politika organizační bezpečnosti
      a) Určení bezpečnostních rolí a jejich práv a povinností

      (…)

   (3) Politika řízení přístupu
      a) Princip minimálních oprávnění/potřeba znát (need to know).
      b) Požadavky na řízení přístupu.
      c) Životní cyklus řízení přístupu.
      d) Řízení privilegovaných oprávnění.
      e) Řízení přístupu pro mimořádné situace.
      f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

      (…)

II. Struktura další dokumentace
      1.1 Zpráva z přezkoumání systému řízení bezpečnosti informací

(…) (Vyhláška č. 82/2018 Sb., příloha č. 4)

Řízení přístupových práv je pouze jednou součástí komplexní bezpečnostní dokumentace. Smejkal (2015) však zdůrazňuje její důležitost a srovnává ji s významem šifrování předávaných informací nebo procesy incident managementu. Zdůrazňuje, že největší riziko je v potenciálních interních hrozbách. Nejvýznamnější z nich je tzv. lidský faktor. Největší vnitřní hrozbou jsou samotní zaměstnanci a nejčastějším iniciátorem útoků jsou právě interní zaměstnanci. Nejlepším způsobem, jak eliminovat toto riziko je omezit možnosti potenciálního útočníka tím, že mu jsou udělena práva a přístupy pouze nezbytná k výkonu jeho role.

4 Vlastní práce

Část bezpečnostní dokumentace, která se do detailu věnuje problematice přístupových práv může mít formální podobu dvojího charakteru:

- samostatný oddělený dokument, na který je odkazováno v hlavní bezpečnostní směrnici, nebo
- součást hlavní bezpečnostní dokumentace.

V případě, že se jedná o druhou variantu, přístupová oprávnění jsou tématem samostatné kapitoly v hlavní bezpečnostní směrnici, která o nich pojednává. Jakou formu zvolit souvisí s tím, jak jsou řešeny další součásti informační bezpečnostní směrnice. Pokud existuje pouze jedna hlavní směrnice, která se neodkazuje na žádné jiné dokumenty nebo neobsahuje přílohy, část pojednávající o problematice přístupových oprávnění bude zahrnuta do textu této směrnice v podobě samostatného oddílu.

V rámci diplomní praxe bylo vybráno několik podniků, které zastupují obě zmíněné formy bezpečnostní dokumentace. Mezi další kritéria výběru podniků, u kterých bylo provedeno studium a následné hodnocení směrnic přístupových práv, patřilo:

- velikost podniku ve smyslu ročního obratu,
- velikost podniku ve smyslu počtu zaměstnanců,
- zda se na podnik vztahuje zákon o kybernetické bezpečnosti,
- odvětví, ve kterém podnik působí,
- míra využití informačních systémů v podniku.

Ze všech podniků, se kterými byla umožněna spolupráce a součinnost v průběhu diplomní praxe, byly vybrány:

- 3 zařízení z oblasti zdravotnictví (nemocnice),
- 3 zařízení poskytující služby v oblasti sociálních služeb (domovy seniorů),
- 2 výrobní podniky,
- 2 instituce veřejné správy.

Kompletní texty zkoumaných vnitřních předpisů výše zmíněných institucí nemohly být v práci zveřejněny, neboť nedošlo k udělení souhlasu s jejich zveřejněním vedením jednotlivých podniků. Části textů, a především jejich hodnocení a obsahová analýza, mohou

být zveřejněny za podmínky, že nebude uveden název organizace, ze které pochází. Neboť výsledky hodnocení nebudou moci být vztaženy ke konkrétnímu podniku, budou vytvořeny dva fiktivní podniky, do nichž budou výsledky jednotlivých institucí agregovány. Doporučení tak budou moci být generalizována na obecnou skupinu podniků se stejnými vlastnostmi.

Dva fiktivní podniky budou v práci nazývány jako malý a velký podnik. Za malý podnik lze pro zobecnění v této práci považovat takový podnik, který má obrat do 200 milionů korun a průměrný počet zaměstnanců do 50. Za velký podnik lze pro zobecnění v této práci považovat takový podnik, který má obrat více než 200 milionů korun a průměrný počet zaměstnanců nad 250. Rozdělení skutečných zkoumaných institucí do dvou fiktivních podniků je následujíc:

VELKÝ PODNIK	MALÝ PODNIK
3 zdravotnická zařízení	3 sociální služby
2 veřejné správy	2 výrobní podniky

Tabulka 4 - Agregace zkoumaných institucí

Každý ze zobecněných podniků v sobě tedy sdružuje vždy 5 skutečných zkoumaných institucí. V následujících kapitolách budou popsány zjištěné nedostatky zkoumaných interních předpisů a jejich závěry a následná doporučení budou vztaženy na zobecněné fiktivní podniky.

4.1 Politika udělování, kontroly a odebírání přístupových oprávnění

Všechny bezpečnostní směrnice musí být v souladu s několika důležitými pilíři podniku – s vizí, strategií a cíli. Jako první je tedy nutné definovat politiku udělování a kontroly přístupových oprávnění, která bude vyjadřovat soulad se všemi třemi opěrami organizace. Politika by měla obsahovat souhrn nejdůležitějších principů, na které pak budou následně podrobněji navazovat zvolené nástroje a postupy.

Cílem snad všech podniků, které se zodpovídají mateřské společnosti, je být v souladu s jejími požadavky. Nutnost být v souladu se však netýká jen velkých korporací, ale i všech ostatních podniků, u kterých lze obecně říci, že chtějí být v souladu s nároky svých zájmových skupin – ať už to jsou akcionáři, vlastníci, zákazníci nebo obchodní partneři. Tento soulad je ověřován nejčastěji pomocí auditu. Jedním ze základních principů politiky tedy musí být to, že celý proces udělování přístupových práv musí být zdokumentovaný, archivovaný a následné kontroly musí být auditovatelnost – poskytují informace o průběhu kontroly, které nevyvolávají pochybnosti.

Žádná z organizacích zařazená do skupiny velkého podniku neměla ve svých směrnicích jasně stanovenou politiku přístupových práv, která by tvořila základní rámec a principy, na kterých by byly založeny všechny další změny směrnice. Při vytváření změn se tedy všechny velké organizace řídili pouze doporučením a zkušenostmi interních zaměstnanců a externích poradců, nikoliv daným základním rámcem politiky.

V předchozích kapitolách bylo zmiňováno riziko, které nesou uživatelé jakožto potenciální škoditelé a význam lidského faktoru. Z toho důvodu je zaváděn proces udělování přístupových oprávnění. Je žádoucí zamezit stavu, kdy jsou uživateli automaticky přidělena běžná výchozí oprávnění bez ohledu na jeho roli nebo povinnosti. Tento fakt je v politice nutné zmínit, neboť při vytváření procesu udělování práv často dochází k velkému tlaku na jeho automatizaci. V podnicích s velkou fluktuací může počet procesů nutných k přidělení a odebrání práv vystoupat až ke stovkám denně. Nutnost co nejlépe fungujícího procesu přidělování a odebírání práv lze tedy přirozeně chápat, avšak jeho důsledkem může být automatizace, která odporuje základní myšlence kontroly přístupových práv.

