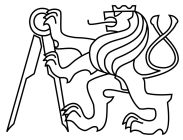
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Analýza problematiky stínového IT
Student:	Bc. Tomáš Zatřepálek
Vedoucí:	Ing. Pavel Náplava
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2016/17

Pokyny pro vypracování

Definujte pojem "stínové IT" a analyzujte, jakým způsobem se tato oblast vyvíjí. Na základě analýzy vymezte hranici mezi "běžným" a "stínovým IT". Zaměřte se na segment SMB a vytvořte tři typické modely fungování těchto společností s ohledem na problematiku stínového IT (otevřená firma, restriktivní firma, elastická firma). Parametry modelů založte minimálně na základě technologických, procesních a finančních parametrů. Pomocí těchto modelů demonstrujte benefity a rizika "stínového IT". Následně vytvořte „simulační“ model, pomocí kterého bude možné nalézt a doporučit "optimální" model využívání "stínového IT" pro různé typy SMB společností. Model ověřte na několika příkladech SMB firem. Na základě modelu potvrďte/vyvraťte hypotézu, že proaktivní přístup ke "stínovému IT" může zvýšit elasticitu a flexibilitu SMB firem za předpokladu minimálního růstu investic a rizik s ním spojených.

Seznam odborné literatury

Dodá vedoucí práce.

L.S.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

prof. Ing. Pavel Tvrdík, CSc.
děkan

V Praze dne 1. února 2016

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra softwarového inženýrství

Diplomová práce

Analýza problematiky stínového IT

Bc. Tomáš Zatřepálek

Vedoucí práce: Ing. Pavel Náplava

9. května 2016

Poděkování

Rád bych poděkoval Ing. Pavlovi Náplavovi za vedení této diplomové práce, za vstřícnost a čas věnovaný pravidelným konzultacím, za odborný dohled, věcné připomínky, pomoc a rady při vypracování této práce. Chtěl bych poděkovat také prof. Ing. Janovi Dohnalovi, CSc. za pomoc při formulování směru, kterým se tato práce ubírá, a za poskytnutí cenných materiálů a osobních zkušeností s problematikou stínového IT. Děkuji firmě Safetica Technologies s.r.o. a především jejím zaměstnancům Ing. Zbyňkovi Sopuchovi, Ph.D. a Ing. Mateji Zacharovi za úpravu a poskytnutí cenných dat z prostředí českých podniků. Chtěl bych také poděkovat anonymním firmám za možnost realizace praktického výzkumu. Poděkování patří i mým rodičům, kteří mě po celou dobu studií podporovali a umožnili mi se plně věnovat vypracování práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 9. května 2016 .....

Odkaz na tuto práci

Zatřepálek, Tomáš. *Analýza problematiky stínového IT*. Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2016.

Abstrakt

Diplomová práce ze zabývá problematikou stínového IT, tj. existencí hardwarových, softwarových i jiných řešení, která jsou součástí informačního ekosystému podniku, bez vědomí IT oddělení. V práci jsou shrnuty poznatky z odborné literatury, proveden průzkum tohoto fenoménu v českých firmách a představen model pro přístup ke stínovému IT v podniku.

Klíčová slova Stínové IT, soulad byznysu s IT, řízení podnikové informatiky, CIO, IT oddělení, podniková informatika, informační bezpečnost, konzumerizace IT

Abstract

This diploma thesis deals with the issue of shadow IT, ie. the existence of hardware, software and other solutions which are part of the enterprise information ecosystem without the awareness of the IT department. The thesis summarizes the findings from the literature, conducts a survey of this phenomenon in Czech companies and introduces a model for shadow IT controlling in the enterprise.

Keywords Shadow IT, business-IT alignment, IT Governance, CIO, IT department, enterprise informatics, information security, IT consumerization

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Předmluva

Tato práce se zabývá problematikou stínového IT, která vlivem technologického vývoje a změnou postojů vedení podniků v posledních letech opět získala na významu pro podnikovou informatiku [1, s. 5]. Pojem stínové IT představuje hardwarová, softwarová i jiná řešení, která jsou součástí informačního ekosystému podniku a fungují bez vědomí IT oddělení [2, s. 274].

Práce je rozčleněna do osmi kapitol. Kapitoly 1 až 5 se týkají rešerše literatury na dané téma a jsou čistě teoretické. Další kapitoly pak představují praktickou část této diplomové práce. V kapitole 6 provádím vlastní průzkum s cílem získání základní představy o stavu stínového IT v Čechách. V kapitole 7 na základě dat dodaných společností Safetica Technologies s.r.o. tvořím modely tří nejčastějších typů firem a interpretuji význam získaných dat. Poslední kapitola č. 8 se pak věnuje tvorbě simulačního modelu stínového IT, je ověřena hypotéza proaktivního přístupu a diskutován finanční pohled na tuto problematiku.

Práce je určena především firemnímu vedení (CEO) a vedení podnikové informatiky (CIO). Přináší ucelený pohled na tuto problematiku optikou převážně zahraniční odborné literatury, zároveň práce obsahuje i praktický průzkum tohoto fenoménu v podmínkách České republiky.

Motivace

Stínové IT úzce souvisí s řízením IT, protože k jeho vzniku často vede nesoulad mezi IT a byznysem [2, 3], a je náplní oboru, který studuji a kterému se hodlám věnovat i v budoucnu. Navíc se jedná v současné době o velmi diskutovanou oblast, která je často zmiňována v souvislosti s novými postupy pro řízení IT [2, s. 275-276]. Proto bych rád prohloubil své poznání této nové problematiky, přispěl k uspořádání znalostí v přehledné formě a ověřil tyto znalosti v praxi.

Cíl práce

Cílem práce je uspořádání dosavadních znalostí o problematice stínového IT, vytvoření modelů fungování firem ve vztahu ke stínovému IT a identifikace benefitů a rizik těchto modelů. Dalším z cílů je ověření hypotézy (pomocí simulačního modelu na příkladech konkrétních SMB firem), že proaktivní přístup ke stínovému IT může zvýšit elasticitu a flexibilitu firem za předpokladu minimálního růstu investic a rizik s ním spojených.

Kapitola 1

Vymezení stínového IT

Stínové IT se podle Walterse [1, s. 5] stalo v poslední době často skloňovaným pojmem především díky technologickému vývoji, ke kterému došlo během uplynulé dekády. Samotný význam pojmu stínové IT byl užíván už s příchodem stolních počítačů [4], v současné době však opět získal na důležitosti a změnilo se i jeho vnímání z pohledu řízení informatiky [5, 6]. V této kapitole je představena definice pojmu, historický pohled a předpokládaný vývoj v budoucnu, změna našeho chápání této problematiky a vymezení hranice mezi stínovým a firemním IT.

1.1 Definice pojmu

V literatuře se objevují různé definice stínového IT v závislosti na zaměření zdroje. Silic a Back [2, s. 274] definují stínové IT jako „Veškerý hardware, software a jiná řešení používaná zaměstnanci ve firemním informačním ekosystému bez souhlasu IT oddělení“ (překlad autora[1]). Velmi podobnou definici uvádí např. Cappuccio [7], Johnson [8, s. 5] nebo McCafferty [9, s. 1]. Tato definice je zároveň dostatečně obecná na to, aby postihovala další definice s užším zaměřením jako např. neautorizované systémy na nepovolených zařízeních v podnikovém prostředí [1, s. 5], systémy replikující data a funkce formálně schválených systémů [10, 3] nebo uživateli (mimo IT oddělení) zajišťovaná řešení [11].

> “Veškerý hardware, software a jiná řešení používaná zaměstnanci ve firemním informačním ekosystému bez souhlasu IT oddělení”
>
> Silic a Back [2, s. 274]

[1] Původní znění: „It represents all hardware, software, or any other solutions used by employees inside of the organisational ecosystem which have not received any formal IT department approval.“

Pojem stínové IT se v anglicky psané literatuře označuje nejčastěji jako *shadow IT* případně *shadow systems* (pokud se jedná o označení konkrétních systémů nebo aplikací). Další a méně častá označení jsou *workaround systems*, *feral systems*, *rogue applications* [10, 2], *dark IT* [2, 12] nebo *stealth IT* [4]. V českém jazyce se používá především termín *stínové IT*, lze narazit i na označení *partyzánské IT* [13, s. 2].

Na význam tohoto pojmu je třeba pohlížet ze dvou úhlů [7]:

1. Pohled optikou 80. a 90. let (V1 dle Cappuccia [7]): Problematika je adresována obecně jako záležitost informační bezpečnosti (není používán termín stínové IT, ačkoliv odpovídá pozdější definici), soustředí se především na PC aplikace, síťovou bezpečnost a datovou bezpečnost (s příchodem internetového připojení a e-mailové komunikace) [4] a představují ji i zaměstnanci mimo IT oddělení, kteří svými dovednostmi často nahrazovali IT podporu pro méně zkušené uživatele a svou činností způsobovali chaos v podnikové informatice [7].

2. Pohled po roce 2000 (V2 dle Cappuccia [7]): Termín stínové IT začíná být hojně používán i v akademické literatuře, opětovný zájem o tuto oblast je zapříčiněn především konzumerizací IT [2, s. 274] a nástupem politiky BYOD[2] [14] a cloudových služeb [2, s. 274]. Tvorba a růst stínového IT v podniku je poháněna potřebami byznysu, požadavky na rychlost implementace a reakcí na vývoj okolního trhu [7].

U řešení, která jsou v informačním ekosystému podniku zaměstnanci používána bez vědomí IT oddělení, je navíc třeba rozlišovat dvě skupiny podle účelu jejich používání. První skupinu tvoří nástroje sloužící pro soukromé potřeby zaměstnanců, druhou nástroje související s prací v podniku. Definice Silice a Backa [2, s. 274] zahrnuje obě skupiny. Avšak pohnutky zaměstnanců, kteří v podnikové informatice vytváří stínové IT kvůli soukromým záležitostem, by se daly zkoumat z mnoha pohledů od psychologie, sociologie, až po pracovní etiku, a proto do oblasti zájmu této práce, kterým je především řízení IT podniku, nepatří. Stínové IT sloužící pro soukromé účely bude v práci posuzováno z hlediska dopadů na informatiku (zvláště pak na bezpečnost), nebudou však rozváděny důvody jeho vzniku.

1.1.1 Historie a předpokládaný vývoj

V této části je popsán vývoj stínového IT od jeho prvních výskytů s příchodem osobních počítačů v 80. letech 20. století a až do současnosti, kdy se mění množství pozornosti, které mu řízení informatiky věnuje, a závažnost jeho dopadů na celý podnik. Původně okrajový problém, který má dopady především

[2]BYOD (z anglického Bring Your Own Device) znamená možnost zaměstnanců používat ve firemním prostředí soukromá zařízení.

na informační bezpečnost, se dostává do centra pozornosti IT oddělení s příchodem k internetu, kdy dochází k nárůstu závažnosti rizik s ním spojených, a řízení podnikové informatiky na ně účinně reaguje zaváděním restriktivní politiky. Příchod mobilních zařízení, rostoucí konzumerizace IT a rychlého vývoje nových technologií mění pohled řízení podniku na tento problém a dochází ke snaze opustit restriktivní přístup a využít předností stínového IT při současném udržení rizik na přijatelné úrovni. V následujících odstavcích je celý tento vývoj popsán podrobněji.

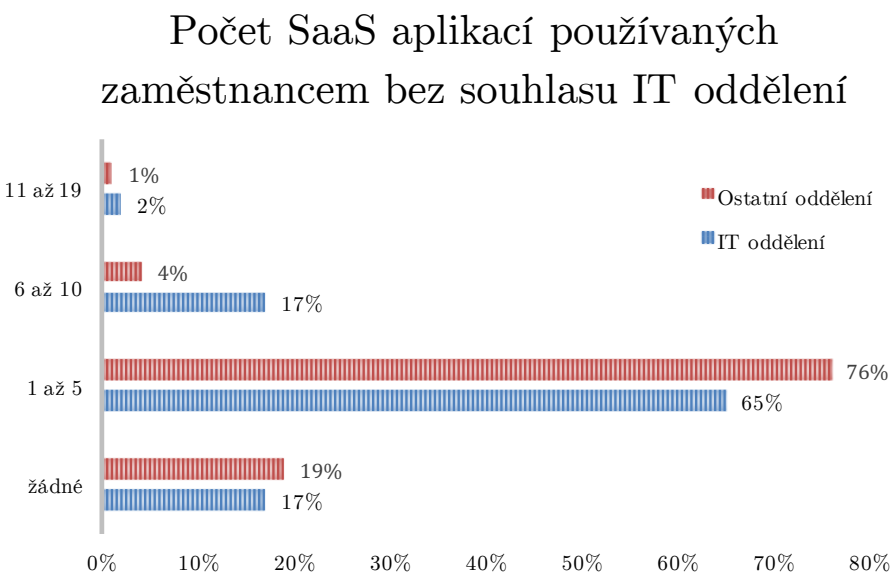
V 80. letech 20. století se podniková informatika proměňuje a od mainframů se přechází k tvorbě infrastruktury založené na osobních počítačích. Vzniká potřeba přenášet mezi jednotlivými PC data a jsou vytvářeny ad hoc sítě počítačů [4]. Při řešení potíží se zaměstnanci často obracejí na své kolegy, kteří nejsou z IT oddělení. Jejich činností vzniká chaos, který můžeme označit za ranou podobu stínového IT [7]. V reakci IT oddělení na nové změny a potřeby podniku začíná být vytvářena formální síťová architektura a zaváděn model klient-server [4].

V 90. letech 20. století do podnikové informatiky vstupuje připojení k internetu a další nové technologie, především e-mail a World Wide Web. IT oddělení musí kromě bezpečnosti stolních počítačů zajistit podnikovou síť firewallem, spravovat e-mailové a webové servery, případně umožnit přístup do podnikové sítě z internetu skrze VPN [4]. Na konci dekády uživatelé (kromě instalace vlastního softwaru nebo zpracování osobních dat na firemních počítačích) často vytvářejí stínové IT nastavováním e-mailových filtrů na přeposílání pošty na soukromý e-mail mimo podnik nebo plněním podnikových serverů soukromými daty (např. hudbou, videy a fotografiemi) [12].

Na přelomu tisíciletí zaměstnanci narušují bezpečnost přinášením vlastních dat nebo softwaru na USB flash discích a jiných zařízeních (např. iPodech [1, s. 5]). Připojováním vlastních Wi-Fi routerů (často nechráněných šifrováním a autentifikací) do podnikové sítě pak zaměstnanci vytvářejí další závažné zranitelnosti v zabezpečení podnikového ekosystému [12]. IT oddělení úspěšně reagují na tyto změny zaváděním restriktivní politiky a snaží se co nevíce omezit možnosti uživatelů stínové IT v podniku vytvářet.

K velké změně dochází po roce 2000 s příchodem mobilních zařízení a konzumerizací IT. Zaměstnanci podniku ve stále větší míře používají nejnovější zařízení a aplikace na trhu a pokud jim mohou usnadnit práci, často je používají na pracovišti bez vědomí IT oddělení, k čemuž přispívá i zavádění politiky BYOD [1, s. 6]. Řízení informatiky má velmi ztíženou pozici v otázce kontroly podnikových dat a monitorování rozsahu stínového IT v podniku se stává velmi nesnadným [2, s. 278].

Krátce po příchodu mobilních zařízení vstupují do podnikové informatiky cloudové služby a model Software as a Service (výstkyt tohoto modelu v rámci stínového IT ilustruje obrázek 1.1). Tyto služby jsou často oficiálně nakupovány a provozovány bez vědomí IT oddělení jinými odděleními v podniku (především obchodním a marketingovým [5, s. 23]), což může vést k vytváření

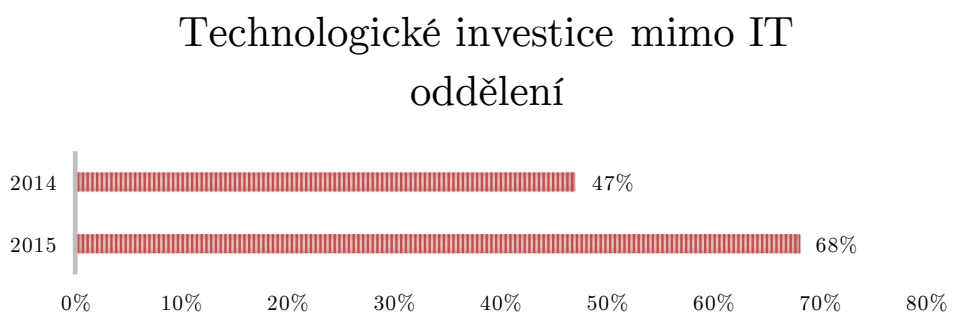


Obrázek 1.1: Rozsah používání SaaS aplikací zaměstnanci podniku bez formálního souhlasu IT oddělení. [15, s. 4]

duplicitních procesů i dat. Hlavním důvodem pro takovéto obcházení standardních procesů pro výběr, nákup a zavedení nových aplikací je rychlost a jednoduchost nákupu a provozu a konkurenceschopnost řešení na trhu [1, 7]. Zároveň v podnicích sílí tlak hlavního vedení na řízení podnikové informatiky, aby podporovalo politiky BYOD (případně BYOS/BYOA) a cloudové služby kvůli jejich pozitivnímu dopadu na výkon zaměstnanců [14, 1].

Jedna z hlavních priorit řízení podnikové informatiky je zajištění integrity a bezpečnosti dat, která je silně narušována obcházením standardních schvalovacích procesů. Tyto procesy jsou z pohledu ostatních oddělení příliš pomalé, a proto jsou obcházeny a dochází k tvorbě stínového IT. V případě, že se IT oddělení snaží tomuto obcházení bránit, dochází ke snaze omezení kompetencí IT oddělení. [14]

V současné době mezi vedením podnikové informatiky a hlavním vedením podniku dochází ke sjednocení postojů, aby IT oddělení lépe podporovalo potřeby ostatních oddělení a zároveň byly dodrženy standardy bezpečnosti dat. Julia Kingová [5, s. 21] předpokládá, že v postoji IT oddělení nevyhnutelně dojde ke změně a začne nabízet své znalosti ostatním oddělením žádaným způsobem. Konzumerizace IT a vzestup stínového IT bude pokračovat, proto IT oddělení musí získat náskok před ostatními částmi podniku a být schopno jim nabídnout novou službu nebo technologii dříve, než sami přijdou s požadavkem na jejich nákup, nebo IT oddělení obejdou [5, s. 21-22]. IT oddělení bude muset poskytovat podporu i školení ostatním zaměstnancům, pomáhat



Obrázek 1.2: Porovnání objemu investic do digitálních technologií mimo rozpočet IT oddělení v letech 2014 a 2015. [18, s. 5]

jim nástroje udržovat a zvyšovat jejich produktivitu [5, s. 22].

Podle současných předpovědí se odhaduje, že role stínového IT bude v budoucnu stále důležitější. Například Gartner předpovídá, že v roce 2020 budou počítačově gramotní zaměstnanci ostatních oddělení, kteří stínové IT vytvářejí, převyšovat zaměstnance IT oddělení v poměru 4:1, zatímco ještě v roce 2005 byl poměr gramotných zaměstnanců 1:9 [16]. Další predikce Gartneru [17] odhaduje, že v roce 2017 bude čtvrtina podniků využívat vlastní obchody s aplikacemi, resp. repozitáře aplikací, které bude spravovat IT oddělení a zaměstnanci si z nich budou instalovat a aktualizovat aplikace stejně snadno, jako jsou zvyklí u svých soukromých aplikací.

Další předpovědi naznačují, že v nejbližších letech bude role CIO oslabena a oddělení marketingu a obchodu budou samostatně rozhodovat o 10 [14] až 35 [5, s. 20] procentech všech výdajů na podnikovou informatiku. Podle studie [18, s. 5] z roku 2015 (na obrázku 1.2) je 68 % (ve střední a východní Evropě dokonce 73 %) technologických investic v podniku je hrazeno z rozpočtů jiných oddělení. Není zde sice zmíněno, zda se jedná o rozhodnutí bez vědomí IT oddělení, nicméně lze předpokládat, že značné rozhodovací pravomoci budou úzce svázány se zdrojem financování. Navíc nárůst takovýchto investic je oproti předchozímu roku o 21 % vyšší a potvrzuje předpovídaný trend.

1.1.2 Hranice mezi firemním a stínovým IT

Protože stínové IT v současné době nabývá na důležitosti pro podnikovou informatiku, je důležité vymezit hranici mezi ním a formálním firemním IT. Podle Walterse [1, s. 6] dochází stále více k propojení osobního a pracovního života a hranice mezi pracovními a soukromými aplikacemi je nejasná. V této práci používám definici „Veškerý hardware, software a jiná řešení používaná zaměstnanci ve firemním informačním ekosystému bez souhlasu IT oddělení“ (překlad autora) [2, s. 274]. Důležitý je tedy souhlas IT oddělení, který může být formální (dokumentovaný, definovaný firemním procesem) i neformální

(ústní formou). V obou případech se jedná o souhlas na úrovni vedení oddělení (vedení ví o takovém rozhodnutí), nikoliv o souhlas řadového zaměstnance IT oddělení bez vědomí vedení o tomto rozhodnutí.

Stínové IT tedy může představovat například aplikace, která je určena pro korporátní sféru, zatímco do firemního IT může patřit program původně určený pro domácí uživatele a naopak. Nezáleží na cílení nástroje, jeho licenci ani podstatě (může se jednat i o hardwarové zařízení nebo jen o neautorizované nastavení schválené aplikace), pouze na odsouhlasení IT oddělením. To je dobrá zpráva z hlediska rozhodování o tom, co je a co není stínovým IT, při posuzování konkrétního nástroje. Naopak nesnadným problémem je odhalení takového nástroje. Uspořádání stínového IT do kategorií, důvodům jeho vzniku, jeho dopadům a způsobům jeho vyhledávání a kontroly v podniku se věnuji v následujících kapitolách.

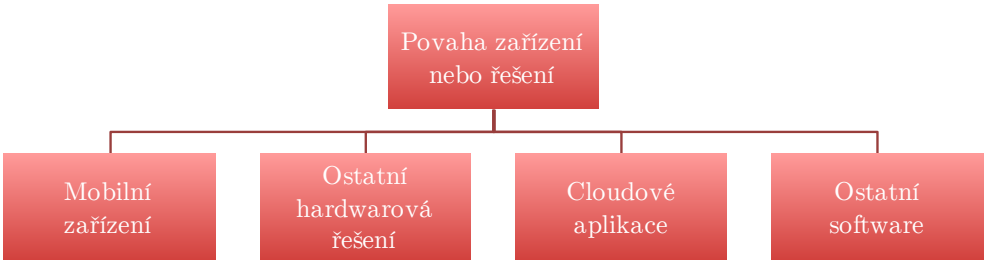
Kapitola 2

Uspořádání forem stínového IT

V této kapitole jsou představena dělení konkrétních forem stínového IT. První dvě obecně pokrývají celou oblast, další dvě se pak zaměřují pouze na softwarové formy. Představená dělení jsou na sobě nezávislá a příslušnost konkrétních forem do daných skupin mezi sebou nemusí nijak souviset. Obsah této kapitoly vychází zejména z rešerše literatury provedené Silicem a Backem [2], výstupem jejich výzkumu a informacemi z dalších studií na toto téma [19, 15].

2.1 Podle povahy zařízení nebo řešení

Toto uspořádání (viz obrázek 2.1) vychází z fyzické povahy dané formy nebo ze způsobu jejího využívání. Obecně by bylo možné vytvořit dvě obsáhlé skupiny pro hardware a software, vzhledem k historickému vývoji a dnešnímu významu určitých podob stínového IT ale bylo zvoleno dělení, na které budou lépe navazovat další kapitoly této práce. To z původních skupin vyčleňuje mobilní zařízení a cloudové aplikace.



Obrázek 2.1: Uspořádání forem stínového IT podle povahy zařízení/řešení.

2.1.1 Mobilní zařízení

Do této kategorie patří všechna přenosná koncová uživatelská zařízení. Tato skupina nabrala na důležitosti především s častějším aplikováním politiky BYOD v podnicích a dále rozvojem na poli informačních technologií. Patří sem především chytré telefony, tablety a notebooky.

2.1.2 Ostatní hardwarová řešení

V této kategorii se nacházejí ostatní hardwarová zařízení, která nejsou ve skupině předchozí. V praxi se nejčastěji jedná o síťové prvky (WiFi routery, switche), tiskárny nebo příslušenství ke stolním počítačům.

2.1.3 Cloudové aplikace

Tuto skupinu tvoří softwarové nástroje, které jsou alespoň z části nebo zcela provozovány mimo podnik, zpravidla prostřednictvím internetu. Nejčastěji se jedná o aplikace dodávané formou SaaS, například datová úložiště, informační systémy nebo webové služby.

2.1.4 Ostatní software

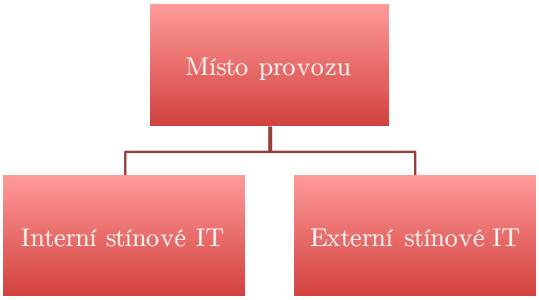
Do poslední kategorie patří ostatní software, který nevykazuje znaky předchozí skupiny. Může se jednat například o firmware, aplikace běžící na mobilních zařízeních zaměstnanců podniku stejně jako o programy instalované na firemní počítače. V praxi jsou typickými zástupci této skupiny programy, které jsou snadno dostupné (open-source a shareware licence, zdarma pro osobní použití a podobně) [2, s. 278].

2.2 Podle místa provozu

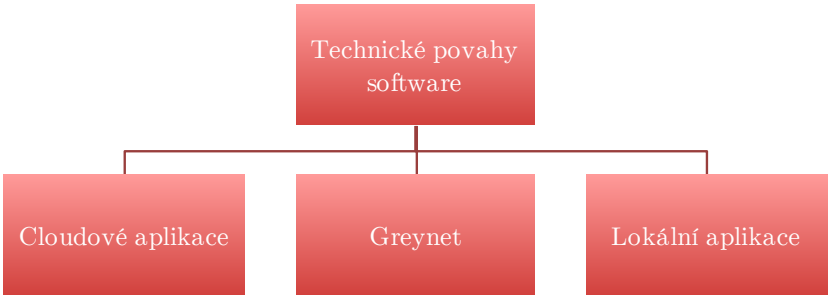
Toto dělení (na obrázku 2.2) vychází z faktu, zda je stínové IT provozováno přímo na schválené (formální) infrastruktuře, nebo zda podnikovou infrastrukturu neschváleným způsobem rozšiřuje.

2.2.1 Interní stínové IT

Formy spadající do této kategorie jsou zpravidla provozovány na existujících komponentách podnikové informační infrastruktury. Jedná se například o neschválené úpravy v nastavení nebo neodsouhlasené instalace software na firemní počítače.



Obrázek 2.2: Uspořádání forem stínového IT podle místa provozu.



Obrázek 2.3: Uspořádání forem stínového IT podle technické povahy software.

2.2.2 Externí stínové IT

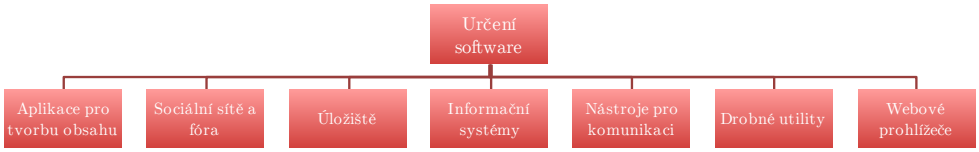
Tuto kategorii tvoří soukromá zařízení zaměstnanců a aplikace, která využívají infrastruktury, o které nemá IT oddělení podniku přehled. Kromě mobilních zařízení zaměstnanců bývají častou formou cloudové aplikace nebo další soukromý hardware (např. WiFi router).

2.3 Podle technické povahy software

U softwarových forem stínového IT lze na základě jejich architektury rozlišit tři skupiny (na obrázku 2.3): cloudové aplikace, greynet a lokální aplikace. Toto dělení vychází ze způsobu práce softwaru s daty a má dopady na rizika spojená se zabezpečením podnikových dat.

2.3.1 Cloudové aplikace

Aplikace provozované v cloudu ukládají data mimo podnik na infrastruktuře dodavatele nebo dodavatelem pronajaté. Klientskou aplikací je zpravidla webový prohlížeč, nebo jednoduchá mobilní či desktopová aplikace, která přenáší data do cloudu (nejčastěji přes internetové připojení). Ta jsou zde zpracována a výstupy zpracování jsou posílány zpět do klientské aplikace.



Obrázek 2.4: Uspořádání forem stínového IT podle určení software.

Nejčastějšími zástupci jsou datová úložiště nebo informační systémy a webové služby nabízené formou SaaS.

2.3.2 Greynet

Software označovaný jako greynet [2] posílá data po síti pomocí různých síťových protokolů, často se jedná o peer-to-peer komunikaci. Takovéto aplikace mohou svým provozem zahlcovat podnikovou síť. Jako typické zástupce můžeme jmenovat například peer-to-peer klienty pro sdílení souborů, různé doplňky pro webové prohlížeče (toolbary) nebo komunikátory (Skype, dříve např. ICQ).

2.3.3 Lokální aplikace

Programy instalované přímo na koncová zařízení jsou zařazeny do této poslední skupiny. Sem patří především programy, které nepotřebují pro své hlavní funkce počítačovou síť nebo připojení k internetu. Mohou být instalovány například na stolních počítačích, noteboocích nebo chytrých telefonech. Většinou slouží pro tvorbu obsahu (tvorba a úprava souborů), manipulaci s dokumenty (komprimace, archivace) nebo správu nastavení daného zařízení (čištění mezipaměti).

2.4 Podle určení software

Poslední čtvrté dělení v této kapitole vychází z nabízené funkcionality daného softwaru (na obrázku 2.4). Převážná část stínového IT vzniká kvůli zvýšení produktivity zaměstnanců (toto téma je podrobněji probráno v kapitole 3) a jeho výskyt v podniku zpravidla závisí na zaměření firmy a agendě jejích zaměstnanců.

2.4.1 Aplikace pro tvorbu obsahu

Do této kategorie patří programy (nikoliv však informační systémy), které produkují dokumenty a soubory přímo související s činností podniku (produkty vnitřních procesů nebo výstupy činnosti podniku). Rozsáhlou skupinou

aplikací jsou kancelářské balíky (například Open Office, Google Apps, Microsoft Office Online) obsahující například textové a tabulkové procesory; tyto nástroje často umožňují i kolaboraci mezi více uživateli, primární určení je však tvorba dokumentů, a proto byly zařazeny do této kategorie a nikoliv do kategorie Nástroje pro komunikaci. Patří sem i další software jako typografické nástroje na sazbu, grafický software a další programy s komplexnější funkcionalitou.

2.4.2 Sociální sítě a fóra

Sociální sítě slouží především pro kolaboraci s kolegy uvnitř i mimo podnik, fóra pak pro vyhledávání informací. Zaměstnanci na sociálních sítích (především Facebooku a Google+) kromě soukromých záležitostí často probírají i ty pracovní. Dále je využívají pro koordinaci své práce a pro sdílení souborů a obrázků (například fotografie zápisu z porady a podobně). Fóra zaměřená na konkrétní tématiku pak slouží pro vyhledání informací nebo položení dotazu komunitě (například vývojářské Stack Overflow). Tyto nástroje často pomohou zaměstnancům v jejich produktivitě, nesou s sebou však riziko vynášení citlivých informací mimo firmu.

2.4.3 Úložiště a sdílení souborů

Pro přenos velkých souborů nebo pro kolaboraci na konkrétním projektu zaměstnanci využívají datová úložiště a služby na sdílení souborů. Úložiště jsou využívána především pro přenos dat, kdy je přenášený soubor příliš velký nebo podnik nemá obdobný nástroj (nebo je dostupný pouze vnitřní sítě podniku). Služby na sdílení souborů jsou používány zejména pro spolupráci více zaměstnanců nad společnými soubory ale i pro sdílení dat se zákazníkem. Služby jako například Dropbox nabízí snadnou integraci na různých platformách a zařízeních a jsou dostupné mimo podnik. Výhodou těchto řešení je rychlost, snadnost použití a cena (často zdarma), rizikem pak únik citlivých informací nebo ztráta dat.

2.4.4 Informační systémy

V této kategorii se nachází informační systémy, které z různých důvodů nedostaly formální souhlas IT oddělení (důvody jsou zmíněny v kapitole Příčiny vzniku stínového IT). Jedná se především o systémy pro jiná než IT oddělení (zejména marketingové oddělení) nebo užší vedení podniku. Nejčastěji to jsou CRM (marketinové analýzy), Business Intellignce, nebo ERP formou SaaS.

2.4.5 Nástroje pro komunikaci

Do této kategorie spadají všechny aplikace a nástroje primárně sloužící pro komunikaci. Jedná se o různé komunikátory (Skype, Slack), webmail (gmail.com,

hotmail.com, seznam.cz) servery nebo webové (video) konference.

2.4.6 Drobné utility

Do této kategorie spadají programy a aplikace s jedinou nebo velmi omezenou funkcionalitou. Často se jedná o nástroje pro manipulaci s PDF soubory (slučování, rozdělování, přidání podpisu), konvertory mezi různými formáty, kodeky, videokonvertory, portable aplikace. Velmi častou aplikací je také CCleaner sloužící pro vymazání nepotřebných souborů operačního systému Microsoft Windows.

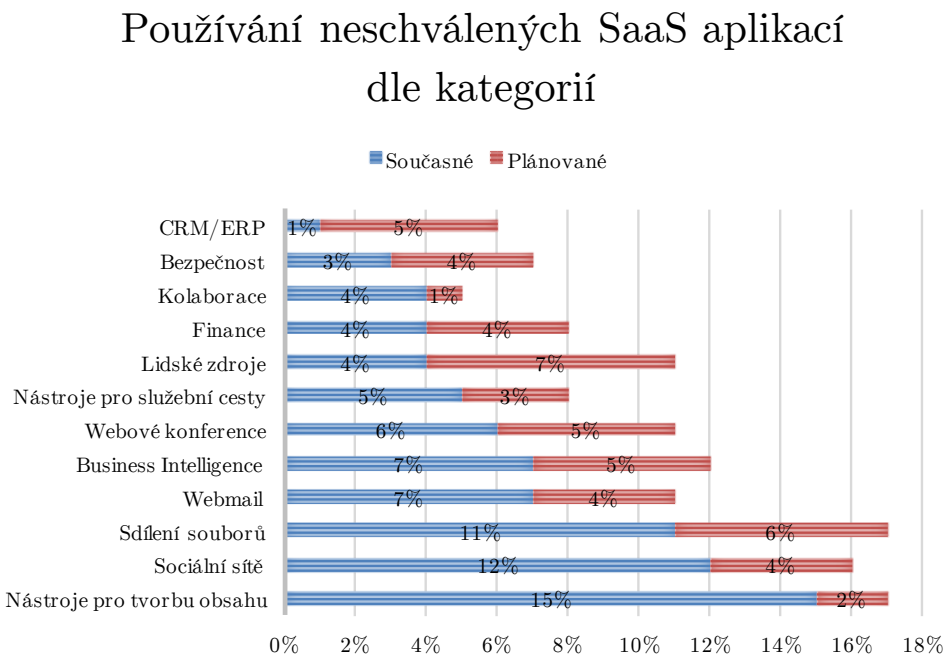
2.4.7 Webové prohlížeče

Mezi často používané neschválené programy patří internetové prohlížeče. Mohou být instalovány přímo na firemním zařízení, pokud to nastavení daného zařízení umožňuje, nebo používány ve formě portable aplikací. Do samostatné kategorie jsou zařazeny z důvodu častého výskytu a jejich úzkého zaměření.

2.5 Předpokládaný vývoj

V této kapitole bylo představeno dělení na základě významu a současného stavu stínového IT. Cílem tohoto uspořádání je vytvoření základu pro orientaci v problematice stínového IT a navazuje se na něj v kapitole 3 zabývající se příčinami a také v kapitole 6 věnované výzkumu stínového IT v České republice (struktura dotazníku pro interview vychází právě z tohoto dělení).

V budoucnu však mohou vzniknout nové kategorie nebo stávající se mohou stát více nebo méně významnějšími. V nejbližší budoucnosti bude pravděpodobně významnou roli hrát využívání informačních systémů ve formě cloudových aplikací (podobný trend je vidět na grafu ze studie společnosti Frost & Sullivan na obrázku 2.5). Význam a četnost stínového IT závisí na hlavních motivátorech pro jeho vznik. Ty jsou podrobně probrány v následující kapitole.



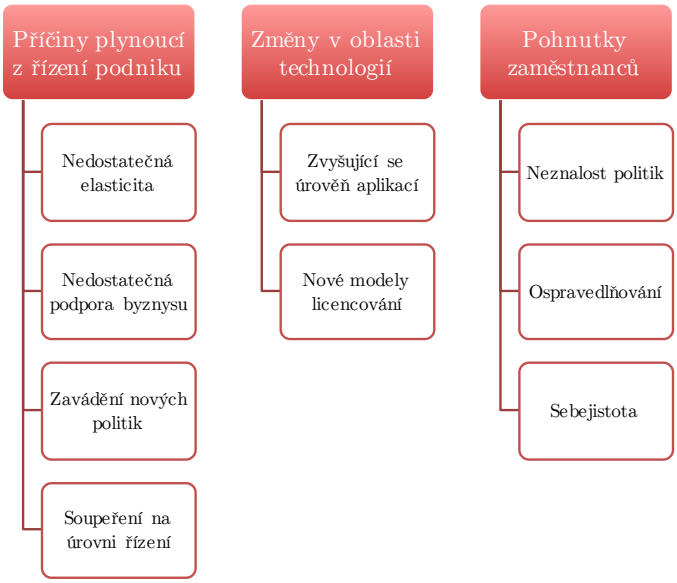
Obrázek 2.5: Míra používání neschválených SaaS aplikací dle kategorií. [15]

Kapitola 3

Příčiny vzniku stínového IT

Ačkoliv do problematiky stínového IT dle definice patří vše od hardwarových zařízení, přes softwarové nástroje až po neautorizovaná nastavení podnikového IT, analýza příčin jejich vzniku umožňuje lépe porozumět stínovému IT jako celku. V této kapitole uspořádáme důvody do skupin, podrobněji popíšeme jejich kontext a zmíníme některé typické formy stínového IT, které takto vznikají.