Příkladem může být automatické udělení přístupu do podnikového intranetu v plném rozsahu hned v první den nástupu nového zaměstnance na danou pozici. Důvodem může být například nutnost přístupu zaměstnance k bezpečnostní dokumentaci, která se na intranetu nachází, a zaměstnanec s ní musí být v co nejkratším čase seznámen. Proces udělení odpovídajícího omezeného přístupu na intranet ale není optimálně nastaven a je zdlouhavý (předání informací z personálního oddělení, potvrzení povinností nadřízeným atd.). Proto byl zvolen postup automatického udělení plného přístupu, který je následně po dokončení celého procesu přiřazení odpovídajících práv omezen. Například riziko úniku citlivých informací je zde zcela zřejmé. Uvedený příklad zdůrazňuje důležitost ukotvení principu zamezení automaticky přidělovaných výchozí oprávnění.

Dvě z velkých organizací praktikovali automatické udělení přístupů – při nástupu zaměstnance mu byla přidělena sada předdefinovaných přístupových práv. Až za několik týdnů a v případě jedné organizace dokonce měsíců byly zaměstnanci přístupová práva zrevidovány a změněny na požadovaný stav. V malých organizacích naopak probíhalo přímo přiřazení odpovídajících práv, které vyplývá z nižší fluktuace zaměstnanců a menší vytíženosti IT pracovníků, kteří mají přidělování na starosti.

Všechna bezpečnostní opatření musí vycházet z provedené analýzy rizik. Do bezpečnostní politiky je třeba uvést pravidlo, které vzájemně propojuje míru rizika a jeho pravděpodobnost s přijatými bezpečnostními opatřeními a jemu odpovídajícími využitými technologiemi. Pokud je například vyhodnoceno velmi vysoké riziko v souvislosti s využíváním externích USB disků, které má zároveň velkou pravděpodobnost, zřejmě nebude za dostatečné opatření považováno zavedení čtvrtletních namátkových kontrol jejich obsahu. Vhodný bude spíše úplný zákaz vnášení neautorizovaných USB disků a zavedení šifrování. V oblasti řízení přístupových práv se bude tento princip týkat především prováděných kontrol – jejich intenzity a hloubky.

Žádná z malých organizací neměla provedenou analýzu riziku žádného z procesů, což bylo vzhledem k omezeným zdrojům organizací předpokládáno. Naopak všechny velké organizace měly vypracované analýzy rizik, ve všech však chybělo detailní zaměření na oblast přístupových práv a byly provedeny obecně na celou oblast informační bezpečnosti.

Každý proces, má-li být efektivní, musí mít svého vlastníka – tedy osobu odpovědnou za jeho výsledek. Princip odpovědnosti pověřeného vedoucího procesu řízení přístupových práv musí být jedním z dalších bodů politiky, aby bylo zajištěno vykonání a vymáhání stanovených pravidel.

Malé organizace neměly vždy jasného vlastníka procesu udělování, odebírání a kontroly přístupových práv. Ačkoliv je počet zaměstnanců v těchto organizacích nízký, vedení nestanovilo jasného vlastníka z řad zaměstnanců IT nebo odboru bezpečnosti, a proto se tito zaměstnanci nepovažovali za vlastníky procesu. Za vlastníky procesu byly považováni členové vedení. Naopak všechny velké organizace měli jasného vlastníka, který byl stanoven v interní směrnici. Ve čtyřech organizacích byly rozděleni vlastníci procesu udělování přístupu, odebírání práv a provádění kontroly a tyto procesy tak od sebe byly efektivně odděleny.

Nejen z legislativních důvodů popsaných v předešlých kapitolách, ale i ze zásad best practice je nutné dbát na zmiňovanou zásadu „need-to-know“. Tato zásada, vzhledem k její důležitosti, musí být zmíněna v politice přístupových oprávnění, neboť všechny procesy (přidělování, odebírání, kontrola, posuzování udělení výjimečných práv) musí společně směřovat k jejímu naplnění. Všechny z velkých organizací měli tento princip zakotven v interní směrnici a také tři ze zkoumaných malých organizací.

4.2 Rozdíly v postojích k řízení přístupových oprávnění u dvou rozlišných podniků

Jak již bylo nastíněno v teoretické části práce, různé podniky musí volit zvolit rozdílné postoje k problematice udělování oprávnění. Rozdíly budou vyplývat především z:

- počtu zaměstnanců,
- s tím souvisejících možností zastupitelnosti klíčových pozic,
- míře využití informačních technologií pro daný proces,
- složitost procesu,
- míra rizika.

4.2.1 Specifika malého podniku

Hlavním problémem takového podniku bude obtížná tvorba, a především následná aplikace, matice vzájemně neslučitelných rolí. Vzhledem k malému počtu zaměstnanců lze předpokládat, že jedna osoba musí vykonávat více rolí a některé z nich mohou být neslučitelné.

Jak ale bylo zmíněno v teoretické části práce, tato situace lze řešit důkladným posouzením možného rizika a v případě, že nelze vytvořit jinou situaci než přidělení vzájemně neslučitelných rolí, je nutné mít zavedená patřičná opatření, která zjištěné riziko budou eliminovat. Takovým opatřením je například pravidelná kontrola náhodně vybraných dílčích transakcí (procesů), které obsahují vykonávání neslučitelných rolí. Dalším prostředkem eliminace rizika může být pravidelná kontrola nikoliv dílčí transakce (procesu), ale kumulace několik dílčích transakcí dohromady. Takovou kontrolu lze provádět například měsíčně.

Žádná ze zkoumaných malých organizacích neprováděla pravidelnou kontrolu přístupových práv a ani neměla zavedený žádný předpis, který by tento proces definoval a stanovoval jeho četnost.

V malých podnicích lze očekávat, že klíčové procesy, které mají označená vysoká rizika neslučitelných rolí, nejsou složitá a obtížná na administrativu. Z toho důvodu může matice neslučitelných rolí být mnohem menších rozměrů, než by tomu bylo u velkého podniku. Malé podniky však neměly vytvořenou matici neslučitelných rolí a ani nedisponovali základním popisem neslučitelnosti nebo alespoň popisem stěžejních rolí.

Největším úskalím malého podniku je však vedení dokumentace o přidělování, odebírání a kontrole přístupových práv. Jedině dle řádně vedené dokumentace, která je auditovatelná, lze nejen předcházet chybám, ale i zpětně vyhodnocovat efektivitu procesu. V malých podnicích je často většina požadavků a informací sdělována ústně. Vyplňování formulářů a jejich následné potvrzování se stává zbytečnou administrativní zátěží. V malých podnicích tak musí být kladen důraz na co nejjednodušší formuláře, jejichž vyplňování je rychlé a intuitivní (nebo částečně předvyplněné).