Obecně ke vzniku konkrétní podoby stínového IT vede zpravidla více důvodů. Proto je třeba v praxi počítat s kombinací více faktorů. Následující dělení (na obrázku 3.1) vždy uvádí jeden konkrétní důvod vzniku, charakterizuje jeho kontext (ve kterém hraje tento důvod zásadní roli) a popisuje nejčastější výstupy ve formě konkrétní podoby stínového IT.



Obrázek 3.1: Uspořádání příčin vzniku stínového IT.

3.1 Příčiny plynoucí z řízení podniku a podnikové informatiky

Následující příčiny vzniku stínového IT úzce souvisí se způsobem vedení celého podniku nebo samotného IT oddělení. Jedná se o neefektivní procesy nákupu a nasazení požadovaného řešení, nesoulad mezi podnikovou informatikou a byznys odděleními, zavádění nových politik nebo soupeření o pravomoci v rozhodování o firemní informatice. Typickým produktem je stínové IT v podobě cloudových aplikací licencovaných jako SaaS.

3.1.1 Nedostatečná elasticita podniku

Standardní procesy nákupu a zavádění požadovaných změn ve firemním IT trvají příliš dlouho a uživatelé se je snaží obcházet. Nejčastěji se jedná o software poskytovaný formou licence Software as a Service (četnost modelu SaaS potvrzuje i obrázek 3.2), který je provozován bez vědomí IT oddělení (např. používání Dropboxu marketingovým oddělením - viz obrázek 3.3). [1, 5]

3.1.2 Nedostatečná podpora byznysu od IT oddělení

S příchodem politiky BYOD často přecházela na IT oddělení zodpovědnost za podporu soukromých zařízení zaměstnanců. Pro IT oddělení byl tento požadavek jedním z nejčastěji uváděných zdrojů frustrace a navyšování počtu podporovaných zařízení znamenalo zhoršení produktivity oddělení. [1, s. 8] Typicky takto dochází ke stahování neschválených programů zaměstnanci [1, s. 6] nebo k neodsouhlaseným úpravám v nastavení aplikací a zařízení [7].

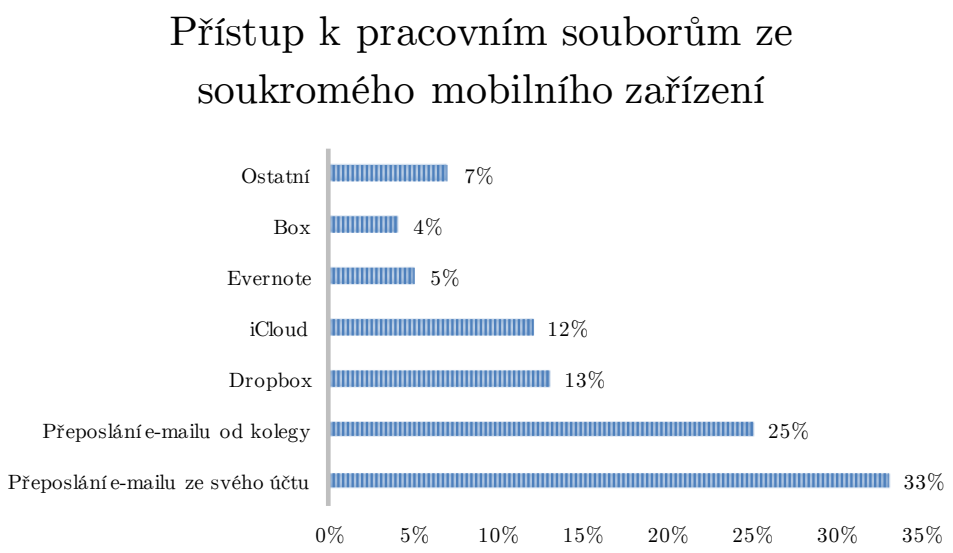
Zaměstnanci vytvářejí stínové IT nejčastěji tam, kde je velký nesoulad mezi požadavky byznysu a poskytovanými službami IT oddělení. Uživatelé se tak snaží zacelit mezeru, která tímto nesouladem vzniká. [10, 2]. Závažnost takového nesouladu může být různá, v případě nedostatečné podpory celého oddělení byznysu je typickým výsledkem používání cloudových aplikací bez vědomí IT oddělení.

3.1.3 Zavádění nových politik

Se zaváděním politiky Bring Your Own Device a Bring Your Own Application se stává mnohem složitějším pro řízení podnikové informatiky udržet kontrolu nad firemními daty, jejich integritou a bezpečností. [1, s. 6-8] Uživatelé používají na svých zařízeních soukromé účty a aplikace (úložiště, komunikátory), přes které vyvádějí data mimo podnik.

3.1.4 Nekonzistentní postoje v řízení podniku, soupeření

V podnicích je často značná část výdajů (10 – 35 %) [5, s. 20] na informační technologie vynakládána zcela mimo rozpočet IT oddělení. Nejčastěji marke-



Obrázek 3.2: Nejčastější způsoby přístupu k pracovním souborům ze soukromého mobilního zařízení. [20]

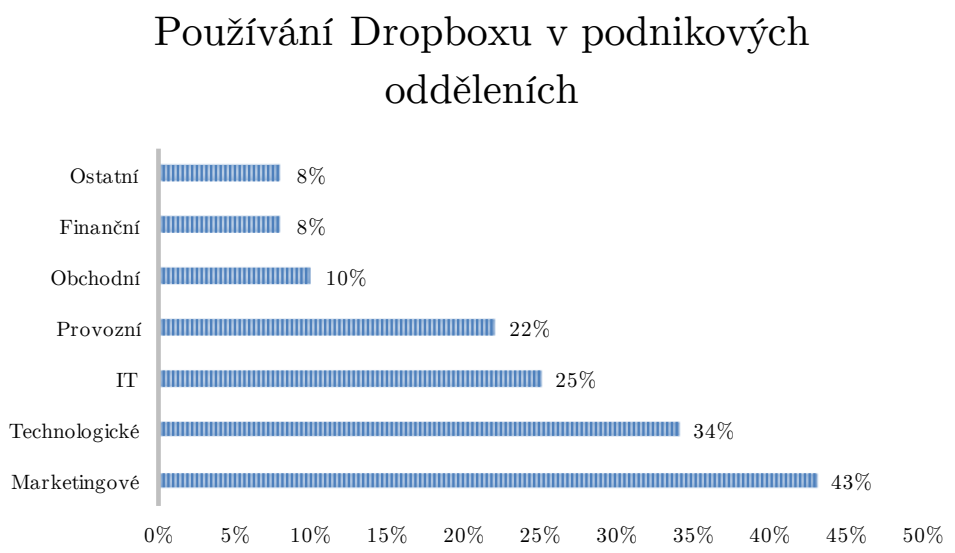
tingové oddělení (ale i jiná oddělení podniku) takto využívá skutečnosti, že na vytváření, úpravách a nasazení aplikací pod licencí Software as a Service se IT oddělení nemusí vůbec podílet. [5, s. 21] Toto vědomé obcházení vedení informatiky ostatními odděleními a soupeření o pravomoci často vede k nákupům cloudových aplikací pod licencí SaaS.

3.2 Změny v oblasti informačních technologií

Mezi další důležité příčiny patří změny v oblasti informačních technologií, které byly vyvolány vývojem na trhu. Jedná se o faktory, které přispěly ke konzumerizaci informatiky – zvláště pak o zvyšující se úroveň dostupných aplikací a nové modely licencování softwaru. Tyto důvody do firemní informatiky přinášejí aplikace a zařízení určené pro koncové uživatele.

3.2.1 Zvyšující se úroveň aplikací a zařízení pro koncové uživatele

Hranice mezi firemními pracovními nástroji a těmi, které jsou určené pro koncové uživatele, se stává méně zřetelnou a na trh se dostávají nové, propracovanější a funkcemi lépe vybavené nástroje a zařízení. [1, s. 6] Například sociální sítě umožňují efektivnější komunikaci mezi zaměstnanci i v obchodních záležitostech a makra v Excelu mohou značně zvýšit produktivitu zaměstnanců. [2,



Obrázek 3.3: Rozsah používání Dropboxu v jednotlivých odděleních podniku. [20]

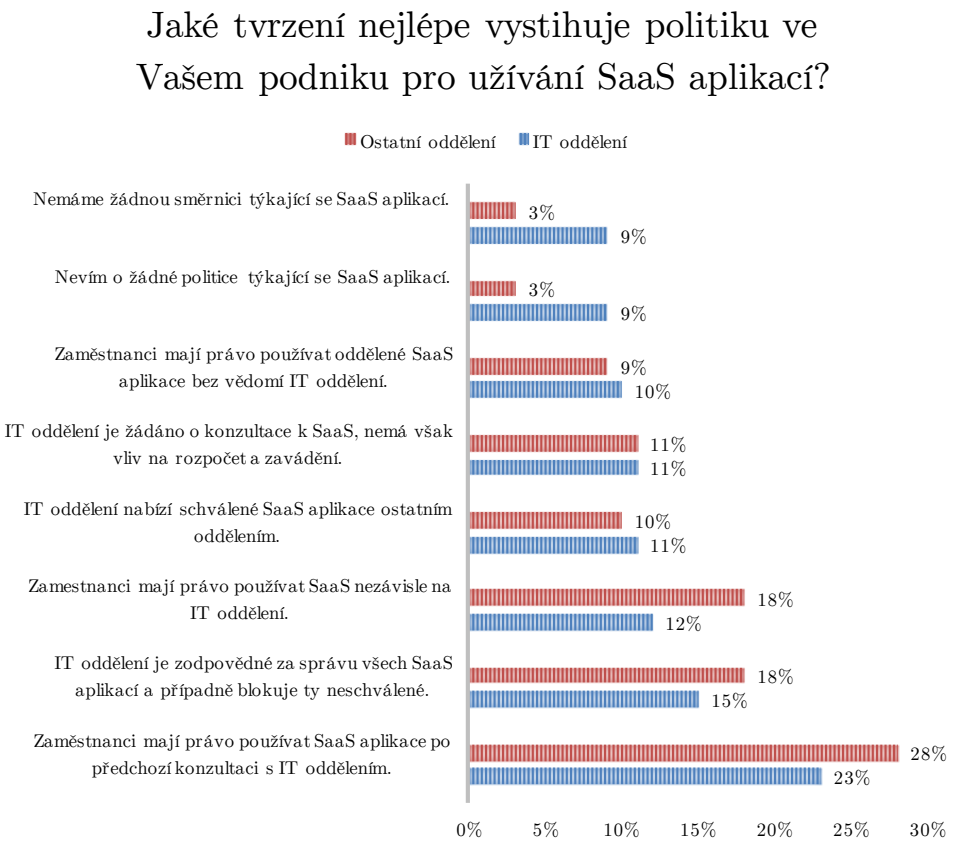
s. 275] Uživatelé se navíc s rostoucí konzumerizací IT stávají více počítačově gramotní a jejich nároky na služby IT oddělení jsou vyšší. [2, s. 278]

3.2.2 Jednoduchost a nové modely licencování software

Důležitou motivací pro uživatele je pohodlnost, jednoduchost a snadnost práce s novými nástroji, poskytovanými zejména modelem Software as a Service. Navíc uživatelé tíhnou k používání více zařízení najednou, včetně svých soukromých, a nebo k využívání soukromých účtů pro firemní účely (např. pro sdílená uložiště). [1, s. 6-7]

3.3 Pohnutky zaměstnanců

Do této skupiny řadíme takové pohnutky zaměstnanců, které nemají významný přesah do ostatních skupin. Zpravidla se nejedná o zlé úmysly ze strany zaměstnance vůči podniku [2, s. 281], většinou jde o neznalost nebo nepochopení vnitřních pravidel podniku. Výslednou formu stínového IT, které takto vzniká, představuje především stahování malých programů a utilit, používání soukromých aplikací ve firemním prostředí nebo narušení bezpečnosti dat (přeposílání na soukromé emaily, nahrávání na soukromá či veřejná úložiště).



Obrázek 3.4: Výsledky studie společnosti Frost & Sullivan dokládající nejasnosti ohledně nastavení podnikových politik týkajících se SaaS aplikací. [15]

3.3.1 Neznalost vnitřních politik a neporozumění

Část zaměstnanců nezná všechny vnitřní politiky podniku nebo nerozumí jejich podstatě. Tito lidé často nemají ponětí, že porušují vnitřní předpisy a vykládají si je vlastním způsobem. To dokládají i výsledky studie společnosti Frost & Sullivan [15], které jsou na obrázku 3.4. Je z nich patrná neznalost směrnic z pohledu zaměstnanců IT oddělení i ostatních zaměstnanců podniku a rozdíl v ponětí o existenci takových politik mezi těmito dvěma skupinami. Typickým představitelem je názor, že instalací open source softwaru při dodržení jeho licence nemůže dojít k porušení vnitřních politik podniku [2, s. 279].

3.3.2 Ospravedlňování jednání

Někteří zaměstnanci si jsou vědomi vnitřních politik podniku i rizik, která jejich porušení mohou způsobit. I tak se však dopouštějí jejich porušování a

jako hlavní důvod uvádějí (podle jejich názoru pádné) argumenty, které jejich jednání ospravedlňují. [21] Jedná se zejména o programy nebo jiné nástroje, se kterými mohou pracovat efektivněji než se schválenými firemními.

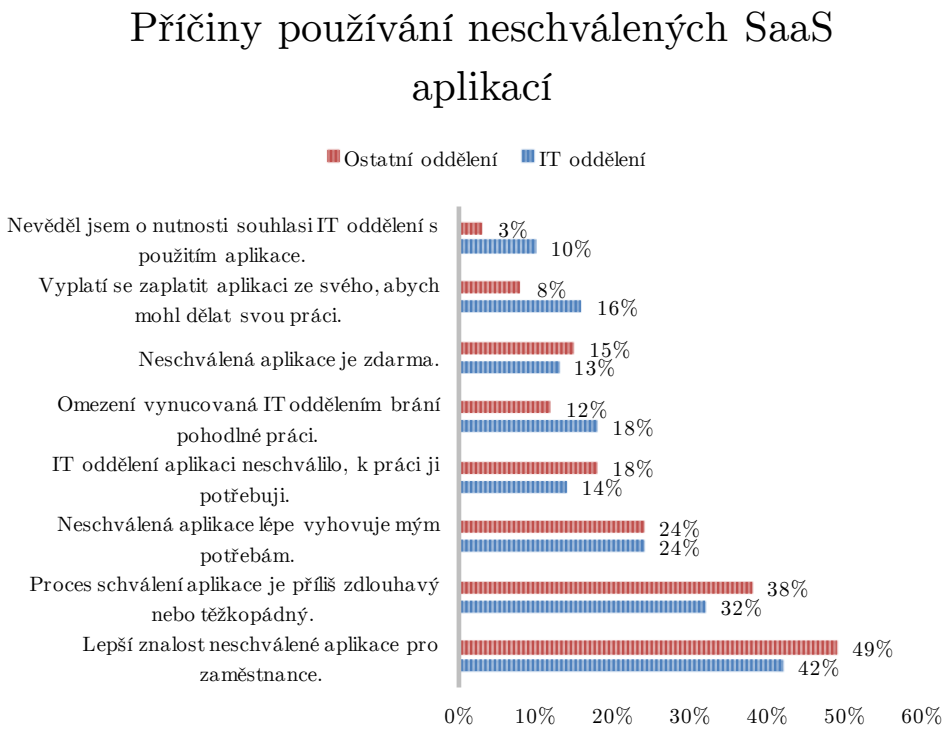
3.3.3 Sebejistota

Část zaměstnanců podniku tato pravidla vědomě porušuje i když vědí, že nebudou moci své jednání relevantně obhájit a mohou za něj být případně potrestáni. Tato skupina zaměstnanců tak jedná z přesvědčení, že takovéto přečiny jsou a budou v podniku tolerovány. [2, s. 279] Častou pohnutkou je představa, že zaměstnanec dokáže řešení podnikové informatiky spravovat lépe než IT oddělení (např. používání aplikace CCleaner). Nejčastěji jsou takovými prohřešky hardwarová zařízení jako WiFi-AP, neschválené úpravy nastavení, peer-to-peer aplikace nebo nelegální software.

3.4 Shrnutí příčin vzniku stínového IT

Příčin vzniku stínového IT je hned několik a často jsou vzájemně provázané, lze však u nich nalézt společný průsečík. Obecně se dají všechny propojit v tom smyslu, že zaměstnanci se snaží co nejlépe a nejpohodlněji dělat svou práci. To potvrzuje i studie [15] provedená společností Frost & Sullivan, jejíž hlavní uváděné příčiny vzniku stínového IT (na obrázku 3.5) spojuje motivace získat správný nástroj nebo aplikaci a to co nejrychleji.

Vznik neschválených aplikací a řešení v podnikovém prostředí je podmíněn nesprávným řízením ze strany vedení podnikové informatiky a celého podniku. Přispívá k nim také vývoj na trhu informačních technologií, hlavní zodpovědnost však musíme přiřadit k nedostatečné reakci řízení na tyto změny. V této kapitole byly shrnuty příčiny z různých zdrojů v literatuře a studiích věnujících se této problematice. V tabulce 3.1 je přehledně shrnuto uspořádání důvodů vzniku stínového IT, které propojuje oblasti řízení podnikové informatiky (IT Governance), souladu podnikové informatiky s byznysem (Business IT Alignment) [11], konzumerizace informačních technologií [2, 1] a firemní kulturu [2, 21].



Obrázek 3.5: Příčiny používání neschválených SaaS aplikací zaměstnanci podniku. [15]

	Příčina	Nejčastější formy stínového IT
4.1	Příčiny plynoucí z řízení podniku a podnikové informatiky	
4.1.1	Nedostatečná elasticita podniku	SaaS aplikace (úložiště)
4.1.2	Nedostatečná podpora byznysu od IT oddělení	Instalace programů a úpravy nastavení, nákup SaaS aplikací
4.1.3	Zavádění nových politik	Soukromá zařízení, účty a aplikace (úložiště, komunikátory)
4.1.4	Nekonzistentní postoje v řízení podniku, soupeření	SaaS aplikace
4.2	Změny v oblasti informačních technologií	
4.2.1	Zvyšující se úroveň aplikací a zařízení pro koncové uživatele	Soc. sítě, makra v souborech z MS Office
4.2.2	Jednoduchost a nové modely licencování software	Soukromá zařízení, účty a aplikace (úložiště, komunikátory)
4.3	Pohnutky zaměstnanců	
4.3.1	Neznalost vnitřních politik a neporozumění	Open source software, instalace programů, používání soukromých účtů a úložišť
4.3.2	Ospravedlňování jednání	Instalace programů
4.3.3	Sebejistota	Vlastní HW (WiFi-AP), P2P aplikace, nelegální software

Tabulka 3.1: Souhrn příčin stínového IT a nejčastějších forem jeho projevů

Kapitola 4

Rizika a dopady stínového IT na podnik

Ačkoliv je stínové IT často vnímáno jako něco nežádoucího pro podnik, může přinášet i žádoucí efekty. V této kapitole jsou dopady členěny na negativní a pozitivní. Do první skupiny často patří nežádoucí efekty, které jsou spojené s neexistencí řízení stínového IT a návazností na existující principy fungování podniku. Druhou skupinu naopak tvoří benefity pramenící ze snahy zaměstnanců dělat svou práci pohodlněji a přizpůsobovat se požadavkům trhu rychleji.