Čtyři z pěti malých organizací, které byly podrobené zkoumání, neměly vytvořený formulář pro dokumentaci žádostí o přidělení nebo odebrání práv. Jedna malá organizace disponovala formulářem pro zaznamenání žádosti a provedení odebrání přístupových práv při odchodu zaměstnance, avšak při bližším zkoumání bylo zjištěno, že se formulář vůbec nevyužívá a vše probíhá ústně.

Obtížná je vůbec i motivace k vedení záznamů, především o změně přístupových práv. Jedním z efektivních řešení je zavedení podmíněného systému, kdy práva nejsou uvedena v platnost, pokud není vyplněn a uzavřen požadavek na jejich přidělení. Povinnost vést záznamy a žádat o přístupová oprávnění příslušnými formuláři však musí být především zakotvena v bezpečnostní směrnici.

Bezpečnostní směrnice ve zkoumaných malých podnicích byly jednoduché krátké dokumenty, které stanovují pouze základní pravidla a jsou vytvořeny externími poradci či zaměstnanci, kteří nemají dostatečné znalosti pro jejich kvalitní vypracování. V malých podnicích totiž často nebyla určena pozice bezpečnostního manažera informačních technologií a povinnosti, které se k pozici váží jsou přiděleny správci IT. Správce IT však nemá potřebnou kvalifikaci ani praxi, aby mohl vytvářet strukturované směrnice. Z toho důvodu je nutné zdůraznit, že ve směrnici týkající se bezpečnosti IT musí být zmíněna povinnost využívat formuláře pro žádosti o přidělení přístupových práv. Bezpečnostní směrnice IT bude v malém podniku jeden dokument, který bude rozdělen do několika málo kapitol. Celá směrnice může být součástí obecné bezpečnostní směrnice vztahující se i na další oblasti bezpečnosti podniku.

4.2.2 Specifika velkého podniku

Hlavním problémem takového podniku bude složitá tvorba matice vzájemně neslučitelných rolí, které bude muset předcházet důkladná analýza rizik. Lze předpokládat, že velké podniky budou mít nejen díky svojí velikosti, ale také kvůli povaze podnikání složité procesy, které vyžadují důkladnou administrativu. Do jedné transakce tak může být zapojeno několik zaměstnanců, z nichž nikdo nesmí vykonávat neslučitelnou roli.

Pouze dva zkoumané velké podniky měly vytvořenou matici neslučitelných rolí. Žádná z nich ale nebyla aktualizovaná od doby svého vytvoření a v obou případech již nebyla aktuální. Reálný proces udělování práv se tedy touto maticí neřídil, neboť nevyhovovala. Obě matice také byly vytvořeny bez předešlé analýzy jednotlivých procesů a jejich vznik byl založen pouze na definici jednotlivých rolí a zkušeností z provozu.

Tři zbývající zkoumané velké organizace o zavedení matice neslučitelných rolí neuvažovali, dvě z nich především neznali její význam ani přínos pro informační bezpečnost. Posouzení, zda je možné určitá práva zaměstnanci přiřadit rozhodoval ve většině vedoucí pracovník daného zaměstnance a jeho rozhodnutí bylo založeno na zkušenostech a subjektivním posouzení možných rizik.

V rámci zkoumání byl v těchto třech organizacích náhodně vybrán jeden zaměstnanec z oddělení účtárny a byly vždy zkoumány jeho přidělená práva ve vztahu k jeho roli. Posouzení probíhalo na základě stanovených principů z teoretické části, konkrétně pomocí metodiky COBIT, ve které je věnovaná velká část právě základnímu procesu objednávka-faktura-skladní list. V žádné z organizací nebylo nalezeno pochybení a žádný ze zkoumaných pracovníků neměl přidělen neslučitelné role. Ačkoliv tedy nebyly neslučitelnosti definovány, na základě subjektivního určení vedoucích nedošlo k vytvoření rizika.

Ve velkých podnicích je předpoklad dostatečného počtu uživatelů, kteří mohou narozdíl od malého podniku eliminovat riziko vzájemně neslučitelných rolí jednoduše tím, že není důvod, aby jeden uživatel vykonával velké množství rolí. Ve velkých podnicích je téměř nemožné provádět odpovídající namátkovou kontrolu transakcí, pokud počet transakcí dosahuje například tisíců za měsíc. Stejně tak je obtížná kontrola jejich kumulací, neboť čísla

kumulovaných transakcí jsou tak vysoká, že případné rozdíly se budou k celkovým částkám považovat za zanedbatelné.

Důkladným definováním všech existujících rolí v podniku a jejich analýze rizik lze vytvořit matici neslučitelných rolí a jedině jejím důsledným dodržováním lze ve velkém podniku efektivně čelit zjištěným rizikům. I ve velkém podniku musí být kladen důraz na důsledné vytváření a vyplňování formulářů žádostí o přidělení, úpravě, odebrání nebo kontrole přístupových práv. Ve velkých podnicích není tolik nutné obávat se jejího nevyplňování z důvodu ústního předávání informací. Administrativní procesy formulářů bývají dobře zažité a jsou také součástí podnikové kultury řešení některých požadavků.

Ve všech zkoumaných organizacích, zařazených do kategorie velký podnik, byly vytvořeny formuláře pro udělení i odebrání přístupových práv. Ve velkém podniku však vzniká riziko v případě, že administrativních požadavků je velké množství a zaměstnanec nemá prostor plnit všechny požadavky administrativního zatížení, a přitom efektivně plnit primární náplň svojí práce. Přesně to byl problém všech organizací – ve všech byla dokumentace buď neúplná (vyplnění pouze části formuláře, chybějící podpisy vlastníků procesu) nebo byly odhaleny nahodilé případy, kdy k určitému zaměstnanci nebyla dokumentace vedená vůbec.

Důležitost vedení dokumentace týkající se přístupových oprávnění však musí mít ve velkém podniku velkou prioritu, neboť je podkladem pro auditní kontroly. Jedním z řešení tedy může být opět systém podmínění, kdy vykonavatel změň v přístupových oprávnění z oddělení informačních technologií nemá právo nijak do nastavení zasáhnout, pokud není kompletně vyplněn odpovídající formulář. Výjimka přirozené může ojediněle nastat v naléhavém odebrání přístupových práv uživatele, a především v případě odebrání privilegovaných účtů, které musí často nastat již do několika hodin.

Všechny velké organizace prošly auditem úspěšně s kladným výrokem, žádný z auditů však nebyl zaměřen přímo na IT bezpečnost, jednalo se vždy o klasický účetní audit, a proto nebyly detailně zkoumány procesy přístupových práv.