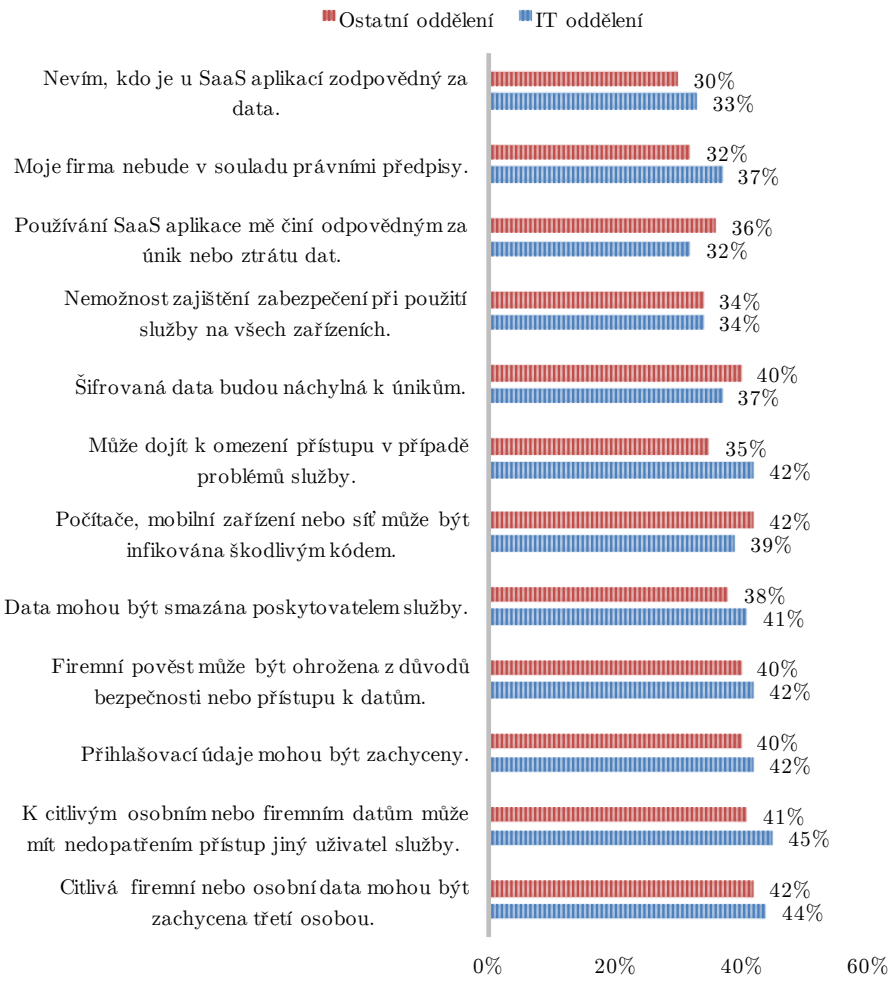
4.1 Negativní dopady

Negativní dopady na podniky často souvisí s informační bezpečností a neexistencí propojení se stávajícím fungováním podniku. Na obrázku 4.1 podle studie společnosti Frost & Sullivan [15, s. 9], zaměřené na neschválené SaaS aplikace ve firmách, si většinu rizik uvědomují i samotní zaměstnanci podniku (označují je sami jako velmi závažná).

4.1.1 Bezpečnost přístupu k firemním datům

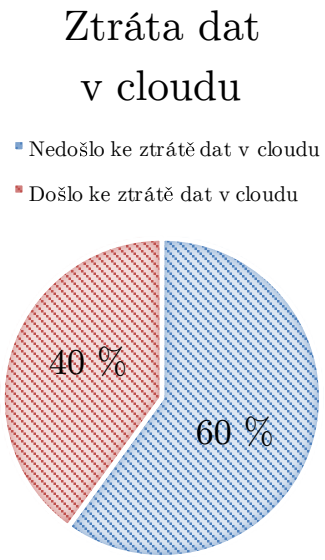
Zvláště u cloudových a SaaS aplikací je hlavním problémem zabezpečení přístupu k datům. Zaměstnanci často zveřejňují citlivé firemní informace na sociálních sítích, posílají je v nezašifrované podobě e-mailem nebo přenášejí na USB flash discích a zařízeních, nebo k nim přistupují přes veřejná připojení např. v kavárnách apod. [22].

Další rizikem je nedosažitelnost dat v cloudu a jejich případná ztráta. Na obrázcích 4.2 a 4.3 je znázorněn podíl společností, které podle studie společnosti Symantec [19, s. 6] řešily ztrátu dat v cloudu, případně měly problémy s obnovováním z vlastní zálohy. Mezi tyto problémy může patřit například

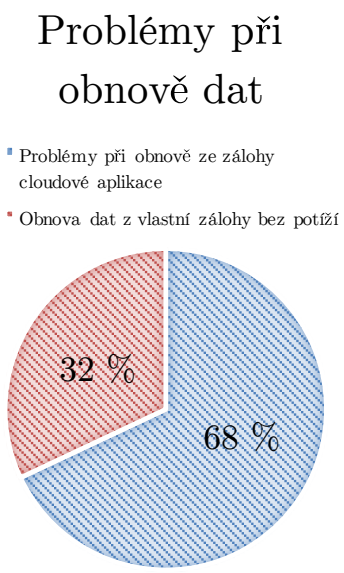


Obrázek 4.1: Rizika identifikovaná zaměstnanci ztažená k používání neschválených SaaS aplikací. [15, s. 9]

komplikovanost procesu vyžadující dodatečné školení pracovníků IT oddělení nebo přílišná časová náročnost.



Obrázek 4.2: Podíl firem, které podle studie [19, s. 6] zaznamenaly ztrátu dat v cloudu v roce 2013.



Obrázek 4.3: Podíl firem, které podle studie [19, s. 6] měly problémy s obnovou dat v cloudu v roce 2013.

4.1.2 Bezpečnost informační infrastruktury

Existence stínového IT může vytvářet podmínky pro narušení bezpečnosti celé podnikové infrastruktury. Může docházet k vytváření zranitelností, díky kterým je útočník schopen proniknout do podnikové sítě – například zapojení a sdílení internetového připojení pomocí vlastního WiFi routeru s nedostatečným zabezpečením [8, 12].

Další hrozbou je zanášení škodlivého SW do podnikového ekosystému. K tomuto může dojít například zapojením soukromého zařízení do podnikové sítě nebo instalací neschváleného programu pochybného původu (nelegální software, instalátory stažené z neautorizovaných zdrojů na internetu apod.) na firemní zařízení. [2, s. 278, 281] Dále může dojít i k úniku přihlašovacích údajů a hesel používaných pro schválené podnikové aplikace a systémy.

4.1.3 Narušení fungování podniku

Další hrozbou pro podnik je využívání stínového IT pro realizaci klíčových procesů. Při vytváření neschváleného prostředí nebývají dostatečně řízena rizika

a zapomíná se na tvorbu krizových scénářů a analýzu souvislostí s ostatními systémy. Důsledkem pak je neschopnost reagovat na výpadek systému nebo neexistence podpory, dokumentace a definice návazností na ostatní informační systémy a procesy. Neschválené systémy pak mohou vnášet chaos do existujícího prostředí (nejsou pod kontrolou datové toky, časové návaznosti a může docházet z zahlcení sítě).

4.1.4 Narušení architektury informačních systémů a dat

Nejsou pod kontrolou datové toky a dochází k duplikaci dat do systémů mimo kontrolu IT oddělení. Úpravou dat na různých místech a jejich nekoordinovaným používáním dochází k nekonzistencím.

4.1.5 Finanční dopady plynoucí z rizik

Incidenty způsobené stínovým IT mohou mít i závažný finanční dopad na podnik. Podle studie společnosti institutu Ponemon [23] je průměrná finanční ztráta způsobená únikem dat až 310 dolarů na uniklý záznam (pro různá odvětví se tato částka liší – viz obrázek 4.4). Podle studie společnosti Safetica Technologies [24, s. 7] může navíc dojít i ke ztrátě zákazníků, důvěryhodnosti společnosti a k poškození dobrého jména.

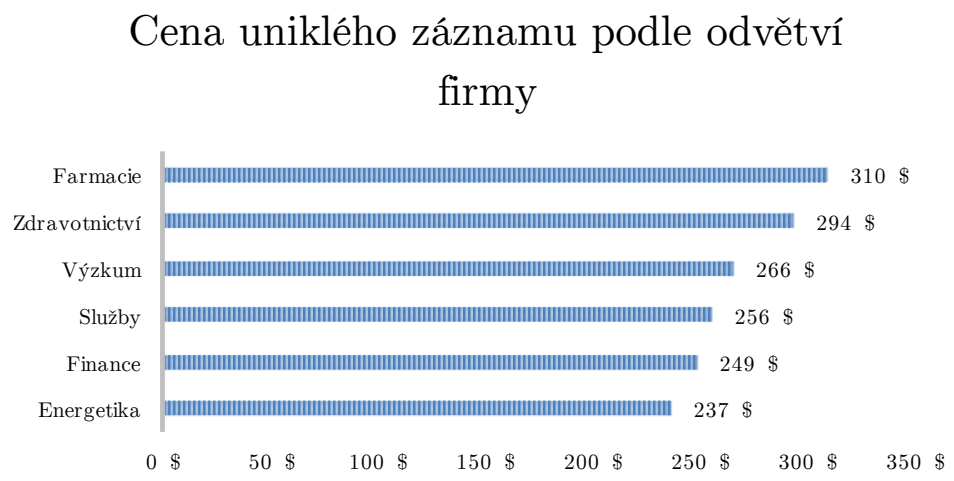
Podnik může citelně zasáhnout i narušení klíčových procesů. Pokud je neschválený systém používán ke klíčové činnosti firmy a dojde k jeho výpadku, může to znamenat zastavení celého podniku – například díky neexistenci SLA a scénářů při nedostupnosti služby nebo ztrátě a zdlouhavé obnově dat v cloudu [19, s. 6]. Zavlečením škodlivého SW nebo vytvořením zranitelností pak může být narušen provoz schválených kritických informačních systémů podniku.

4.2 Pozitivní dopady

Žádoucí dopady stínového IT vycházejí především z faktu, že hlavním motivátorem pro vytváření neschválené informační infrastruktury je snaha zaměstnanců dělat svou práci lépe a pohodlněji. Kromě zvýšené produktivity zaměstnanců sem spadá i schopnost podniku zavádět nová a konkurenceschopná zařízení a aplikace rychleji a lépe reagovat na změny na trhu.

4.2.1 Zvýšená produktivita zaměstnanců

Stínové IT může znamenat pro podnik přínos v podobě zvýšené produktivity zaměstnanců. Například společnost Intel zavedením politiky BYOD zvýšila produktivitu zaměstnanců o necelou 1 hodinu denně. [1, s. 8] Avšak studie společností iPass and MobileIron ukazuje, že zavedení politiky BYOD naopak může zahltit IT oddělení a zhoršit jeho produktivitu. [1, s. 8] Další studie



Obrázek 4.4: Cena uniklého záznamu podle odvětví firmy. [23]

ukazují, že například sociální sítě umožňují rychlejší komunikaci mezi zaměstnanci a vlastnoručně psaná makra v souborech programů Microsoft Excel a Microsoft Access představují důležité nástroje pro rychlejší tvorbu výstupů zaměstnanců. [2, s. 275]

4.2.2 Zvýšená elasticita podniku

Stínové IT umožňuje podniku rychleji reagovat na změny a zavádět nejnovější technologie a postupy rychleji. To je způsobeno rychlým vývojem na poli informačních technologií a konzumerizací trhu. Zaměstnanci často mají svá soukromá zařízení novější, výkonnější nebo s lepšími parametry než firemní zařízení, jsou zvyklí používat novější verze programů nebo zcela nové aplikace a přirozeně se stávají inovátory. Obcházením formálních schvalovacích procesů změny pak zavádějí rychleji.

4.2.3 Finanční úspory

Obcházení stínového IT může podniku též přinášet finanční úspory. Uživatelé často vyhledávají snadno dostupný software, především pak open-source software, který je volně ke stažení a často pod velmi permisivní licencí. [2, s. 278] Tento pozitivní dopad však často vyvažuje jiný negativní; pokud se jedná o aplikaci nebo řešení, které by IT oddělení formálně neschválilo, často to může být z důvodů licenčních (například licence zdarma pouze pro nekomerční použití) nebo bezpečnostních (bezpečnost uložení a přenosu dat, soulad s legislativou, absence podpory a další).

4.3 Shrnutí dopadů stínového IT na podnik

Stínové IT má na podniky dopady pozitivní i negativní. Z pohledu fungování podniku je problémem především informační bezpečnost a absence řízení rizik nekontrolované části podnikové informatiky (například výpadek klíčového systému pro primární procesy podniku). Pozitivním přínosem je pak elasticita podniku a schopnost reagovat na změny na trhu a rychle se přizpůsobit nové situaci. Přímý finanční dopad může stínové IT přinášet ve formě úspor z provozu, negativní formou jsou pak především ztráty a pokuty plynoucí z bezpečnostních incidentů a omezení činnosti podniku. Podle průzkumu z roku 2002 [11] je největší hrozbou spojenou se stínovým IT zaměstnanec podniku a jeho nedostatečné porozumění podnikové informatice a bezpečnostním politikám. Dopady stínového IT na podnik je tedy vhodné vždy posuzovat ve vztahu ke znalostem, úrovni školení a počítačové gramotnosti zaměstnanců.

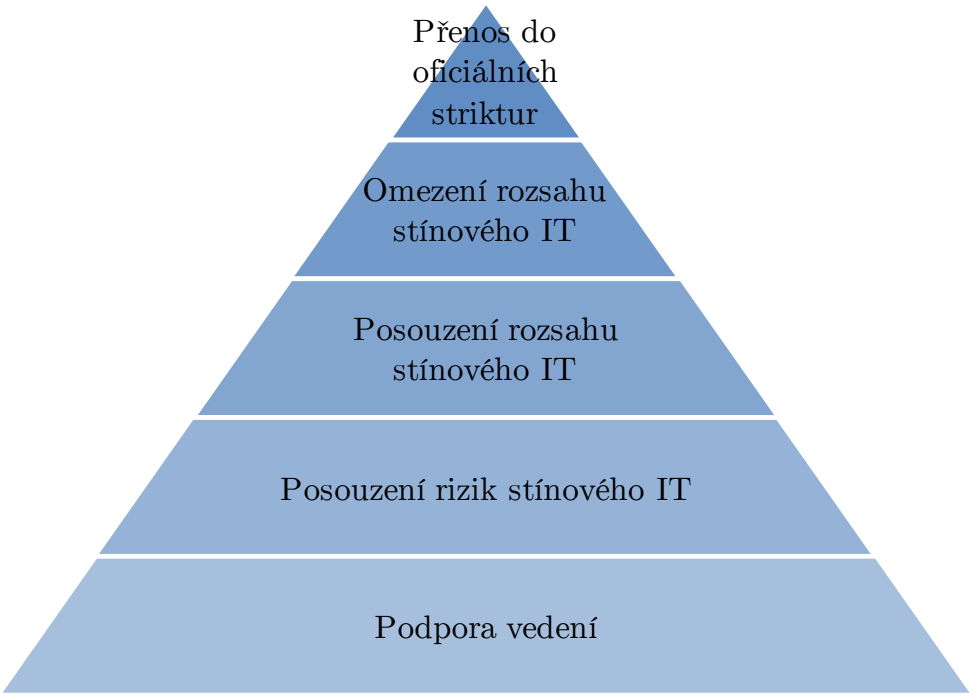
Kapitola 5

Způsoby řízení stínového IT

V této kapitole jsou uvedeny stručné principy pro řízení stínového IT tak, jak je zmiňuje odborná literatura. Doporučení pro řízení podnikové informatiky zpravidla vychází z výsledků studií postavených na kvalitativních metodách a jeho principy jsou ilustrovány na obrázku 5.1. Zejména jsou použity různé metody ať už pro nalezení korelace mezi výsledky z jiných metod, nebo pro zprůměrování jejich výsledků (triangulace). Nejčastější metodou jsou interview přímo s ředitelem IT oddělení (CIO), případně se zaměstnanci. Méně časté jsou pak kvalitativní analýzy dokumentace různých informačních systémů nebo seznamy nainstalovaných programů pro kontrolu koncových stanic uvnitř podniku.

Ze studií zabývajících se propojením podnikové informatiky a byznysu vyplývá, že hlavní motivátory pro vznik stínového IT jsou do jisté míry určovány podnikovými procesy a kulturou. Mezi hlavní příčiny vzniku stínového IT patří neschopnost podniku uspokojovat potřeby byznysu – na toto tvrzení je třeba nahlížet zejména optikou uživatele, který nemá dostatečnou podporu pro vytváření hodnoty uvnitř podniku. Velkou bezpečnostní hrozbou je dále nedostatečná gramotnost uživatelů informačních technologií – studie ukazují, že rizika plynoucí z nedostatečné znalosti informačních technologií a pracovních procesů na ně navázaných mohou být u zaměstnanců úspěšně minimalizována školením a jejich edukací. Dalším problémem je nedostatečné propojení zaměstnanců s IT oddělením nebo nedostatečná korelace nabízených služeb IT oddělením a potřebami zaměstnanců. [11]

Několik zdrojů [9, 25, 5] týkajících se řízení podnikové informatiky doporučuje proaktivní přístup. Například Julia Kingová [5, s. 21] upozorňuje na nevyhnutelnost existence neschválených informačních řešení v podniku, která je navíc poháněna vývojem informačních technologií. IT oddělení podniku by se mělo samo snažit předcházet situacím, kdy není schopno nabídnout potřebnou službu, a snažit se odhadnout a připravit se na budoucí poptávku zaměstnanců nebo celých oddělení (stát se iniciátorem změny a nečekat na impulz od zaměstnanců).



Obrázek 5.1: Principy řízení stínového IT v podniku.

IT oddělení by zároveň mělo proaktivní přístup aplikovat ve formě spolupráce s pracovníky mimo své oddělení [5]. Vhodné je například vyhledávat spojence, kteří jsou dostatečně gramotní a zároveň sdílejí vizi hledání nových nástrojů a řešení pro podporu pracovní činnosti. IT oddělení za pomoci těchto lidí (nebo i samo) by mělo plnit roli edukátora a tvůrce návrhů, pomocí kterých dokáže zaměstnancům vstřebatelnější cestou předat potřebné znalosti a nástroje a předejít tak tvorbě stínového IT.

Řízení stínového IT je nesnadným problémem, protože už z definice je těžké ho v podniku vyhledat a kontrolovat. Tradiční imperativní a zákazové metody selhávají, nebo jsou dokonce kontraproduktivní. Řízení informatiky by si mělo uvědomit následující: [16, s. 2-3]

- Stínovému IT se nedá zcela zabránit.
- Není možné zakázat veškeré technologie mimo organizaci.
- Snaha o řízení pouze posouvá problém mimo dohled („více do stínu“).
- Drakonické snahy zamezit stínovému IT podkopávají reputaci organizace, mohou poškodit agilitu a kreativitu společnosti a snížit motivaci zaměstnanců.
- Moderní podniky využívají různé technologické zdroje a schopnosti.

- Obecná produktivita zaměstnanců závisí na nástrojích poskytovaných IT oddělením a zaměstnanci chtějí mít přímou kontrolu nad zařízeními, která používají.

5.1 Motivace a posouzení rizik

Vedení informatiky by v první řadě mělo posoudit rizika plynoucí ze stínového IT vzhledem ke stavu podnikové informatiky. Problémem často bývá chybějící motivace ze strany vedení informatiky nebo celého podniku se vůbec tomuto problému věnovat. Z předcházející kapitoly známe potenciální rizika a dopady stínového IT na podnik, kromě nich však ke komunikaci o tomto problému uvnitř firmy lze podle [16, s. 2] využít tato témata:

- Podstata byznys modelu a jeho závislost na efektivní, propojené a zabezpečené podnikové informatice.
- Zranitelnost klíčových systémů vůči vedlejším vlivům a škodám působených provozem neschválených aplikací a řešení.
- Možnost vnějších škod nebo ztráty pověsti vlivem špatné funkcionality stínového IT (poškození dobrého jména, krádež a ztráta firemních nebo osobních dat).

Posouzení přesné úrovně rizik může být nepřesné bez znalosti rozsahu stínového IT v podniku. Na druhou stranu lze zkonstruovat rámec na základě propojení podnikové informatiky s byznysem a získat podporu ze strany vedení firmy.

5.2 Posouzení rozsahu stínového IT

Protože stínové IT je z podstaty skrytý problém a při snaze o jeho monitorování má tendenci se ještě více skrývat, jsou nepřímé metody účinnější pro posouzení jeho rozsahu. Přímé dotazování nebo získávání informací od uživatelů nebo tvůrců stínového IT je často ztíženo lhaním nebo zatajováním informací a způsobuje snahu o ještě větší utajení neschváleného nástroje.

Jako vhodné zdroje pro posouzení rozsahu stínového IT se jeví především následující [16, 2, 1]:

- Dokumenty a informace z oddělení nákupu a financí (firemní účetnictví).
- Posouzení ze strany vedoucích jednotlivých oddělení (zde záleží především na důvěře mezi CIO a těmito vedoucími; vedoucí nesmí mít snahy kontrolovat stínové IT sami nebo ho udržovat).

- Poohlížení se po nástrojích používaných zaměstnanci při běžné agendě (např. při poradách vedení a schůzkách na cizích odděleních).
- Požadavky (i zamítnuté) o podporu a integraci na IT oddělení organizace.
- Požadavky na IT oddělení o formální i neformální posouzení různých záležitostí týkajících se podnikové informatiky (zkušenosti s konkrétními nástroji apod.).
- Analýza instalovaného software na koncových zařízeních pomocí specializovaných nástrojů.
- Analýza síťového provozu pomocí specializovaných nástrojů.

5.3 Omezení rozsahu stínového IT v podniku

Stínové IT z podniku není možné zcela vymýtit, nicméně je možné jeho rozsah omezit a vytěsnit jeho nebezpečné podoby (snížit rizika s ním spojená). Je rovněž důležité přehodnotit přístup IT oddělení dovnitř firmy od „ovládání a kontroly informatiky“ k přístupu „kooperativního IT“. [5] IT oddělení v současných podnicích už nemá funkci dodavatele, často ani správce software. Jeho činnost se soustředí především na přehled, která data jaké aplikace používají, které z nich jsou kritické a kdo se stará o jejich chod. [5]

Krátkodobým řešením problémů způsobených stínovým IT je reakce ve formě restrikcí. Cílem je zamezení vzniku stínového IT, avšak je nutné zaměřit se na příčinu jeho vytváření – protože pokud ta přetrvá, zaměstnanci se budou snažit postupně obejít i nově zavedená opatření. Například odebráním administrátorských práv může dojít krátkodobě ke zmenšení rizika používání vlastního software na pracovních stanicích. Uživatelé však začnou časem hledat způsoby, jak nová omezení obejít (např. využíváním portable aplikací). Je tedy důležitá edukace uživatelů a nabídnutí podpory pro jejich potřeby (u zaměstnanců nesmí dominovat pocit, že je lepší vyřešit problém vlastními silami a nepoptávat podporu u IT oddělení).

Pokud firma dlouhodobě přistupuje pouze k restrikcím a nenabízí vstřícný přístup k zaměstnancům a jejich potřebám, dochází ke změně formy stínového IT. Zaměstnanci například místo instalovaného software využívají portable aplikace nebo upravují nastavení firemního software, aby uspokojili potřebu, která je k tvorbě stínového IT vede. Vedení podniku vkládá úsilí do omezení stínového IT, stejnými kroky však pohání motivaci zaměstnanců k jeho vytváření (např. chybějící firemní služba na sdílení souborů je suplována veřejným cloudovým úložištěm – pokud je například pomocí firewallu zakázán přístup z podnikové sítě, nezmizí potřeba uživatelů sdílené úložiště používat a začnou hledat jiné nástroje pro dosažení svých cílů).

Pokud je rozsah stínového IT omezen intervencí ze strany vedení podniku nebo informatiky a nejsou řešeny příčiny jeho vzniku, v krátkodobém horizontu dojde skutečně k omezení rozsahu stínového IT uvnitř firmy. Postupně však zaměstnanci zkouší pravidla porušovat a obcházet a po čase se stínové IT vrátí na původní úroveň. Proto je vhodné s tímto fenoménem pracovat ve dvou rovinách: operativně řešit akutní problémy (zavádět restrikce) a držet se naplánované strategie práce se stínovým IT (odstraňovat motivátory pro jeho vznik, edukovat zaměstnance a snažit se o přenos z neoficiálních do oficiálních struktur).

5.4 Přenos stínového IT do oficiálních struktur

Podniky by se v boji se stínovým IT měly snažit mu předcházet a snažit se ho začlenit po bok oficiálního IT ve firmě. Tento přístup se dá postihnout analogií s vrženým stínem: Pokud například posvítíme na nějaký předmět, jeho přivrácená strana i okolí bude sice jasnější, avšak vržený stín ostřejší a kontrast mezi osvětlenou a neosvětlenou částí větší. Stejně tak restriktivním přístupem stínové IT více posilujeme (sice krátkodobě můžeme omezit rozsah, ale zhoršíme tím schopnost vedení IT stínové IT detekovat). Cílem by tedy mělo být vytvoření prostředí s difuzním osvětlením – žádné přímé osvětlení a tedy žádné ostré stíny. [1, s. 10]

Základním kamenem přenosu stínového IT do oficiálních struktur je jeho začlenění. Ukotvení jeho pozice například ve směrnicích může být problematické z důvodu legislativních (například firmy podléhající určitým standardům a certifikacím musí mít informační architekturu podniku přesně evidovanou). Pokud to však je možné, je dobré udělat vstřícný krok vůči zaměstnancům a povolit jim určitou volnost týkající se nekritických aplikací. Je důležité je poučit o rizicích a dopadech [2, s. 281], není však vhodné monitorovat využívání těchto aplikací (požadovat reporty o používání aplikací). Příkladem mohou být soukromé e-mailové služby: Pokud má výpadek firemní poštovní server, zaměstnanci mohou použít soukromý e-mail. Citlivá data by měla být zašifrována (např. ZIP chráněný heslem), zároveň by zaměstnanec měl pamatovat, že se nemůže spolehnout na firemní zálohování (v případě výpadku nebo havárie nemusí poskytovatel soukromé e-mailové schránky garantovat žádné záruky).

Další krok, který může podnik pro začlenění stínového IT udělat, je vyhledávání problémů. IT oddělení by mělo mít uvnitř podniku zájem na zlepšování svých služeb dodávaných konkrétním zaměstnancům a oddělením [26, s. 20]. Jeho přístup by měl být přátelský a otevřený – zaměstnanec je jeho zákazníkem a IT oddělní by mělo usilovat o jeho spokojenost. Toho lze dosáhnout vyhledáváním problémů – pokud se bude zaměstnanec i IT oddělení soustředit na společný cíl odstranit problém, je vybudována vzájemná důvěra. Zaměstnanec pak sám spíše přizná (nebo navrhne) použití aplikace řešící daný problém, kterou zná soukromě. Stejně tak IT oddělní může „přimhouřit oči“, navrhnout

neformální řešení a dát (neformální) souhlas s jeho používáním.

IT oddělení zároveň musí kvalitně reagovat na oficiální požadavky ostatních oddělení a zaměstnanců. Pokud IT oddělení dostatečně rychle a pružně nereaguje na potřeby byznysu, dochází ke snahám ho obejít a poradit si bez jeho pomoci. Je tedy důležité, aby všechny požadavky byly včas a vstřícně řešeny a zaměstnanci podniku věděli, že se mohou vždy na IT oddělení obrátit a že to jim pomůže s řešením jejich problému lépe, než pokud by se o to snažili sami. Zde je důležité poznamenat, že IT oddělení zároveň musí mít podporu vedení podniku a musí mít pro tuto činnost dostatečné prostředky. Například zavedením politiky BYOD může dojít k rapidnímu zvýšení nároků na podporu IT oddělení a přetížením jeho pracovníků může dojít ke zhoršení kvality většiny jeho služeb. Výsledkem je pak vznik stínového IT primárně ne z důvodu přítomnosti soukromých zařízení, ale z důvodu nedostatečného uspokojování zaměstnaneckých požadavků IT oddělením. [1, s. 8]

IT oddělení by se také mělo snažit stát se iniciátorem změny. Trh a požadavky byznysu se neustále mění a IT oddělení je kromě dodávky nasmlouvaných služeb nuceno na tyto změny reagovat. Na rozdíl od všech ostatních oddělení uvnitř podniku IT oddělení disponuje nejlepšími znalostmi týkajícími se jednak dostupných aplikací a řešení na trhu (avšak zde mohou být užitečné a kvalitnější zkušenosti zaměstnanců daných oddělení s aplikacemi určenými přímo pro jejich činnost), zejména však informacemi důležitými pro úspěšné začlenění do stávající informační architektury podniku. Je tedy vhodné, aby samo IT oddělení přicházelo s návrhy na změny a dokázalo tak určovat směr vývoje podnikové informatiky na základě dobrého souznění s požadavky byznysu. [5, s. 21-22]

Poslední a neméně důležitou částí je edukace zaměstnanců. Kromě vysvětlování technické stránky věci (bezpečnostní rizika, možné dopady) je vhodné ze strany vedení firmy i IT oddělení vyjasnit zaměstnancům svou pozici a částečně tak „odkrýt karty“. Pokud boj se stínovým IT není veden v rovině jeho vymýcení a ukončení pracovního vztahu se zaměstnanci, kteří ho vytváří, je vhodné tuto pozici zaměstnancům sdělit. Je vhodné zaměstnancům vysvětlit, proč může být stínové IT pro podnik nebezpečné a že předznamenává hlubší problém (špatná funkce IT oddělení uvnitř podniku), a primárně ten chce vedení podniku řešit. [11, s. 8]

5.5 Vztah stínového IT a rámce ITIL

Pro řízení podnikové informatiky je často používána knihovna rámce ITIL, tato část je věnována analýze jeho vztahu ke stínovému IT. Obecně lze říci, že pojem stínové IT jako takové rámec nezmiňuje, věnuje se však oblastem, které se stínovým IT souvisí. Rámec ITIL se v několika oblastech dotýká záležitostí, které mohou být se stínovým IT spojené, následující odstavce podrobněji vysvětlují toto propojení.

Kniha ITILu (v3) věnující se strategii služeb se mimo jiné zabývá správou financí IT služeb. Nastavení procesů schvalování výdajů na IT může omezit vznik stínového IT na úrovni oddělení, protože může existovat povinnost (byť jen jako formalita) schválení všech výdajů na informatiku pracovníkem IT oddělení. Další částí, která (byť jen volně) souvisí se stínovým IT, je analýza a vyhodnocení rizik – zde je nutné kvalifikovaně odhadnout možné finanční dopady rizik způsobených stínovým IT. [27]

Další kniha týkající se uvedení služeb do provozu řeší mimo jiné řízení znalostí. Stínové IT může představovat problém v dostupnosti nebo ztrátě znalostí (například ukládání pracovních dat pouze na soukromá zařízení nebo do soukromého cloudu). [27]

Kniha zaměřená na provoz služeb se pak věnuje reakci na problémy a řízení incidentů, bezpečnostnímu auditu a podpoře. Řízení incidentů, monitorování a podpora jsou pak hlavní procesy, kde se stínové IT projevuje nebo bývá detekováno. [27]

Poslední knihou, kde jsem nalezl významnější průsečík se stínovým IT, je ta, která se věnuje neustálému zlepšování. Tento proces je jedním z hlavních nástrojů k předcházení vzniku stínového IT a umožňuje lépe sladit potřeby byznysu s činností IT oddělení. Cílem podniku je neustále zlepšovat své procesy a předcházet tak tvorbě problémů, které může stínové IT přinášet. [27]

5.6 Shrnutí řízení stínového IT

Při řízení stínového IT je vhodné pochopit jeho principy a podle toho přijímat opatření a vytvářet strategii pro práci s ním. U některých podniků může být vhodné s ním proaktivně pracovat, u jiných to přípustné není a je třeba co nejvíce omezit jeho rozsah. Důležité je však k tomuto problému přistupovat s vědomím dlouhodobých dopadů a historického (i budoucího) vývoje. V boji proti stínovému IT se nedá vyhrát – tento fakt je třeba přijmout a s problémem buď aktivně pracovat nebo dlouhodobě pracovat na jeho omezování.

Kapitola 6

Průzkum stínového IT ve vybraných malých a středních podnicích v České republice

V této kapitole je popsán mnou provedený průzkum stínového IT v českých firmách. Popisuji zde způsob výběru a oslovení firem, získaná data a jejich význam, výsledky průzkumu a jejich diskuzi.

6.1 Cíle průzkumu

Cílem průzkumu je především ověření znalostí představených v předcházejících kapitolách (převážně pocházejících ze zahraniční literatury) v praxi českých firem. Vzhledem k náročnosti průzkumu, který by přesně mapoval stínové IT v dostatečně velkém vzorku českých podniků, byly zvoleny metody a vybrány firmy takovým způsobem, aby výstupem byla jakási úvodní studie představující stav této problematiky v České republice. Na ní se bude moci dále stavět v případě rozsáhlého průzkum na statisticky dostatečně velkém vzorku zkoumaných podniků. Při výběru firem tedy nešlo o kvantitu ale reprezentativnost.

Z těchto důvodů byly jako hlavní výzkumné metody zvoleny metody kvalitativní, především pak interview (v průběhu interview jsem se mohl doptávat na nejasnosti a korigovat tak výstupy). Interview bylo použito jako hlavní nebo jedna z hlavních výzkumných metod i v jiných výzkumech týkajících se stínového IT [2, 28, 10, 3]. Rozhodl jsem se zkombinovat tento přístup se zapojením kvantitativních dat a jejich porovnáním výsledků ve snaze o větší průkaznost (inspiroval jsem se ve výzkumu Sandy Behrens [10], kde autorka triangulovala výsledky 3 různých metod).

Kromě toho, že cílem není komplexní analýza firem v ČR, ale vhled a ověření tvrzení uvedených v literatuře, dalším problémem jsou aspekty patřící do společenskovědních disciplín, zejména sociologie a psychologie. Mimo to,

Počet zaměstnanců	200
Počet zaměstnanců IT oddělení	2
Počet zaměstnanců konzumujících služby IT oddělení	200
Sektor	soukromý
Odvětví	farmaceutický průmysl
Územní působnost	ČR, částečně EU
Přibližné stáří firmy	10 let

Tabulka 6.1: Charakteristiky firmy 1 z výzkumné části.

že kvalitativní i obecně další kvalitativní výzkumné metody s sebou nesou spoustu vedlejších efektů, které mohou ovlivnit výsledky pozorování, obecně i stínové IT je svou podstatou složitá problematika a respondenti mohou mít různé důvody pro lhaní nebo zatajování informací. V tomto výzkumu jsem se snažil tyto efekty minimalizovat a předvídat pohnutky respondentů tak, abych z nich dokázal vytěžit maximum informací.

6.2 Metodika výběru firem

Při výběru firem jsem se oslovil malé a střední podniky (SMB). Pro účely této práce považuji za malé podniky firmy s alespoň 10 zaměstnanci (menší považuji za mikro-podniky) a méně než 250 zaměstnanci, středními podniky pak rozumím firmy od 250 zaměstnanců po 1000 zaměstnanců (firmy nad 1000 zaměstnanců spadají mimo oblast zájmu této práce). Obecně platná hranice mezi kategoriemi není stanovena, já jsem stanovil intervaly pro SMB firmy takto především z důvodu existence formálního IT oddělení, které je pro můj výzkum zásadní (u menších firem formální IT oddělení často chybí). Zároveň pro mě byl důležitý i počet zaměstnanců, kterým IT oddělení své služby dodává (pokud vezmu v úvahu počet pouze těchto zaměstnanců, všechny tři firmy mohu zařadit mezi malé podniky).

Firmy jsem vybíral tak, aby byly dostatečně rozmanité. Podařilo se mi oslovit firmy z různých sektorů, působících v odlišných odvětvích a s různou historií. Podniky, které se mi podařilo pro účast v této práci zajistit, mají charakteristiky uvedené v tabulkách 6.1, 6.2 a 6.3.

6.3 Způsob oslovení firem

Prvotní oslovení firem jsem prováděl prostřednictvím e-mailu, případně jsem je dále upomínal telefonicky. Z původních sedmi oslovených firem se mi podařilo provést potřebná interview a získat data ze tří z nich (ostatní čtyři nereagovali a při upomínce přímo odmítly účast v této práci). Ve všech třech firmách jsem

Počet zaměstnanců	300
Počet zaměstnanců IT oddělení	1
Počet zaměstnanců konzumujících služby IT oddělení	90
Sektor	soukromý
Odvětví	výrobní firma
Územní působnost	ČR, částečně EU
Přibližné stáří firmy	20 let

Tabulka 6.2: Charakteristiky firmy 2 z výzkumné části.

Počet zaměstnanců	700
Počet zaměstnanců IT oddělení	4
Počet zaměstnanců konzumujících služby IT oddělení	200
Sektor	veřejný (příspěvková organizace)
Odvětví	správa a údržba silnic
Územní působnost	ČR
Přibližné stáří firmy	8 let

Tabulka 6.3: Charakteristiky firmy 3 z výzkumné části.

provedl potřebná interview osobně, další kvantitativní data jsem pak obdržel prostřednictvím e-mailu.

Všechny tři firmy požadovaly částečnou nebo naprostou anonymitu. Při jejich oslovování jsem anonymní formu přímo navrhoval, jejich reakce napovídala, že jedině na tento způsob spolupráce jsou ochotni přistoupit. Formu kvantitativní časti výzkumu jsem volil s ohledem na tuto skutečnost tak, aby nebylo nutné ve firmách nic instalovat (a nebylo nutné pro mě zajistit administrátorská práva na koncových stanicích), a v případě síťových dat jsem se nepodílel na jejich sběru, ale byla mi předána již bez citlivých údajů.