Ve velkých podnicích je běžná pozice bezpečnostního manažera informačních technologií, který má kompetence k vytvoření strukturované, obsáhlé a detailní dokumentace. Bezpečnostní dokumentace týkající se přístupových práv je oddělená od zbytku bezpečnostní

dokumentace týkající se informačních technologií obecně. Vzhledem k časově a administrativně náročnému procesu aktualizace nebo změny bezpečnostních směrnic lze předpokládat, že nejvhodnějším přístupem bude rozdělit bezpečnostní směrnici přístupových oprávnění rozdělit do minimálně 4 základních částí – úvod a základní ustanovení, udělování přístupových práv a provádění změn, odebírání přístupových práv a kontrola přístupových práv. Zkoumané velké organizace popsali obtíže v procesu změn směrnic, který je zdlouhavý a administrativně náročný. Při změně v některé z dílčích částí tak nemusí docházet ke kompletní revizi celé dokumentace týkající se přístupových práv. Právě náročnost procesu změn směrnic bylo primárním důvodem, proč obsahovali neaktuální nebo nevyhovující pasáže.

Proces aktualizace jedné části (například jedné kapitoly nebo dokonce jen jednoho odstavce) velké směrnice, která obsahuje všechna informační bezpečností témata, se může významně komplikovat. Různé zájmové skupiny se mohou snažit prosadit další jiné změny, které však nijak nesouvisí s původně upravovanou částí směrnice. Jelikož je však směrnice otevřena pro změny a byl zahájen proces schvalování těchto změn, otevírá se potenciální prostor pro další možné zásahy, které mohou celý proces prodloužit a zkomplikovat.

Další výhodou oddělených částí informační bezpečnostní směrnice je větší přehlednost a organizovanost ve správě směrnic. Směrnice je nutné pravidelně revidovat s ohledem na jejich platnost a především kontrolovat, zda stále odpovídají cílům bezpečnostní politiky a snižují rizika stanovená na základě analýzy rizik. Jednotlivé části směrnice tím pádem mohou vyžadovat odlišný přístup v jejich revizi – různě dlouhé intervaly kontrol i různé pověřené osoby, které tuto kontrolu provádí.

Oblast informační bezpečnosti se neustále vyvíjí s ohledem na to, jak dynamický je vývoj informačních technologií obecně. Důležitost a angažovanost IT v podnicích stále roste a s tím i důraz na informační bezpečnost. Vytváření zcela nových směrnic lze tedy považovat za běžný a zcela přirozený jev v podnikové informační bezpečnosti. Pokud jsou jednotlivé oblasti informační bezpečnosti vzájemně oddělené, přidáváním nových směrnic pouze přehledně vytváříme nový ucelený dokument. Pokud však do jedné hlavní směrnice potřebujeme přidat zcela nové téma, je nutné ho logicky začlenit mezi některé kapitoly. Číslování kapitol se změní (což může být v některých oblastech podnikové činnosti obtíž) a směrnice nabývá na velikosti až může dosáhnout rozměrů tak obrovského dokumentu, že se v něm lze jen těžko orientovat a pro koncového uživatele, který se jí má řídit, je téměř nečitelná.

4.3 Hodnocení přístupů z hlediska legislativního

V předchozích kapitolách by zdůrazňován princip tzv. need-to-know. Na jeho základě by měly být zpřístupněny informace pouze nutné k výkonu jejich povinností. Stejný princip je tedy nutné aplikovat v přístupu ke všem druhům informací – tedy i k bezpečnostním směrnicím. Příkladem může být směrnice zabývající se udělením a kontrolou výjimečných přístupových práv (práva správců a administrátorů). Zaměstnanec, který je pověřený přidělováním běžných standartních oprávnění nemusí zároveň provádět udělování výjimečných administrátorských práv. Není tedy nutná jeho znalost této směrnice a tím lze zamezit potenciálnímu zneužití vědomosti o fungování procesu přidělování administrátorských práv.

Všechny velké organizace měly tento princip zakotven ve svých směrnicích, především kvůli doporučené struktuře bezpečnostní směrnice, kterou určuje příloha vyhlášky o kybernetické bezpečnosti. Jedna z velkých organizací měla tento princip obsažen také kvůli požadavkům ISO a metodickému doporučení Národního centra kybernetické bezpečnosti. Malé organizace tento princip obsažený neměly. Malé organizace především nedodržely povinnost provést posouzení rizik neoprávněného přístupu k osobním údajům, které vyžaduje GDPR a neměly zavedená žádná opatření v udělování přístupových práv, která by zabránila neoprávněnému použití osobních informací ve smyslu určeném GDPR.

Dvě z velkých organizací ve veřejné správě jsou zařazeny mezi povinné osoby, které určuje zákon o kybernetické bezpečnosti. Obě organizace dodržují základní principy týkající se přístupových práv, kterými je udělování přístupu na základě rolí, omezovat privilegované účty nebo provádět kontroly a vést dokumentaci. Obě organizace také prokázaly splnění požadavku na existenci nástroje pro řízení přístupových oprávnění.

4.4 Hodnocení přístupů z hlediska best practice

Za efektivní variantu z pohledu best practice lze považovat obsažení problematiky přístupových oprávnění do samostatného dokumentu, stejně jako všech dalších významných témat informační bezpečnosti. Jedním z hlavních důvodů pro vytvoření samostatných dokumentů pojednávajících vždy o jednom samostatném oddílu informační bezpečnosti je snadnější proces aktualizací jednotlivých směrnic. Při změně ve znění směrnice, především pokud se v ní nachází stanovení postupů při vykonávání některých povinností nebo kontrol (například postup při udělování přístupových práv nebo kontrola jejich odebrání) vyžaduje někdy náročný administrativní proces. Do tohoto procesu musí být zapojeny všechny relevantní osoby a schvalování změn nebo aktualizací musí podléhat kontrole těchto relevantních osob. Oddělením různých problematik do samostatných dokumentů je při jejich revizi zatěžován především ten, kdo má s oblastí přímou souvislost a není tak třeba zapojovat do procesu úplně všechny osoby. Žádná ze všech deseti zkoumaných organizací však toto doporučení nedodržela.

Z pohledu malých organizací bylo zásadním problém aplikování platnosti dané směrnice i na externí dodavatele. Malé podniky velkou měrou využívaly outsourcing, avšak bezpečností směrnice svojí platností necílily na skupinu externistů, kteří přistupovali do informačních systémů malých podniků. Externistům tedy byly často přiděleny práva administrátorů nebo jinak privilegované přístupy, které nebyly následně revidovány a po skončení spolupráce včas odebrány. Privilegované účty byly ve zkoumaných malých podnicích problémem i u interních zaměstnanců. Vzhledem k nízkému počtu uživatelů v systému, například pouze dva uživatelé, nebyla pociťována důležitost vytvoření různých rolí a oba uživatelé dostali přidělené privilegované účty.

V malých podnicích nedocházelo ke kontrole přidělených práv ani ke zpětné kontrole procesu přidělování, jelikož k němu neexistovala dokumentace. Ve velkých organizacích naopak k pravidelné kontrole přidělených práv docházelo, především byl kladen důraz na kontrolu privilegovaných účtů. Ve třech velkých zkoumaných organizacích byla také vedena podrobná dokumentace provedené kontroly – jméno odpovědné osoby za kontrolu, metodika a průběh kontroly, výsledky a přijatá patření. Organizace, které měly definované vzájemně neslučitelné role, také prováděly jejich pravidelnou revizi, o které vedly záznamy.

U malých organizací nebyl předpoklad, že budou disponovat vypracovanou maticí vzájemně neslučitelných rolí. Z pohledu best practice, ale i ze zásad kybernetického zákona a jeho příslušných metodických doporučení vyplývá, že je nezbytné přijmout opatření, která by rizika neslučitelných rolí omezila. Malé podniky však žádné takové kroky pro snížení rizik nepodnikly, především nebyla prováděna žádná kontrola práv ale především provedených transakcí.

5 Výsledky a diskuse

Výsledný návrh směrnice se odvíjí z legislativních požadavků, ze zásad best practice a především reflektuje výsledky zkoumání bezpečnostních směrnic deseti různých podniků a jejich praktické aplikaci z oblasti přístupových práv. Do směrnice jsou zahrnuty jak pozitivní zjištění ve smyslu dodržování zákonných povinností, tak úspěšná aplikace a dodržování zásad best practice. Všechny nedostatky zjištěné v rámci studia poskytnutých interních směrnic byly taktéž zařazeny do směrnice, aby případné využití tohoto návrhu směrnice v praxi zjištěné nedostatky odstranilo.

Z důvodů zachování anonymity zkoumaných organizací popsaných v úvodní části vlastní práce jsou výsledky vztaženy ke dvěma obecným organizacím nazývanými jako malý a velký podnik. Studium a hodnocení bezpečnostní dokumentace deseti různých organizací vztahující se k problematice přístupových práv poskytlo výsledky, které byly popsány v předešlých kapitolách a mohou být shrnuty do následující tabulky:

VELKÝ PODNIK	**MALÝ PODNIK**
Dodržení legislativy	GDPR – neposouzení rizika – nezabránění neoprávněného přístupu a použití
Obsáhlý dokument – obtížné provedení změn	Informační bezpečnost součástí obecné bezpečnostní politiky
Nedefinovaná politika určující základní principy	Rozsah platnosti nevztažen i na externí poskytovatele
Neúplná dokumentace	Nevedení dokumentace
Omezené a revidované privilegované účty	Neomezení privilegovaných účtů
Zpracované SoD matice nebo jinak definované neslučitelné role	Nedodržení principu need-to-know
Revize neslučitelných rolí	Žádná opatření snížení rizika neslučitelných rolí
Pravidelné kontroly s dokumentací	Neprovádění kontrol
Pravidelné audity	Žádný externí audit

Tabulka 5 - Výsledky výzkumu

Směrnice je rozdělena do osmi částí, které jsou na základě výzkumu ve velkých organizacích doporučeny evidovat odděleně, aby případná úprava jedné z osmi částí neznamenala kompletní revizi celého souboru bezpečnostní dokumentace týkající se přístupových práv. Směrnice má tyto části:

1. Účel
2. Rozsah platnosti
3. Politika přístupových práv
4. Řízení přístupových práv
5. Řízení privilegovaných účtů
6. Udělování přístupových práv
7. Odebírání přístupových práv
8. Požadavky na kontrolu přístupových práv

Směrnice obsahuje také přílohu, kterou je formulář pro dokumentování žádosti a provedení přidělení, odebrání a kontrole (obsaženo v kolonce „jiné“) přístupových práv. Tento formulář se předpokládá v elektronické podobě jako součást tiketovacího systému na vznášení požadavků.

5.1 Výsledný návrh směrnice

1 Účel

1) Účelem směrnice řízení přístupů je definovat pravidla pro přístupová oprávnění do IT systémů. Tato pravidla představují jeden z preventivních kroků proti neoprávněnému přístupu k informačním systémům, vnitřním sítím, datům, informacím a proti zneužití oprávnění pro provádění změn a získávání nebo mazání dat.
2) Tato směrnice navazuje na směrnici Bezpečnostní politika. Bezpečnostní politika je této směrnici nadřazena.

2 Rozsah platnosti

1) Tento vnitřní předpis byl schválen představenstvem podniku dne 3. prosince 2019 a je účinný ode dne 1. ledna 2019. Tento předpis v plném rozsahu nahrazuje vnitřní předpis „Starý předpis pro řízení přístupů“ ze dne 1. prosince 2014, jehož platnost a účinnost končí dnem 1. ledna 2019.
2) Tato směrnice je závazná pro všechny zaměstnance podniku, včetně zaměstnanců vykonávajících pro podnik práce na základě dohod o pracích konaných mimo pracovní poměr a také pro osoby vykonávající pro podnik práce na základě jiných smluvních vztahů (dále jen „zaměstnanci“).
3) Tato směrnice je závazná i pro externí poskytovatele služeb – outsourcingové partnery – a jejich zaměstnance a subdodavatele. Podmínka závaznosti musí být smluvně zakotvena formou dodatku ke smlouvě nebo zahrnutím do nových smluv s partnery.

3 Politika přístupových práv

1) Musí být implementovány postupy udělování, odebírání a kontroly přístupových práv, které:
   a) jsou plně dokumentovány a jsou vytvořeny vzory požadovaných formulářů,
   b) splňují podmínku auditovatelnosti.
2) Musí být dodržen princip „need-to-know“, aby uživatelům byla udělena pouze taková oprávnění, která jsou potřebná k výkonu jejich povinností.
3) Musí být odstraněny a zakázány všechny možnosti automatického udělování výchozích předem nastavených oprávnění, která nezohledňují povinnosti a roli uživatele, aby se zabránilo jejich neoprávněnému použití.

4) Použité bezpečnostní produkty, funkce, procesy a opatření musí odpovídat hodnocení rizik informační bezpečnosti a klasifikaci těchto rizik.
5) Každý z osob pověřených správou přístupových oprávnění odpovídá za vhodnost a udržování přístupových práv uživatelů pod jeho kontrolou.
6) Musí být stanoven přesný postup procesu přidělení, odebrání a kontroly přístupových práv.
7) Přidělení, odebrání a kontrola přístupových práv může být provedena jen na základě vyplněného elektronického formuláře, jehož podoba je přílohou č. 1 této směrnice.

4 Řízení přístupů uživatelů

1) Žádný z uživatelů nemůže nabýt přístupových práv bez souhlasu nadřízeného nebo oprávněné osoby pověřené nadřízeným.
2) Každá změna v rozsahu přístupových oprávnění musí podléhat souhlasu nadřízeného nebo oprávněné osoby pověřené nadřízeným.
3) Udělení nebo změna výjimečných privilegovaných oprávnění musí podléhat souhlasu nadřízeného nebo oprávněné osoby pověřené nadřízeným a zároveň také souhlasu osoby pověřené kontrolou privilegovaných oprávnění.
4) Uživatelé se nesmí žádným způsobem pokoušet narušit, pozměnit nebo oslabit bezpečnostní opatření chránící data, včetně přiřazených práv. Zjištěné případy neoprávněných a neautorizovaných zásahů budou považovány za závažné porušení pracovní kázně.
5) Uživatel může nabýt přístupových práv pouze na základě Matice přístupových práv. O výjimce z této Matice přístupových práv musí být vytvořen záznam, který schválí nadřízený zaměstnance a bezpečnostní IT manažer. Tento záznam musí být uchováván pro případ auditní kontroly.