Přístup firem k podílení se na výzkumné části této práce byl z počátku lhostejný. Pozitivní přístup jsem pociťoval ze strany vedení informatiky umožněním výzkumu a podporou při hledání vhodných kandidátů. U zaměstnanců byla naopak cítit skepse týkající se smysluplnosti výzkumu (naopak projevy nedůvěry jsem u nich nezaznamenal). Přístup IT oddělení se v každé firmě lišil, od vstřícného až po lhostejný (viditelná snaha o minimalizaci času stráveného součinností).

6.4 Metody výzkumu

Jak už jsem zmiňoval v úvodu této kapitoly, pokusil jsem se zkombinovat metody kvalitativní i kvantitativní. V případě kvalitativních šlo o interview se třemi zaměstnanci mimo IT oddělení a pak jedním pracovníkem oddělení informatiky. U kvantitativních zdrojů dat jsem byl omezen omezen přístupem do firem (osobní a citlivá data, politiky řízení přístupu a uživatelských oprávnění) a informacemi, kterými firma disponovala (často nebylo hlavním problémem to, že by nějaká data nebyla ochotna firma poskytnout, ale že je nesbírala a vůbec je neměla).

6.5 Získaná data a jejich význam

Ze všech tří firem se mi podařilo získat interview a seznamy instalovaných programů. Interview trvala zpravidla 15 – 20 minut a jejich osnova je v příloze B. Pro způsob získání instalovaných programů jsem zvolil systémový příkaz *wmic product get*, který je dostupný v operačních systémech Windows a bylo jej tedy možné získat ze všech tří firem bez nutnosti instalace dalšího software. Ze seznamu instalovaných programů jsem se na základě interview s pracovníkem IT oddělení i zaměstnanců snažil určit programy, které by mohly být součástí stínového IT. Jedna z firem využívala nástroj Safetica pro bezpečnostní audit a ochranu před úniky dat a po domluvě mi byla pro účely diplomové práce poskytnuta anonymizovaná data z produktu.

Získaná data nelze považovat za zdroj zcela postihující stav stínového IT ve firmách, lze na něm však ověřit a potvrdit některé domněnky zmíněné v odborné literatuře. Proto při interpretaci dat nehodnotím jako příliš vypovídající četnost výskytu stínového IT v tomto vzorku (je pravděpodobné, že velká jeho část nebyla tímto způsobem odhalena), ale snažím se zdůraznit literaturou předpovídané výsledky, které získaná data potvrzují.

6.6 Výsledky průzkumu

V kvalitativní části výzkumu (interview se zaměstnanci) byla zjištěna tato fakta související se stínovým IT:

- Ochrana podnikové sítě a kvalita konektivity je pro firmy prioritou. Častými prohřešky zaměstnanců je vytěžování firemní sítě stahováním velkého množství dat nesouvisejících s pracovní činností. IT oddělení se na tuto oblast pečlivě zaměruje.

- Firmy často přistupují k plošnému omezení administrátorských práv na koncových stanicích, ale v nemalém množství případů je třeba toto opatření zmírnit. K tomu dochází pravidla pouze u některých zaměstnanců,

kteří ke své pracovní činnosti administrátorská práva potřebují, nebo používají takové programy, které je vyžadují.

- Firmám chybí mechanizmus pro snadné sdílení velkých souborů mimo firmu. Absenci takovéto služby nahrazují veřejnými úložišti. Kromě snadnosti tohoto řešení pro samostatné zaměstnance je důležité zmínit i přístup zákazníků mimo firmu – ti také raději používají službu, kterou znají a nejsou příliš ochotni podvolit se případnému firemnímu řešení.
- Dále se potvrdila (zejména z interview s pracovníky IT) stoupající gramotnost zaměstnanců v oblasti výpočetních technologií. Pracovníci jsou mnohem častěji schopni vyřešit problémy s informačními technologie vlastními silami.
- Hlavním problémem, který zaměstnanci ve vztahu k informačním technologiím pociťují, je zpravidla urgentní řešení konkrétního problému, než že by jim něco dlouhodobě chybělo.
- Zaměstnanci také často přistupují k porušování směrnic, protože si myslí, že nebudou detekování a že jim daný prohřešek projde bez povšimnutí.
- Pracovníci IT oddělení se shodují, že práci se stínovým IT se nemohou věnovat a musí se při své agendě věnovat jiným problémům.
- Dále zaměstnanci tvrdí, že vedení je dostatečně otevřené novým změnám, avšak zde se dá pochybovat o upřímnosti respondentů (ve svých odpovědích se neodkazují na žádný konkrétní případ, používají obecné a obligátní formulace; naopak v jednom případě zaměstnanec dokonce použil v tomto směru ironii).
- Možnost využívat pracovní zařízení berou zaměstnanci spíše jako benefit, než nepříjemnou povinnost. Navíc pracovníci na služebních zařízeních tráví zpravidla více času než se soukromými.
- Časté je také občasné použití soukromého e-mailového účtu pro vyřízení firemních záležitostí.
- Služební telefon je zpravidla nabízen čistě jako benefit s výhodným voláním a datovými službami. Pro jakýkoliv další účel jsou pracovní telefony využívány minimálně.
- IT oddělení i zaměstnanci se shodují, že soukromá zařízení se nevyplatí ve firmě plošně povolovat a používat – IT oddělení a celé firmě by to mohlo přinést více starostí než užitku.
- Časté jsou také neformální úmluvy například týkající se používání webových úložišť. Směrnice jsou často definovány pouze pro případu auditů ve firmě.

- V jednom případě bylo také odhaleno použití cloudové aplikace pro analýzu dat, do které jsou nahrávána citlivá data. Pořízení této placené aplikace bylo provedeno zcela bez vědomí IT oddělní se souhlasem přímo od nejvyššího vedení a finančního oddělní.

Kvantitativní část výzkumu přestavují seznamy instalovaných aplikací ze všech tří firem a další dodatečné informace o aktivitách uživatelů a síťovém provozu (tato data jsou k dispozici pouze za jednu firmu):

- Seznam instalovaných programů z deseti koncových stanic v každé firmě je na počítačích zaměstnanců vykonávajících podobné pozice obdobný. Žádné aplikace, které by se daly identifikovat jako stínové IT, v těchto seznamech nalezeny nebyly ani u jedné firmy.

- Z jedné firmy pak byly k dispozici síťové logy, které obsahovaly zdrojovou a cílovou IP adresu a čas relace. Drtivá většina těchto záznamů se týkala komunikace po vnitřní firemní síti. Servery mimo se buď nepodařilo reverzním prohledání DNS (na vyhledávačích Bing a Yahoo pomocí příkazu *ip:* společně s hledanou IP adresou) identifikovat nebo pravděpodobně sloužily pro pracovní účely (přístup na ně byl zablokován z důvodu nepovolené zdrojové IP adresy). Jen část webů se podařilo identifikovat jako webové stránky pravděpodobně nesouvisející s pracovní činností, ty však jsou lépe identifikovány v následujícím zdroji dat.

- Posledním zdrojem kvantitativních dat byla část anonymizovaných reportů z nástroje společnosti Safetica Technologies, který umožňuje monitorovat akce uživatelů (případně zabránit předdefinovaným akcím). Z reportů vycházejí jako stránky navštěvované mimo pracovní agendu především ty, které se týkají soukromých záležitostí (sociální sítě, zprávy, video servery, nakupování, pornografické stránky). Bylo zde zachyceno pár výskytů úložiště ulož.to a úschovna.cz, stejně tak soukromé e-mailové schránky na serverech seznam.cz a centrum.cz. Zároveň pomocí tohoto nástroje byly detekovány i pokusy o použití portable aplikací (konkrétně webového prohlížeče Opera).

6.7 Diskuze výsledků

Výsledky průzkumu provedeného ve třech českých firmách je třeba brát v kontextu rozsahu, avšak potvrzují některé aspekty stínového IT zmiňované v odborné literatuře (převážně z anglosaských univerzit). Například předpovídaný trend stoupající počítačové gramotnosti a schopnosti uživatelů řešit více problémů bez podpory IT oddělení potvrzuje jak vedení informatiky, tak zaměstnanci ostatních oddělní. Na druhou stranu se ukázalo, že zaměstnanci nemají zájem o používání soukromých zařízení (naopak jim vyhovují více oddělená a spravovaná pracovní zařízení) – tento výsledek je však vhodné vztáhnout

ke skutečnosti, že průzkum probíhal v České republice (je pravděpodobné, že například v zemích, kde cena konzumní elektroniky vzhledem k průměrnému platu představuje menší část, se může vyskytovat naopak opačný postoj).

Firmy se snaží hlavně chránit svou podnikovou síť a oficiální architekturu. Poměrně častým problémem je pak používání úložišť, které v případě špatného zacházení s daty může znamenat jejich únik nebo ztrátu. Zároveň se také v jednom případě potvrdilo, že IT oddělení může být obejito s formálním souhlasem vedení a finančního oddělení. Ve všech firmách pak existují určité výjimky z nastavených striktních pravidel, která mohou přecházet i v neformální úmluvy a kolektivnímu nedodržování politik.

Mnou provedený průzkum měl za cíl provést prvotní analýzu stavu stínového IT v České republice. Podařilo se mi poměrně věrohodně potvrdit některé premisy (byly jasně potvrzeny ve všech třech firmách různých charakteristik), avšak zejména nepotvrzené předpoklady o stínovém IT nelze brát jako vyvrácené. Pro lepší průzkum a větší vypovídající hodnotu by bylo vhodné zejména zlepšit následující parametry:

- Provést průzkum na větším vzorku firem. Zkoumané firmy by pak měly tvořit reprezentativní vzorek český firem (hledání klíče a tvorba reprezentativního vzorku je další výzvou, zároveň je třeba vypořádat se s případným odmítnutím některých firem).

- Větší využití kvantitativních metod, například monitorovacího software a aplikací pro diagnostiku uživatelských zařízení. Zde jako potenciální problém vidím schopnost těchto nástrojů detekovat výskyt stínového IT.

- Dále by mohlo poskytnout zajímavé výsledky zaměření se na větší firmy s větším IT oddělením.

- Cenným zdrojem by mohly být také seznamy incidentů uvnitř firem. Zde však může být výrazným problémem neochota firem takováto data poskytnout.

V úvodu této kapitoly jsem naznačil, že daný průzkum není dostatečně vypovídající a to zejména z důvodu malého vzorku zkoumaných firem, omezeními danými vůlí firmy určitá data poskytnout a použitou kvalitativní metodou (a sociologickými aspekty s ní spojenými). Všechna tvrzení, která jsou popsána v odborné literatuře a průzkum na ně nenalezl jednoznačnou odpověď, je třeba považovat za nezodpovězená (není jasné, zda pro český trh platí či nikoliv). Dále se některé metody průzkumu ukázaly jako značně nevypovídající o stavu stínového IT v podnicích (zejména seznam instalovaných programů získaný systémovou funkcí *wmic product get*).

Pro mě osobně bylo překvapivé zjištění, že přístup českých zaměstnanců (ve všech třech firmách) je vůči soukromým zařízením značně konzervativní. Nejen, že zaměstnanci je nevyužívají a naopak sami preferují ta pracovní, ale

zejména mě překvapil postoj, kdy by sami byli proti uvolnění politik a zavedení soukromých zařízení do firmy. Ve větší míře si nedovedou představit, že by se to firmě vyplatilo a že by IT oddělení bylo schopno novou situaci kvalitně řešit.

Kapitola 7

Modely SMB firem

Na předchozí výzkum formou interview navazuji tvorbou modelů SMB firem, pro které jsem získal anonymizovaná data od společnosti Safetica Technologies s.r.o., která vyvíjí software Safetica pro bezpečnostní audit a prevenci úniku dat. Na základě komunikace se společností jsem vydefinoval tři typické kategorie firem, na které může být z pohledu stínového IT pohlíženo odlišně. Modely firem jsou vytvořeny spojením této definice a výsledků analýz, které mi firma poskytla.

Analýzy dodané firmou byly anonymizované a obsahovaly souhrn dat za období v úseku jednoho měsíce. Za každou ze tří firem jsem obdržel tři měsíční reporty, které obsahovaly data týkající se produktivity zaměstnanců při práci s počítačem, způsob jejich práce s daty a využití IT prostředků (data byla sbírána na pracovních počítačích a výsledky byly zpracovány pouze za pracovní dobu podniku). Data byla poskytnuta firmou Safetica Technologies s.r.o. jako důvěrná, nemohu je tedy uvést v textu práce ani příloze nebo na CD přiloženém k této diplomové práci. V následujících odstavcích však popisuji jejich strukturu.

První část reportu se věnuje analýze produktivity zaměstnanců při práci s počítačem. Dokumenty obsahovaly na začátku celkové využití (časový údaj – hodiny, minuty a vteřiny) aplikací zaměstnanci za daný měsíc. Každá aplikace byla zatříděna do určité kategorie (webové prohlížeče, e-mailoví klienti aj.) a bylo u ní určeno, zda se jedná o pracovní či nepracovní aplikaci. Kromě vizualizace těchto dat v koláčovém grafu byly nejvíce využívané aplikace sepsány v tabulce a okomentovány analytiky společnosti Safetica Technologies (např. který zaměstnanec se jakou měrou podílel na využívání daných aplikací). Doba, po kterou je zaměstnanec aktivní v dané aplikaci je počítána v případě, že je okno programu v operačním systému Windows aktivní a v popředí (tj. není např. minimalizované na liště).

Další části týkající se produktivity jsou navštěvované weby. Webové adresy jsou rozřazeny do předdefinovaných kategorií (zábava, sociální sítě, zprávy aj.) a část webů, pro které se kategorii nepodařilo určit, je zahrnuta v kategorii

ostatní. Tato kategorie zpravidla představuje pouze zlomek všech záznamů (řádově do 10 %) díky nastavení společností Safetica Technologies (zkušenosti z dostatečného množství firem pro účinné nadefinování českých webů), ale i možnosti administrátorů aplikace Safetica upravit pravidla a dodefinovat další webové stránky pro konkrétní skupiny. Data kromě grafů opět v tabulce zdůrazňují rizikové weby z pohledu bezpečnosti s komentářem analytiků, zároveň je zde uveden celkový neproduktivní čas (získaný vynásobením doby trávené v prohlížeči a času stráveného na webu neproduktivně, případně přičtením času používání neproduktivních aplikací, pokud se v dané firmě vyskytují). U některých reportů je uvedena i průměrná superhrubá mzda (superhrubá mzda je stanovena na základě dat Českého statistického úřadu) a vynásobením této částky a celkového neproduktivního času jsou vyčísleny náklady na mzdy, které představují část mezd vynakládaných na neproduktivní činnost zaměstnanců.

Uvnitř části věnované webovým stránkám je i sekce zaměřená na vyhledávání pracovních nabídek zaměstnanci. Software Safetica je zaměřen na zachycení obvyklého vzorce chování zaměstnance, který společnost chce opustit (nejprve je nespokojený a klesá jeho produktivita, později začne hledat pracovní nabídky a nakonec kopíruje data a vynáší je z firmy). Vyhledávání pracovních nabídek je znamením, že zaměstnanec přestává být loajální svému zaměstnavateli, avšak pro účely této diplomové práce tato část reportu není tolik zajímavá.

Další částí je práce s firemními daty. V reportech je zachyceno vynášení dat prostřednictvím e-mailu, USB disků a externích zařízení nebo datových úložišť. V rámci reportu je opět uveden slovní komentář u nejčastějších prohřešků a jsou podrobněji rozvedeny vybrané případy, které by mohly znamenat největší hrozbu z pohledu úniku citlivých informací.

Závěrečná kapitola reportu se věnuje využívání IT zdrojů. Buď se může jednat o statistiky používání firemních tiskáren a počtu vytisknutých stran (aplikace rozlišuje a ukládá statistiky o počtu vytištěných stránek černobíle nebo barevně), nebo času běhu jednotlivých počítačů a jejich využití pracovníky. Na základě statistik o vyžívání počítačů a programů je sestaven přehled doporučení, týkající se softwarových licencí. Pomáhá tak snížit náklady firmě ušetřením za nevyužívané programy.

7.1 Způsob konstrukce modelů

Jak již bylo zmíněno v předchozí části, modely jsou konstruovány spojením obecné definice firmy, která by mohla mít z pohledu stínového IT zajímavé vlastnosti, a dat z monitorovacího softwaru Safetica. Prvotní definice (na obrázku 7.1) vychází z firemní kultury a její strategie na trhu:

Otevřená firma – Jedná se o stabilní firmu, která nemá příliš striktní vnitřní politiky. Pojmem stabilní rozumím skutečnost, že firma je dobře etablovaná

Obrázek 7.1: Prvotní definice modelových firem reprezentativních z pohledu stínového IT.

na trhu a nesoustředí se na dynamický růst. Zároveň její pozice není ohrožována vysoce konkurenčním prostředím a nemusí vynakládat velké úsilí na udržení své pozice. Podniková kultura je spíše demokratická, firemní strategie se zaměřuje na posílení vztahů se zákazníkem.

Restriktivní firma – Stabilní firma, která je svázána směrnicemi a přesně definovanými procesy. Firma může mít rovněž stabilní pozici na trhu, avšak prostředí v jejím odvětví je hodně konkurenční a soustředí se tedy na udržení své pozice. Druhým důvodem, proč je firma takto svázána, mohou být legislativní nebo procesní požadavky (zákony, případně různé certifikace upravující způsob nakládání s osobními údaji a dalšími citlivými daty). Způsob řízení zaměstnanců je spíše autoritářský. Firma může k tomuto vedení přistoupit i například z důvodu snižování nákladů.

Elastická firma – Prototypem této firmy jsou rychle rostoucí start-upy. Jedná se mladé a dynamicky rostoucí společnosti, které vznikají v nových odvětvích nebo přicházejí na trh s inovativními produkty či byznys modelem. Firemní kultura bývá zpravidla přátelská (ze strany vedení i mezi zaměstnanci), způsob řízení nevyžaduje složitou hierarchii a zaměstnanci se mezi sebou zpravidla dobře znají. Směrnice a procesy jsou v takové firmě nastaveny (nebo obcházeny) tak, aby jí nebránily v růstu nebo dalším operativním rozhodnutím. Taková firma je schopna rychle reagovat na změny podmínek a často je vyžadováno přijímat rozhodnutí ad-hoc podle nastalé situace.

Mimo tyto předběžné definice a data poskytnutá společností Safetica Technologies, mi byly sděleny praktické zkušenosti od zástupce této společnosti, které byly získány provozem softwaru Safetica pro bezpečnostní audit a zabránění úniku dat. Tyto zkušenosti nejsou použity jen při tvorbě tří základních modelů, ale pomahají utvořit obraz o významu dat, který je reflektován na konci této kapitoly při posouzení benefitů stínového IT. Jedná se především o následující poznatky:

- Změna chování zaměstnanců v čase zpravidla souvisí s procesními změ-

Počet zaměstnanců	30
Počet zaměstnanců IT oddělení	1
Počet zaměstnanců konzumujících služby IT oddělení	30
Sektor	soukromý
Odvětví	farmaceutický průmysl
Územní působnost	ČR i zahraničí
Přibližné stáří firmy	10 let
Ve firmě dochází pouze k monitorování, nikoliv k blokování spouštění aplikací nebo závadného obsahu.	

Tabulka 7.1: Charakteristiky reprezentanta otevřené firmy.

nami nebo jinými impulzy týkajícími se postoje vedení ke stínovému IT. Může se jednat například o oznámení monitorování (dojde ke změně oproti výsledkům z bezpečnostního auditu ve skrytém režimu), nebo například dojde k disciplinárnímu řízení se zaměstnancem na základě prohřešků odhalených monitorováním.

- Ve firmách, kde jsou dlouhodobě zavedená pravidla upravující existenci stínového IT, jsou zaměstnanci méně náchylní k porušování těchto pravidel.
- Pracovní kolektivy skládající se ze starších zaměstnanců jsou z pohledu porušování a stínového IT méně kreativní.
- V některých organizacích (často ve veřejném sektoru) je těžké zavádět změny politik a upravovat tak stínové IT. Hlavním problémem bývá nedostatečná podpora vedení a malý tlak na dodržování zavedených změn.
- Český trh je oproti firmám ze západních zemí specifický. Stínové IT v českých podnicích je oproti těm v západních zemích méně časté a méně rozsáhlé.

7.2 Otevřená firma

Obecná definice firmy je představena v předcházející podkapitole, v této části (i dalších dvou) nejprve představuji dodaná data od společnosti Safetica Technologies a na závěr diskutuji jejich význam a tvořím zobecněný model tohoto typu firmy. Charakteristiky firmy jsou uvedeny v tabulce 7.1.

Podle dat v dodaných reportech zaměstnanci tráví dominantní dobu v pracovních aplikacích, přibližně jedna pětina pracovní doby je pak trávena ve webových prohlížečích. Drtivou část stráveného času tvoří webmailové servery (přibližně 65 %), přibližně 20 % je pak označeno jako neproduktivní časové

využití (sociální sítě, volnočasové a hobby stránky). V podniku je používán e-mailový klient Microsoft Office Outlook, firma však používá pro e-maily cloudovou službu od firmy Google. Jedná se tedy i v případě přístupu na webmailové servery převážně o pracovní vyžití. V seznamu navštívených webových adres se nachází i soukromé e-mailové servery, jako seznam.cz nebo centrum.cz (se subdoménou například „mail.“, je tedy zřejmé, že se jedná o přístup do e-mailové schránky). V jednom ze tří měsíčních reportů se nachází i analýza odeslaných e-mailů (není specifikováno, zda se jedná o výstupy pouze s používání Microsoft Office Outlook nebo i webových klientů) a přibližně jedna čtvrtina směřuje na freemailové domény (gmail.com, seznam.cz, yahoo.com). Část e-mailů obsahovala i přílohy, ty však analytikem nebyly shledány jako rizikové z pohledu úniku dat.

Část reportu týkající se uniku dat neodhalila rozsáhlejší problémy. Při kontrole uploadu dat do cloudu nebyla analytikem shledána žádná data potenciálně riziková, avšak v jednom reportu byla odhalena aplikace Dropbox u jednoho zaměstnance jako zdroj vytěžování sítě. Jednalo se především o synchronizaci soukromých dat v úložišti a bylo doporučeno zavést politiky nastavující používání těchto aplikací na pracovišti. V dalších repotech není zmíněno, zda politika byla zavedena, nicméně tento problém už v nich není zmíněn. V případě přenosných USB úložišť bylo zaznamenáno nahrávání potenciálně citlivých firemních dat a bylo doporučeno prověření obsahu těchto souborů a zavedení používání šifrovaných přenosných úložišť ve firmě.

Z analýzy těchto dat usuzuji, že firma nemá závažnější problémy se stínovým IT a daří se jí jeho rozsah udržovat v rozumně omezené míře. K nejzávažnějším potenciálním rizikům patří používání soukromých e-mailů a kopírování dat na přenosná úložiště. Ta mohou být zdrojem úniku dat (z dodaných dat nelze usuzovat, zda opravdu k únikům došlo). Reprezentantem stínového IT v podobě aplikace je instalace klienta služby Dropbox, nezdá se však, že by se jednalo o dlouhodobý problém neřešitelný stávajícím způsobem řízení organizace. Na závěr dodejme že celkový čas zaměstnanců strávený neproduktivně se pohybuje v intervalu 3 % až 4 %.

Model firmy z pohledu stínového IT

Otevřená firma nabízí zaměstnancům určitou volnost a daří se jí udržovat stínové IT v omezeném rozsahu. Dle mého názoru k tomu přispívá loajalita zaměstnanců a jejich vědomí, že jsou monitorováni (to by potvrzovala i poměrně nízká část času stráveného neproduktivně). Zaměstnancům je i v pracovní době do určité míry tolerováno zařizování soukromých záležitostí (například možnost využití soukromých e-mailových schránek), zároveň firma není příliš striktní v používání informačních technologií (používání přenosných USB úložišť bez šifrování). Tímto na sebe firma bere určitá rizika (únik dat) - je možné, že firma se snaží těmto rizikům bránit, provádí to však skrze řízení zaměstnanců a technicky si vystačí pouze s bezpečnostním auditem (ačkoliv má

Počet zaměstnanců	100
Počet zaměstnanců IT oddělení	2-3
Počet zaměstnanců konzumujících služby IT oddělení	50
Sektor	soukromý
Odvětví	výrobní firma
Územní působnost	ČR i zahraničí
Přibližné stáří firmy	20 let
Ve firmě dochází k bezpečnostnímu auditu a blokaci určitých webových stránek a aplikací.	

Tabulka 7.2: Charakteristiky reprezentanta uzavřené firmy.

nástroj, pomocí kterého by snadno mohla restrikce zavést). Model práce se stínovým IT je založen na důvěře v zaměstnance a jejich kontrole monitorovacím nástrojem.

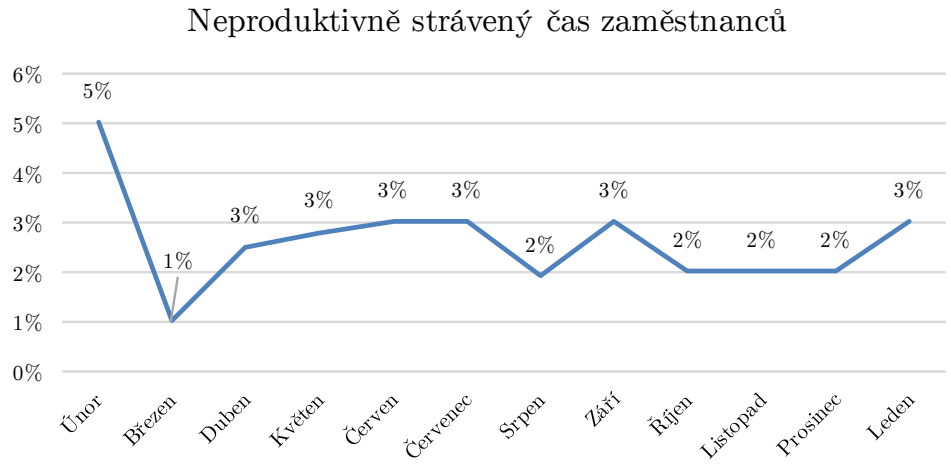
7.3 Restriktivní firma

Tento typ firmy je oproti předcházejícímu z různých důvodů více svázán omezeními. Důvody těchto omezení mohou být vnitřní (firemní kultura, způsob řízení ze strany vedení, firemní strategie) nebo vnější (konkurenční prostředí). Podrobnější obecná definice firmy je v části 7.1. Charakteristiky firmy jsou uvedeny v tabulce 7.2.

Pracovní čas zaměstnanců je převážně tráven v aplikacích pro pracovní účely, zhruba 13 % času je pak tráveno v prohlížeči. V dodaných reportech se pak neproduktivně strávené časy v prohlížeči poměrně lišily (pohybovaly se v rozmezí od 5 % do 1 % a kopírovaly trend celkové neproduktivity zmíněný dále). Pro tuto firmu mi byla dodána ještě jedna souhrnná analýza vývoje neproduktivity (souhrn neproduktivního času v prohlížeči i dalších aplikacích) za celý rok, je zobrazena na obrázku 7.2. Kromě prohlížeče byla detekována další neproduktivní činnost používáním aplikací Diablo II, Solitaire a Sudoku (počítačové hry). Po zaznamenání činnosti v těchto aplikacích došlo vždy v následujícím měsíci k jejich přidání do seznamu blokovaných aplikací.

Dalšími monitorovanými aplikacemi jsou komunikační nástroje Skype a jiné instant messaging aplikace. V těchto programech se zaměstnanci mohou věnovat neproduktivní činnosti a zároveň může hrozit únik dat. Ten se však nepotvrdil, přes komunikační nástroje bylo přenášeno minimum souborů (byly přenášeny pouze v případě programu Skype a nejednalo se o citlivá data).

Mezi aplikacemi pro sdílení souborů bylo zachyceno používání klienské aplikace pro cloudové úložiště Dropbox. Dále bylo v případě jednoho zaměstnance odhaleno používání torrentového klienta a jeho činností došlo ke stažení velkého množství dat (filmů) a došlo tak k vytížení firemní sítě. Dalším závaž-



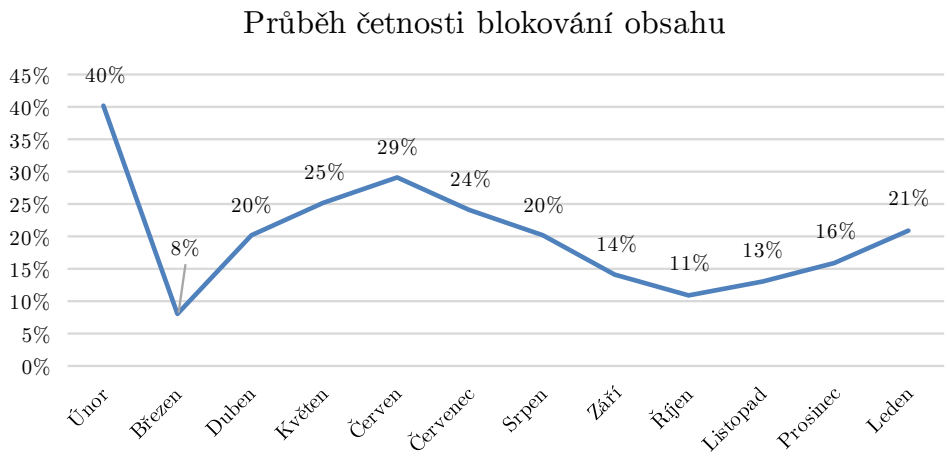
Obrázek 7.2: Část neproduktivně stráveného času u reprezentata uzavřené firmy dle společnosti Safetica Technologies.

ným problémem bylo zachycení aplikace typu keylogger, která slouží k odposlouchávání stisknutých kláves a potenciálně může odhalit i přístupová jména a hesla na počítači, na kterém je spuštěna.

V případě chování uživatelů ve webovém prohlížeči byla zaznamenána činnost osobního charakteru (sociální sítě, on-line nakupování, hraní online her nebo sázení přes internet). Závažnějším zjištěním je pak odhalená návštěva pornografických stránek – tyto stránky jsou rizikové zejména z důvodu bezpečnosti, protože se zpravidla jedná o pochybné weby, které mohou prohlížeč a počítač infikovat škodlivým softwarem. Při zachycení rizikových nebo neproduktivních stránek docházelo postupně k jejich přidávání na seznam blokovaných webů (opatření se projevila v následujícím měsíci).

Blokované weby patřily do kategorií sdílení souborů, sociální sítě, hry, stránky s nelegálním obsahem, malware, pornografické stránky, zprávy, volný čas a nakupování. Dominantní část blokovaných webů od začátku restrikcí tvořily sociální sítě, které nad ostatními kategoriemi v průběhu provozu omezení získávaly stále větší podíl (až přes 90 %). Tento trend vysvětlují analytici společnosti Safetica Technologies přístupy na stránky, které nemají povahu sociálních sítí, ale obsahují vložené služby sociálních platforem (například tlačítko „To se mi líbí“).

V případě webmailových serverů byla zachycena aktivita přibližně dvou desítek uživatelů (především na serveru seznam.cz, v menší míře i jiných). V tomto případě existuje riziko úniku firemních dat, které se i potvrdilo (docházelo k odesílání smluv a jiných citlivých právních dokumentů). Bylo zachyceno i chování jednoho zaměstnance, který nejvíce kopíroval citlivá data uvnitř firmy a právě on i nejvíce těchto dat odeslal.



Obrázek 7.3: Průběh četnosti blokování obsahu po zavedení restrikcí u reprezentanta uzavřené firmy dle společnosti Safetica Technologies.

Zaměstnanci dále v podniku používáním USB zařízení suplují funkce chybějícího síťového úložiště, které analytici doporučují zavést (přispěje k lepší kontrole nad daty a předejde tak jejich ztrátě). V případě CD a DVD byl zachycen software pro vypalování dat na tato média, tato činnost však nebyla zaznamenána (zaměstnanci pouze z těchto médií data četli). Dále bylo zachyceno i používání mobilních telefonů pro přenos pracovních dat, zde existuje opět riziko úniku dat.

V souhrnné analýze za celý rok je zmíněn i trend postupné adaptace zaměstnanců. V případě zavedení restrikcí chvíli trvá, než si na ně zaměstnanci zvyknou a poměrně často zkouší, v čem jim nová omezení zabrání a v čem nikoliv. Na obrázku 7.3 je znázorněno i rychlé vracení se do původního stavu z důvodu dočasného vyřazení blokace některých skupin webových stránek.

Z dat, která jsem měl k dispozici, soudím, že firma od počátku bezpečnostního auditu čelila velkému rozsahu stínového IT a snažila se ho restrikcemi postupně omezovat. Uvnitř firmy existovaly poměrně rozmanité podoby stínového IT. Zavádění restrikcí uživatelé přijímali postupně a byla u nich patrná značná setrvačnost ve snaze porušovat zavedená opatření. Jako velmi významný fakt hodnotím, že pokud vedení polevilo ve snaze udržet přísnou úroveň blokace (nebo došlo k jejímu dočasnému vyřazení), zaměstnanci se velmi rychle začali chovat stejným způsobem, jako před zavedením restrikcí. Poskytnutá data tedy dobře ilustrují, že ihned po zavedení restrikcí dojde k prudkému poklesu, v zaměstnancích však zůstává motivace pro obcházení omezení a postupně si hledají nové způsoby, jak opatření obejít.

Počet zaměstnanců	10
Počet zaměstnanců IT oddělení	1
Počet zaměstnanců konzumujících služby IT oddělení	10
Sektor	soukromý
Odvětví	obchod
Územní působnost	ČR i zahraničí
Přibližné stáří firmy	5 let
Ve firmě probíhá bezpečnostní audit ve skrytém režimu, žádné restrikce nejsou zavedeny.	

Tabulka 7.3: Charakteristiky reprezentanta elastické firmy.

Model firmy z pohledu stínového IT

Uzavřená firma se snaží kontrolovat stínové IT a bránit jeho vzniku restrikcemi. Dle mého názoru je tento přístup nutný tam, kde z různých důvodů (například legislativní požadavky, kázeň zaměstnanců a firemní kultura) není rozsah stínového IT dostatečně omezen (v případě zkoumané uzavřené firmy byly jeho podoby rozmanité a rozsah značný) jinými, než technologickými prostředky. Samotné vědomí, že jsou zaměstnanci monitorováni, nestačí ke změně chování zaměstnanců a firma musí dlouhodobě pracovat na restrikcích (jinak by došlo k vrácení do původního stavu), protože zaměstnanci zkouší restrikce obcházet. Lze předpokládat, že tento způsob soupeření se zaměstnanci může mít určitý negativní dopad na firemní kulturu, vztah zaměstnanců k vedení a osobní iniciativu. Firma tímto přístupem vynakládá značné úsilí, zároveň přenáší zodpovědnost za případné incidenty do značné míry na zaměstnance (firma má bezpečnostní politiky jasně nastaveny, jejich dodržování prokazatelně vynucuje a tím přenáší břemeno odpovědnosti na stranu pracovníka). Způsob řízení stínového IT je tedy založen především na nástrojích pro zabránění jeho vzniku.

7.4 Elastická firma

Obecný popis elastické firmy je představen v části 7.1, její hlavní charakteristikou je především dynamický rozvoj a hledání mezery na trhu. Z tohoto důvodu přistupuje firma benevolentněji k zavádění striktních politik a problémy řeší operativně. Charakteristiky firmy jsou uvedeny v tabulce 7.3.

Zaměstnanci v pracovní době dominantně používají webový prohlížeč (50 % až 75 %), mezi dalšími často využívanými aplikacemi nebyly žádné, které by nesouvisely s pracovní činností. Z celkového času stráveného na webových stránkách je označeno zhruba 20 % jako neproduktivní (celkový neproduktivní čas se tedy pohybuje kolem 15 %).

Zaměstnanci se na webu věnují převážně soukromým záležitostem. Převažují u nich sociální sítě (Facebook, Twitter a LinkedIn), dále tráví čas na webech s volnočasovou tematikou. Zastoupeno je také čtení zpráv, přehrávání hudby a videa a ojedinělé používání webmailových serverů. V případě použití soukromé e-mailové schránky nebyl registrován žádný únik firemních dat.

Zaměstnanci využívají komunikační aplikaci Skype, která může znamenat rizika z pohledu ztráty dat. V jednom měsíci došlo k odeslání několika souborů, jednalo se i o pracovní data. E-mailová komunikace pak je z 85 % interní a při analýze e-mailů odeslaných na externí adresy nebylo detekováno žádné riziko (data byla odesílana z firemních adres, k odesílání e-mailů s přílohami docházelo v čase rovnoměrně).

Vážné riziko představuje používání torrentového klienta jedním uživatelem, které pro firmu znamená hrozbu infekce škodlivým softwarem nebo zanesení nelegálního obsahu na pracovní počítače. Dále bylo zachyceno i časté používání cloudových úložišť Dropbox, iCloud, One Drive, na která byla nahrávána a synchronizována firemní i osobní data. Činnost těchto dvou skupin programů značně vytěžuje firemní síť a připojení do internetu. V případě používání USB zařízení nebyly zaznamenány vážnější incidenty až na případ kopírování filmu (riziko nelegálního obsahu). CD a DVD nejsou pro výměnu dat téměř vůbec používány.

Z těchto dat usuzuji, že firma se nepotýká se zásadními problémy způsobenými stínovým IT. Potenciální hrozbou je pro ni zejména únik firemních dat, případně rizikové chování některých zaměstnanců (nebezpečí nakažení počítačovým virem nebo šíření nelegálního obsahu uvnitř firmy). Zarážející je poměrně vysoká hodnota neproduktivně stráveného času, vzhledem k povaze firmy lze předpokládat, že firemní kultura je poměrně uvolněná.

Model firmy z pohledu stínového IT

Elastická firma podobně jako otevřená nepřistupuje k restrikcím, ale spoléhá na bezpečnostní audit. Zároveň je u ní patrná větší důvěra v zaměstnance (je jim tolerována nižší produktivita). Incidentům není bráněno striktními politikami, ale jsou řešeny až v rámci nastalé situace (například v případě používání torrentového klienta bylo pravděpodobně přistoupeno k domluvě zaměstnanci, v dalších reportech pak nedošlo k výskytu tohoto problému). Podobně jako v případě otevřené firmy i zde nejsou problémy řešeny zaváděním restrikcí, ale jiným (netechnickým) způsobem. Elastická firma na rozdíl od otevřené využívá data z monitorování operativně a snaží se zaměstnanci individuálně komunikovat a posouvat tak firmu dopředu (konkrétní příklad je uveden v následující části práce).