5 Řízení privilegovaných práv

1) Za výjimečná privilegovaná oprávnění jsou považována taková oprávnění, která náleží pověřeným zaměstnancům nebo zaměstnancům outsourcingového partnera nebo smluvního partnera, kteří spravují informační systémy, technologie a síťové prvky a opravňují držitele k provádění veškerých úkonů ve všech místech systému.
2) Použití privilegovaných účtů je omezeno na minimum. Pokud to není nezbytné pro výkon práce zaměstnance nebo managera IT Security nezbytné, pracuje se svým běžným účtem.
3) Privilegované (administrátorské) přístupy jsou omezené na vybrané IT administrátory, na základě oprávněné potřeby a požadavku. Požadavek zadává IT Manager přes elektronický formulář, který je přílohou č 1 této směrnice a který je schválen IT Security Managerem.

6 Udělování přístupových práv

1) Proces udělování privilegovaných práv se řídí body z části č. 3 a 4 této směrnice. Proces udělování privilegovaných přístupových práv se řídí body z části č. 5 této směrnice.
2) Každému uživateli musí být přiřazeno permanentní neměnné jedinečné identifikační číslo. Oprávnění jsou přiřazována k tomuto identifikačnímu číslu.
3) Proces udělování privilegovaných práv podléhá dvojímu souhlasu. Souhlas musí vyjádřit nadřízený nebo oprávněná osoba pověřená nadřízeným a zároveň také osoba pověřená kontrolou privilegovaných oprávnění.
4) Žádosti o nové uživatelské účty nebo změnu práv musí být předkládány v elektronické formě příslušného formuláře, který je v příloze č 1 a musí být odsouhlaseny vlastníkem (vedoucím pracovníkem uživatele).
5) Odsouhlasení přiřazení požadovaných přístupových práv může být uděleno pouze na základě souladu s Maticí přístupových práv.
6) Elektronický formulář žádosti udělení přístupových práv musí obsahovat následující informace:
   - jméno, příjmení a jedinečné identifikační číslo zaměstnance,
   - popis pracovní pozice nového uživatele,
   - platnost od do,
   - požadovaný termín nastavení (okamžitě nebo ke stanovenému datu),
   - jméno nadřízeného zaměstnance, tj. žadatele a jeho funkční zařazení
   - výsledek – přidělení, nebo omítnutí požadavku o přístup,
   - datum a jméno zaměstnance, který přidělení práv provedl.
7) Pro změnu přístupových oprávnění je využíván stejný formulář, pouze je označen příznakem „změna oprávnění“.
8) Vedoucí pracovník odpovídá za to, že uživatel byl před přidělením přístupu poučen a seznámen s užíváním příslušného informačního systému a rozsahu svých oprávnění.
9) Všichni uživatelé musí před získáním přístupových účtů a přístupových práv podepsat prohlášení, že je seznámen s pravidly používání informačního systému.
10) Udělení oprávnění spojená s uživatelskými soubory nesmí umožňovat číst nebo přepisovat soubory jiných uživatelů. Oprávnění ke sdílení souborů je možné pouze po prokázání, že je toto sdílení nezbytné k práci dané skupiny.

7 Odebrání přístupových práv

1) Odebrání přístupových údajů do Active Directory, Single-Sign-On, emailu a připojení ke vzdálené ploše musí proběhnout nejpozději na konci následujícího pracovního dne po podání žádosti. Všechny ostatní přístupové údaje mohou být odebrány do sedmi pracovních dnů.
2) Odebrání přístupových oprávnění privilegovaných účtů musí proběhnout do 3 hodin od podání žádosti.
3) O odebrání přístupových oprávnění a zrušení účtu žádá pověřený zástupce personálního oddělení při zahájení výstupního procesu zaměstnance. Žádost podává elektronicky přes určený formulář v příloze č. 1 této směrnice.
4) Elektronický formulář žádosti odebrání přístupových práv musí obsahovat následující informace:
   - jméno, příjmení a jedinečné identifikační číslo zaměstnance,
   - požadovaný termín nastavení (okamžitě nebo ke stanovenému datu),
   - odebrání přístupových práv daného uživatele (uživatelského účtu) z aplikací,
   - datum a jméno zaměstnance, který provedl blokaci uživatelských účtů.
5) Účty, které jsou neaktivní, musí být deaktivovány automatickým systémem nejpozději čtyřicátý den neaktivity.

8 Požadavky na kontrolu přístupových práv

1) Za ověřování a kontrolu přístupových práv zodpovídá IT Security Manager.
2) Privilegovaná oprávnění podléhají častější kontrole než běžná přístupová oprávnění. Kontrola probíhá alespoň jednou za 3 měsíce.
3) Kontrola běžných uživatelských oprávnění je prováděna alespoň v pololetním intervalu a vždy po změně rolí nebo struktury sdílených disků.
4) Výstupem této kontroly je Protokol o kontrole přístupových práv, který je podepsán IT Security Managerem a ve kterém je vyznačen buďto soulad, nebo nesoulad, s označenými problémovými oblastmi a popisem jejich okamžité nápravy.
5) Ke kontrole jsou použity výpisy/exporty z tiketovacího systému, který obsahuje formuláře se záznamy přidělení nebo odebrání a výpisy/exporty z příslušných informačních systémů s detailem přiřazených práv zaměstnance.

6) Výsledky této kontroly jsou postoupeny vedení společnosti.
7) Přístupy do systému, domény a aplikací jsou monitorovány, činnost je zaznamenávána do auditních záznamů, které jsou ukládány do zabezpečené složky, jejíž obsah nemůže neautorizovaná osoba vymazat. Monitorovací logy vyhodnocuje IT Security Manager a postupuje k řešení IT oddělení.
8) Monitorovány jsou minimálně následující události:
    - použití účtu supervizora/administrátora,
    - spuštění a ukončení systému,
    - změny v datech významně ovlivňující chod a výstupy informačního systémů.

Podoba elektronického formuláře:

Přístup

Aplikace / Systém	
Přístupová práva dle matice	

Uživatel

Jméno	
Příjmení	
Uživatelské jméno	
Útvar	

Kontaktní údaje zadavatele

Telefonní číslo	*pro další informace nebo zaslání oznámení o přidělení či zamítnutí přístupu*
Emailová adresa	@

Důvod požadavku (vyberte):

Nový nebo dodatečný přístup	☐	Smazání přístupu (práva již nejsou požadována)	☐
Úprava současných přístupových práv	☐	Jiné (prosím specifikujte níže)	☐
Jiné:			

Schválení přístupu IT Manager / IT Security Manager / Nadřízený žadatele

IT manažer (podpis + datum)	
IT Security manažer (podpis + datum)	
Nadřízený žadatele (podpis + datum)	
Zadal do aplikace / systému (podpis + datum)	**Po schválení všech výše jmenovaných!**

5.2 Odhad finančního a personálního zatížení na zavádění

Zkoumané malé podniky neuvažují o zavedení nové směrnice pomocí interních zdrojů vlastních zaměstnanců, neboť nedisponuje vhodnými odborníky v této oblasti. Jedinou možností, kterou by zvolilo všech pět zkoumaných malých organizací, by bylo využití externího konzultanta. Předpoklad organizací je přenechání všech činností související s implementací na externím dodavateli. Žádná z dotazovaných organizací však k využití externího konzultanta přistoupit nechce, neboť očekávají vysoké náklady. Tři ze zkoumaných malých organizací tyto náklady nemohou akceptovat z důvodu omezených finančních prostředků ročního rozpočtu organizace. Zbývající dvě organizace považují vynaložení finančních prostředků na externího konzultanta pro IT bezpečnost za neefektivní vyložení svých omezených finančních zdrojů a předpokládané náklady by raději investovali do jiných aktivit.

Zkoumané organizace byly dotázány na průměrnou hodinovou sazbu bez DPH jejich externích konzultantů pro oblast softwarového, účetního, finančního a obecně právního poradenství. Průměrná hodinová sazba konzultantské práce všech organizací byla 4 100 Kč. Dle zkušeností nebo smluv zkoumaných organizací s konzultantskými společnostmi se jednotlivé projekty stanovují na minimální rozsah alespoň 10 hodin práce konzultanta s následným navýšením počtu hodin, které se odvíjí od náročnosti projektu. I při započtení minimálního objemu 10 hodin by výsledná částka 41 000 bez DPH byla pro zkoumané malé organizace zátěží, především pak pro ty působící v oblasti poskytování sociálních služeb.

Všechny velké podniky by naopak bez rozdílu neuvažovali o využití externího konzultanta a využili by svých interních zaměstnanců, kteří mají dostatečné odborné znalosti v oblasti bezpečnostní dokumentace a IT Security. Žádná z organizací by pro tento úkol neplánovala navýšení počtu nebo rozsahu pracovních úvazků. Úkol zavedení nové části bezpečnostní dokumentace by bylo přiděleno zaměstnanci jako jeden z jeho dalších pracovních úkolů. Velké organizace tedy neočekávají žádné dodatečné náklady na zavedení nové směrnice. Jedinou obtíž v procesu implementace spatřovali časovou náročnost procesu a jeho časové plánování. Zaměstnanec, kterému by byl úkol implementace svěřen, byl totiž ve všech velkých organizacích natolik vytížen, že by mohl proces zavedení začít nejdříve za půl roku.

5.3 Diskuze nevýhod a dalších příležitostí směrnice

Předpokladem této práce bylo vytvoření univerzálního předpisu interní směrnice, kterou by bylo možné, s několika změnami, aplikovat v organizacích všech velikostí nebo předmětu činnosti. Výzkum však prokázal, že požadavky – a především praxe – malých podniků se výrazně liší od těch velkých. Ačkoliv tedy práce přednáší návrh jedné podoby směrnice, není možné ji bez větších úprav přímo využít pro všechny podniky, především pro ty malé. Příležitostí směrnice je tedy vytvoření jejich dalších variant, které by reflektovaly velikost podniku a z toho vyplvající specifika. Dalším vhodným rozvojem variant by mohlo být zaměření se na jednotlivé předměty činnosti podniků, jelikož výzkum práce potvrdil jejich významné rozlišnosti projevující se ve zpracování a přístupům k bezpečnostní dokumentaci.

Ve směrnici je zmiňován protokol a zpráva o provedené kontrole přístupových práv, která má být předložena vedení organizace. Na rozdíl od šablony formuláře pro žádost přidělení, změny nebo odebrání přístupových práv není tato zpráva pro vedení společnosti součástí navržené směrnice. Předpis určující tuto zprávu a její obsah by mohl být obsahem další práce, která by mohla obsahovat také postup při zjištění nedostatků a způsob přístupu k jejich řešení. Především by tato zpráva mohla sloužit pro rozvedení tématu reportingu, controllingu a souvisejícímu internímu auditu.

Výzkum v deseti organizacích se také zabýval existencí Matic neslučitelných rolí, definicí jednotlivých rolí a provedení analýzy rizik jednotlivých procesů. Neboť si práce kladla za cíl vytvořit směrnici v obecné rovině, nebyly provedeny analýzy rizik ani tvorba Matice neslučitelných rolí. Příležitostí jiné odborné práce by však mohlo být podrobení konkrétního podniku zkoumání a pro konkrétní podnik provést potřebné analýzy k definování rolí a jejich neslučitelnosti.

Za velkou příležitost směrnice je považován především její vzdělávací a informační charakter pro malé organizace. Ačkoliv neuvažují o zavedení této směrnice, jejím nastudováním došlo k významnému posunu v odborné vzdělanosti klíčových zaměstnanců, kteří si na jejím základě doplnili znalosti o zákonných požadavcích a také některé ze zásad best practice.

6 Závěr

Výstupem práce je návrh interní směrnice, která pojednává o řízení přístupových oprávnění k informačním systémům v podnicích. Návrh směrnice je v souladu s legislativou a respektuje poznatky tzv. „best practice“. V teoretické části této práce byla identifikována legislativa týkající se problematiky řízení práv. Zmíněná legislativa posouzena z pohledu významu na oblast bezpečnosti přístupových oprávnění. Dále byly analyzovány poznatky „best practice“, byla provedena jejich vzájemná komparace a provedena specifikace nejvýznamnějších poznatků.

V praktické části práce byly analyzovány přístupy k řízení přístupových práv z praxe na příkladu anonymizovaných firem. Byl proveden výzkum v rámci diplomní praxe, který zahrnoval studium interních směrnic deseti podniků různých velikostí a různých předmětů podnikání. Jednotlivé přístupy byly zkoumány z pohledu legislativních požadavků a srovnávány s identifikovanými zásadami „best practice“. Na základě hodnocení zkoumaných interních směrnic z pohledu stanovené legislativy a „best practice“ z teoretické části této práce byl vytvořen vlastní návrh interní směrnice. Na samotný závěr práce byl stanoven odhad finančního a personálního zatížení na zavádění navrhnuté interní směrnice ve zkoumaných organizacích.

Výstup této práce byl využit v praxi a je uvažováno o jeho dalším využití v jedné ze zkoumaných organizací.

7 Seznam použitých zdrojů

BASL Josef a NOVOTNÝ Ota, *ITIL a Cobit řídí komunikační technologie* [online]. Praha: Hospodářské noviny, 2004. [cit. 18.9.2018] Dostupné z: https://archiv.ihned.cz/c1-14454590-itil-a-cobit-ridi-komunikacni-technologie

BEHR, Alyson a COLEMAN, Kevin. *Separation of duties and IT security* [online]. CSO technolytics institute magazine, 2017. [cit. 8.7.2018] Dostupné z https://www.csoonline.com/article/2123120/government/separation-of-duties-and-it-security.html

BERNARD, Pierre. *Foundations of ITIL®* 2011 Edition. Van Haren, 2012. ISBN: 978 90 8753 923 8

BOSWORTH, Seymour a KABAY, M. E. *Computer Security Handbook*. Hoboken: John Wiley & Sons, 2002, str. 116 -136. ISBN 04-714-1258-9

BUCHALCEVOVÁ, Alena. *Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky*. 1. vyd. Praha: Grada, 2005. 163 s. Management v informační společnosti. ISBN 80-247-1075-7

COCKBURN, Alistair. *Growth of human factors in application development* [online]. 1995 [cit. 6.7.2018]. Dostupné z http://alistair.cockburn.us/Growth+of+human+factors+in+application+development

CLARK, D. D. a WILSON, D. R. *A comparison of commercial and military computer security policies*. Oakland: IEEE Symposium on Security and Privacy, 1987, s. 184-194.

End user devices security guidance [online]. Příručka. Londýn: 2016. [cit. 14.9.2018]. Dostupné z: https://www.ncsc.gov.uk/guidance/end-user-devices-security-guidance-introduction-0

FERRONI, Stefano. *Implementing Segregation of Duties: A Practical Experience Based on Best Practices* [online]. ISACA Journal, 2016, Volume 3. [cit. 28.12.2018]. Dostupné z: https://www.isaca.org/Journal/archives/2016/volume-3/Documents/Implementing-Segregation-of-Duties_joa_Eng_0516.pdf

GDPR. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

GRAMLING, Audrey A. *Addressing problems with the segregation of duties in smaller companies*. The CPA Journal, 2010, 80 (7), s. 30-34. ISSN 0749-8284

ISACA Information systems control journal. Illinois: Information Systems Audit and Control Association, 2017. ISSN 1526-7407

ISO/IEC 29146:2016 Information technology – Security techniques – A framework for access management [online]. Ženeva: ISO, 2016. [cit. 7.9.2018] Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:29146:ed-1:v1:en

KOBELSKY, K. A *Conceptual Model for Segregation of Duties: Integrating Theory and Practice for Manual and IT-supported Processes* [online]. International Journal of Accounting Information Systems, 2014, 15(4), str. 304-322. [cit. 29.12.2018] Dostupné z https://www.sciencedirect.com/science/article/pii/S1467089514000293?via%3Dihub

KOTLER, Philip a ARMSTRONG, Gary. *Principles of Marketing*. 9th ed. New Jersey: Prentice-Hall, 2001. 785 s. ISBN 0-13-029368-7

LEE, T.M.P. *Using mandatory integrity to enforce commercial security* [online]. IEEE Symposium on Security and Privacy. Oakland: 1988, s. 140-146. [cit. 7.7.2018] Dostupné z https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-160.pdf#page=147

LIGHTLE, Susan S. a VALLARIO, Cynthia W. *Segregation of duties in ERP: an automated assessment tool enables internal auditors at MeadWestvaco to enhance their SOD control reviews throughout the enterprise*. Internal Auditor, 2003. ISSN 0020-5745

MIČR (Ministerstvo informatiky ČR). *Národní strategie informační bezpečnosti České republiky* [online]. Praha: Ministerstvo informatiky ČR, 2005. [cit. 7.7.2018] Dostupné z https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-typ=tematicky&v=0addcddacc98e7a51b58564ca16eb256

MINISTR, Jan. *The influence of human resources on the IT service management.* [online] Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces. IEEE, 2013, s. 323-328. [cit. 30.12.2018] Dostupné z: https://ieeexplore.ieee.org/abstract/document/6649047

NASH, Michael J. a POLAND, Keith R. *Some conundrums concerning separation of duty* [online]. Research in Security and Privacy. Proceedings., 1990 IEEE Computer Society [cit. 19.9.2018] Dostupné z: https://www.computer.org/csdl/proceedings/sp/1990/2060/00/20600201.pdf

NILSSON, Hanieh. GDPR compliance and access control – what you should already be doing [online]. Specops password management and desktop deployment blog, 2018. [cit. 10.7.2018] Dostupné z https://specopssoft.com/blog/gdpr-compliance-access-control-already/

NÚKIB (NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST). *Věcný záměr zákona o kybernetické bezpečnosti - verze schválená vládou.* [online] Praha: Národní bezpečnostní úřad, 2012. [cit. 9.7.2018] Dostupné z:

https://www.nbu.cz/cs/aktualne/844-808-vecny-zamer-zakona-o-kyberneticke-bezpecnosti-verze-schvalena-vladou/

NÚKIB (NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST). *Aktuální legislativa.* [online] Praha: Národní bezpečnostní úřad, 2018a. [cit. 9.7.2018] Dostupné z: https://www.govcert.cz/cs/kyberneticky-zakon/legislativa/

NÚKIB (NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST). *Podpůrné materiály*. [online] Praha: Národní bezpečnostní úřad, 2018b. [cit. 15.7.2018] Dostupné z: https://nukib.cz/cs/kyberneticky-zakon/podpurne-materialy /

ORR, Anthony a BLOKKUM, Dag. *Best practice insight – focus on ITIL service design and operations.* [online] BMC Software Inc., 2016. [cit. 29.12.2018] Dostupné z: http://bmc.lookbookhq.com/itil/476468.pdf

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

STUPKA, Václav. Kybernetická bezpečnost v České republice [online]. Brno, 2018 [cit. 20.10.2018]. Disertační práce. Masarykova univerzita, Právnická fakulta. Dostupné z https://theses.cz/id/plyrf9/.

Symposium on. IEEE, 1990, s. 201-207. [cit. 6.7.2018] Dostupné z http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.8374&rep=rep1&type=pdf

SHOCKLEY, W. R. *Implementing The Clark/Wilson Integrity Policy Using Current Technology* [online]. Eleventh National Computer Security Conference. Baltimore: 1991, s. 29-37 [cit. 7.7.2018] Dostupné z https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-160.pdf#page=163

ŠKORNIČKOVÁ, Eva. *Co považuje GDPR za osobní údaje* [online]. Praha, 2018 [cit. 2.9.2018]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

VRANA, Ivan a RICHTA, Karel. *Zásady a postupy zavádění podnikových informačních systémů: praktická příručka pro podnikové manažery*. Praha: Grada Publishing a.s., 2005. 188 s. ISBN 80-247-1103-6

Vyhláška č. 82/2018 Sb. ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Sbírka zákonů. 1.1 2015. ISSN 1211-1244

Zákon 181/2014 Sb. ze dne 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

ZEMAN, P. *Česká bezpečnostní terminologie.* 1.vyd. Masarykova univerzita v Brně, 2002. 186 s. ISBN 80-210-3037-2, str. 39