7.5 Benefity stínového IT

Z modelů uvedených výše (a získaných dat) vyplývá, že stínové IT příliš benefitů nemá (přináší do firmy především bezpečnostní rizika). Na základě komunikace se zástupcem společnosti Safetica Technologies jsem však dostal informace týkající se elastické firmy, kde bylo detekováno podezřelé chování jednoho zaměstnance (neproduktivita, komunikace mimo firmu), který následně začal vyhledávat i pracovní nabídky u konkurence. Z tohoto chování se dalo usuzovat, že zaměstnanec by mohl v nejbližší době podat výpověď. Došlo k pohovoru iniciovanému ze strany vedení, kde se podařilo odhalit důvody nespokojenosti zaměstnance a nabídnout mu změnu pracovní náplně i provést změnu určitých firemních mechanizmů. To mělo pozitivní efekt na chod celé firmy a navíc se podařilo zaměstnance ve firmě udržet.

Nejen z tohoto příkladu usuzuji, že stínové IT se dá využít jako určitý odraz nesouladu uvnitř firmy a aktivním přístupem k němu se dá rychleji odhalit a řešit vnitřní problémy podniku. V případě dat získaných u uzavřené firmy se jednalo o detekci používání USB zařízení ve velké míře, která signalizovala absenci sdíleného síťového úložiště ve firmě. Pokud má firma dostatečně účinné mechanismy na odhalování stínového IT, může získaná data využít ke zlepšení stavu podnikové informatiky i firemní kultury.

Je důležité zmínit, že nástroje pro odhalení stínového IT jsou užitečné zejména v případě, kdy jsou provozovány bez restrikcí a nevynucují změnu chování zaměstnanců. Zabraňují tak vytváření prostředí, kdy se zaměstnanci cítí být omezováni, ztrácejí důvěru ve firemní informatiku a snaží se buď soupeřit s tímto přístupem, nebo rezignují na osobní iniciativu. Tuto myšlenku mohu podpořit i výstupy z mého průzkumu v přecházející kapitole, kde mi někteří zaměstnanci ze dvou firem, ve kterých byla pracovníkům poskytnuta určitá volnost, potvrdili, že v jejich firmě došlo na základě jejich požadavku k zavedení pracovních nástrojů, které znali soukromě (a vlastní iniciativou se podíleli na zlepšení fungování podniku).

Kapitola 8

Simulační model stínového IT

V této kapitole se věnuji shrnutí poznatků získaných z odborné literatury a výzkumů z předchozích dvou kapitol. Cílem je potrhnout význam důležitých informací uvedených v dosavadním průběhu práce a vytvořit tak ucelený pohled na problematiku stínového IT. Na základě těchto znalostí sestavuji simulační model, který nabízí návod, jak a za kterých podmínek by se firma měla ke stínovému IT stavět. Simulační model vychází z modelů firem v předcházejících kapitolách, je s nimi konzistentní (odpovídá charakteristikám firem a jejich způsobu řízení stínového IT) a lze ho na tyto firmy aplikovat.

Tři typy firem (otevřená, uzavřená a elastická – viz kapitola 7) byly zvoleny jako vhodní reprezentanti z pohledu přístupu k řízení stínového IT. Přístupy v těchto modelech se v určitých aspektech odlišují (uzavřená firma tvoří určitý protipól), dva typy jsou si pak relativně podobné (otevřená a elastická firma se staví k existenci stínového IT benevolentněji). Volba jejich parametrů a vlastností však poměrně přesně odpovídá reálným přístupům většiny firem, což na základě svých zkušeností potvrdili i pracovníci společnosti Safetica Technologies.

Otevřená firma se drží firemní kultury, která je založena na důvěře v zaměstnance. Na jejich zodpovědnosti a úsudku jsou do jisté míry ponechávána rozhodnutí, co je a co není vhodné z pohledu informačních řešení na pracovišti využívat. Zaměstnanci tak sami mohou zkoušet zavádět vlastní nápady a přinášet tak firmě užitek. Tímto způsobem se aktivně podílejí na souladu byznysu s IT. Tento přístup propaguje například Francisco Barbeira, CIO banky BPI, který tvrdí, že s tímto přístupem „je každý pracovník zároveň IT pracovník“ [29]. Snahy o podobný přístup v České republice probíhají například u bank jako jsou Komerční banka a ČSOB, což mi potvrzuje vedoucí práce Ing. Pavel Náplava na základě workshopů s těmito firmami.

Model elastické firmy je do jisté míry podobný otevřené firmě. Také je zde nastavena určitá volnost pro zaměstnance, díky které si zachovávají osobní iniciativu a přispívají ke zlepšování stavu vnitřního fungování firmy. Na rozdíl od otevřené firmy se elastická ještě více zaměřuje na aktivní přístup ke stíno-

vému IT a snaží se vyhledávat jeho potenciální výhody, které by pak mohlo využít ve svůj prospěch. Základní přístup je tedy stejný, ale rozdíl je v chápání stínového IT jako příležitosti.

Problémem těchto modelů je předpoklad dostatečné kompetentnosti a loajality zaměstnanců. V případě, že si zaměstnanci nedostatečně uvědomují rizika nebo mají zlé úmysly, mohou v otevřené i elastické firmě napáchat více škod, něž ve firmě uzavřené, která omezeními a striktními politikami snižuje riziko škod plynoucích z existence stínového IT.

Uzavřená firma má politiky nastaveny natolik přísně, aby k tvorbě stínového IT docházelo minimálně, a dodržování těchto politik zaměstnanci vynucuje. Nástrojem pro účinné vynucování dodržování restrikcí jsou úpravy nastavení pracovních počítačů (odebrání administrátorských práv) a blokovací nebo monitorovací aplikace, které umožňují analyzovat činnost zaměstnanců (v reálném čase nebo zpětně) a umožňují zabránit pracovníkovi v provedení určitých nepovolených akcí. Tento přístup však s sebou nese odmítavý postoj zaměstnanců, kteří postupně rezignují na jakékoliv snahy aktivně se podílet na formování a úpravě pracovních procesů.

Problémem stínového IT je, že zaměstnanec, který ho vytváří, je vždy o krok dál než IT oddělení. Zpravidla nalezne nějakou novou skulinu ve stávajících opatřeních a pokud je tento způsob obcházení opatření odhalen, podnik na to reaguje zpětně. Tomuto faktu napomáhá i technologický a společenský vývoj, kdy zaměstnanci jsou čím dál více počítačově gramotní a vlivem konzumerizace informačních technologií jsou schopni sami provozovat nejnovější řešení na trhu (často jim k tomu stačí pouze zaplatit poplatek a mohou pak službu využívat bez nutnosti instalace na pracovní počítač – například pouze přes webový prohlížeč). Zejména v případě webových služeb a cloudových aplikací je tento trend v posledních letech dominantní a boj se stínovým IT se soustředí zejména na tuto oblast.

8.1 Optimální model a jeho ověření

Na základě obecných principů v přecházející části je sestaven model, který slouží pro určení priorit firmy, která se chce stínovým IT zaobírat. Model je tvořený skupinami otázek (jak firmy fungují, případně jak by chtěly fungovat) a odpovědí. Na základě odpovědí na tyto otázky je stanoven doporučený přístup ke stínovému IT, je zdůvodněna tato volba a jsou vyjmenována pro a proti tohoto přístupu.

1. Působí firma v odvětví, kde je nucena velmi pečlivé chránit svá data z důvodů legislativních nebo jiných nařízení (například podmínek pro udělení certifikace)?

    - *Ano* – Uzavřená firma (data musí být pečlivě chráněna).
      Výhody: Firma má předem definované nároky, podle kterých musí

chránit svá data.
Nevýhody: Firma musí přikročit k restrikcím bez možnosti vlastního rozhodnutí.

- *Ne* – Všechny typy firem (je na vedení firmy, jakou strategii zvolí).
  Výhody: Firma si může zvolit způsob, jakým bude se stínovým IT pracovat.
  Nevýhody: Nemusí existovat jasně daný rámec, jak nastavit vnitřní pravidla – rozhodnutí o jejich nastavení musí udělat vedení podniku.

2. Firma má dostatečně velký rozpočet na IT?

   - *Ano* – Všechny typy firem (firma není nucena finanční situací a může si sama přístup zvolit).
     Výhody: Firma si zvolí, podle jaké strategie bude postupovat.
     Nevýhody: Žádné.
   - *Ne* – Otevřená a elastická firma (nejsou nutné náklady na monitorovací a blokovací nástroje).
     Výhody: Firma je nucena spíše ke spolupráci než k soupeření se zaměstnanci.
     Nevýhody: Firma musí spoléhat na kompetentnost a loajalitu zaměstnanců.

3. Firma se primárně snaží o udržení pozice na trhu.

   - *Ano* – Otevřená a uzavřená firma (menší snaha riskovat, firma se soustředí na svou činnost a své zákazníky případně se snaží ochraňovat své know-how).
     Výhody: Otevřený přístup poskytuje zpětnou vazbu, restriktivní se snaží zakonzervovat původní stav (není vyžadováno rychlé přehodnocení strategie).
     Nevýhody: Stínové IT poskytuje užitečnou zpětnou vazbu a nabízí potenciál, který nemusí být zcela využit.
   - *Ne* – Uzavřená a elastická firma (v případě ztráty pozice na trhu je lepší uzavřená firma, která krátkodobě brání negativním dopadům stínového IT; elastická firma je vhodná při hledání nových možností a snaze nalézt nové trhy).
     Výhody: Rychlý nástup reálných opatření a omezení rozsahu stínového IT (uzavřená firma), dlouhodobě výhodné vzhledem k podpoře důvěry a kreativity zaměstnanců (elastická firma).
     Nevýhody: Nutnost dlouhodobé práce kvůli zamezení návratu stínového IT na původní hodnotu (uzavřená firma), kompetentnost a loajalita zaměstnanců (elastická firma).

4. Firma se primárně snaží o rychlý růst a vybudování pozice na trhu.

- *Ano* – Elastická firma (předpoklady pro využití potenciálu ve stínovém IT pro firemní zdokonalení a růst).
  Výhody: Možnost posílení firmy zevnitř a získání náskoku před konkurenty.
  Nevýhody: Kompetentnost a loajalita zaměstnanců.
- *Ne* – Otevřená a uzavřená firma (firma nemusí riskovat při práci se stínovým IT)
  Výhody: Řízení plně v kompetenci vedení.
  Nevýhody: Stínové IT poskytuje užitečnou zpětnou vazbu a nabízí potenciál, který nemusí být zcela využit.

5. Je při výběru strategie práce se stínovým IT kladen důraz na spolehlivost a kvalitu ostatních firemních procesů?

   - *Ano* – Uzavřená firma (je důležité kontrolovat a řídit rizika ze strany vedení)
     Výhody: Rizika ohrožení činnosti podniky jsou minimalizována restrikcemi.
     Nevýhody: Značné úsilí je vynakládáno na udržení restrikcí na dostatečné úrovni tak, aby nedošlo k navrácení do původního stavu.
   - *Ne* – Všechny typy firem (firma si může zvolit vlastní přístup)
     Výhody: Řízení plně v kompetenci vedení.
     Nevýhody: Žádné.

6. Je počet zaměstnanců příliš velký na operativní řízení?

   - *Ano* – Otevřená a uzavřená firma (není možné aplikovat ad-hoc řízení).
     Výhody: Nutnost definované organizační hierarchie (může být i nevýhodou).
     Nevýhody: Není možné aplikovat ad-hoc řízení.
   - *Ne* – Všechny typy firem (pro malé firmy lze aplikovat libovolný model).
     Výhody: Zvolený způsob řízení plně v kompetenci vedení.
     Nevýhody: Chybějící definovaná organizační hierarchie (může být i výhodou).

7. Jsou ve firmě problémy s firemní kulturou?

   - *Ano* – Uzavřená firma (potřeba zavedení nových politik).
     Výhody: Pomáhá se změnou firemní kultury k lepšímu (dochází k vynucování dodržení restrikcí).
     Nevýhody: Vyžaduje nemalé úsilí po dlouhou dobu.
   - *Ne* – Všechny typy firem (firma si může zvolit vlastní přístup)
     Výhody: Zvolený způsob řízení plně v kompetenci vedení.
     Nevýhody: Žádné.

8.2 Význam a způsob použití optimálního modelu

Cílem optimálního modelu popsaného v předchozí části bylo vytvořit rozhodovací strom, který pomohl vedení informatiky při volbě, jaký způsob řízení stínového IT vybrat jako nejvhodnější pro její firmu. Při tvorbě modelu se však ukázalo, že některé otázky jsou navzájem nezávislé a nemusí na sebe tedy vždy nutně navazovat. Stejně tak odpověď na většinu otázek zcela nevylučuje odlišný přístup doporučovaný v případě určité odpovědi u jiné otázky. Z tohoto důvodu bylo od tvorby rozhodovacího stromu nakonec upuštěno.

Význam zjištění z předcházejícího odstavce lze interpretovat tak, že stínové IT je poměrně rozsáhlou problematikou a tvoří ho nezávislé oblasti, ke kterým se firma může stavět různě. Může být tedy výzvou zvolit jednotný přístup v případě komplikovanějších podmínek. Z tohoto důvodu by se dalo polemizovat o jasně vymezených hranicích představených modelů – ve vší obecnosti mohou existovat podniky, které stojí na jejich pomezí a pro určité oblasti jejich fungovaní je vhodné vybrat odlišné modely.

Dle mého názoru je však vhodné celkový přístup ke stínovému IT sjednotit a přistupovat ke všem oblastem jednotně. Hlavním důvodem je jasné nakládání s benefity a řízení rizik představených v uvedených modelech. Rozdělení modelů podle typu firem (otevřená, uzavřená a elastická) považuji za dostatečně reprezentativní, toto dělení ve vztahu ke stínovému IT mi jako vhodné potvrdil i Ing. Matej Zachar ze společnosti Safetica Technologies na základě praktické zkušenosti se stínovým IT v českých firmách.

Pro lepší orientaci v optimálním modelu, který slouží pro rozhodnutí, podle jakého modelu firmy by měl podnik se stínovým IT nakládat, jsem vytvořil tabulku s ohodnocením odpovědí (viz tabulka 8.1). Čísla otázek jsou v levém sloupci, na základě kladné nebo záporné odpovědi na danou otázku je pak dle pravidel modelu přičten k modelu dané firmy bod. Na posledním řádku tabulky je pak uveden maximální a minimální součet bodů pro daný model (není možné ohodnotit odpověď kladně i záporně najednou). Na základě ohodnocení odpovědí pak lze získat součet pro reálnou firmu a určit tak model (s přihlédnutím k maximálnímu a minimálnímu možnému dosažitelnému výsledku), který bude pro danou firmu nejvhodnější.

8.3 Hypotéza proaktivního přístupu

V této podkapitole se snažím potvrdit či vyvrátit hypotézu, že proaktivní přístup ke stínovému IT může zvýšit elasticitu a flexibilitu SMB firem za předpokladu minimálního růstu investic a rizik s ním spojených. Opět využívám závěrů a dat z předchozího textu této práce a snažím se svá tvrzení podložit argumenty.

Proaktivním přístupem rozumím snahu vedení s tímto problémem pracovat. Nedochází ke kategorickému zakazování, ale snaze o porozumění stíno-

Č. otázky	Odpověď	Otevřená firma	Uzavřená firma	Elastická firma
1	ano	0	1	0
	ne	1	1	1
2	ano	1	1	1
	ne	1	0	1
3	ano	1	1	0
	ne	0	1	1
4	ano	0	0	1
	ne	1	1	0
5	ano	0	1	0
	ne	1	1	1
6	ano	1	1	0
	ne	1	1	1
7	ano	0	1	0
	ne	1	1	1
Maximum		7	7	7
Minimum		2	5	1

Tabulka 8.1: Tabulka pro výpočet hodnocení firmy dle optimálního modelu

vému IT v podniku a snaze s ním pracovat. Tento přístup je popsán v modelu elastické firmy, lze tedy předpokládat, že elasticita a flexibilita podniku s tímto přístupem vzroste a umožní mu rychleji reagovat na změny okolního prostředí (nečekané události na trhu).

Předpoklad minimálního růstu investic a rizik spojeních s proaktivním přístupem je komplikovanější problém. Investice v případě otevřené a elastické firmy jsou obdobné (je nasazen stejný monitorovací program, případně používán stejný nástroj pro posouzení rozsahu stínového IT). V případě elastické firmy je pak věnováno více času výsledku a následným akcím, jsou-li třeba. Zde se však nejedná o zásadní nárůst nákladů (není třeba zavádět nějaká bezpečnostní opatření), pouze o dostatečnou zainteresovanost vedení. Rizika jsou pak podmíněna především kompetentností a loajalitou zaměstnanců – pokud provedu srovnání s otevřeným modelem firmy, k nárůstu nedojde; v případě uzavřené firmy pak ano. Z praktické části práce je patrné, že v případě uzavřené (restriktivní) firmy dochází k větší oscilaci morálky, i tak však není možné se na zaměstnance v obecném případě plně spolehnout.

Z tohoto důvodu není možné hypotézu v plném znění potvrdit. Její závěrečnou část týkající se především rizik lze jen těžko prokázat. Naopak pro zvýšení elasticity a flexibility existuje několik argumentů. Například v jedné z firem z kapitoly 6 mi při interview byl sdělen názor, že uvnitř firmy jsou nastaveny restrikce z důvodu směrnic potřebných pro certifikaci, avšak při práci by byly natolik omezující, že bylo jejich plošné porušování umožněno a tolerováno. Ve dvou firmách z výzkumu téže kapitole 6 byl zachycena osobní

iniciativa zaměstnanců, kteří v proaktivním prostředí jsou dostatečně aktivní a přicházejí s vlastními nápady.

8.4 Finanční pohled na model

Tvorba finančního modelu pro stínové IT je limitována dostupnými daty. Lze jen těžko vyčíslit, jakou měrou je schopno stínové IT nahradit formální IT a přinést tak úspory. Stejně tak v případě politik BOYD dochází k úspoře za pracovní zařízení (to samo o sobě v tu chvíli není příkladem stínového IT), v případě na něm nainstalovaných aplikací bez vědomí IT oddělení bych jen velmi složitě určoval míru úspor, podobně jako v předchozím případě.

V případě problémů způsobených stínovým IT mi ze strany zkoumaných firem nebyla poskytnuta data o těchto incidentech – jednak je firmy považovaly za příliš citlivá a navíc často samotné firmy kolikrát nejsou schopny věrohodně vyčíslit vzniklou škodu. Finanční pohled na tuto problematiku tedy mohu podložit exaktními čísly pouze v případě reportů z kapitoly 7, kde jsou uvedeny v procentech časy strávené neproduktivně. Avšak často se jedná o čas trávený pro soukromé účely a nepatří do oblasti zájmu této práce.

V každém případě loajální a kompetentní zaměstnanec mi může skrz stínové IT přinést užitek, protože se sám sobě může stát podpůrným IT pracovníkem a firma pak vynaloží méně nákladů na jeho školení, zadávání úkolu a řešení problémů spojených s podnikovou informatikou. Z tohoto pohledu je tedy stínové IT něčím, s čím se dá pracovat i ve smyslu úspor.

Závěr

V této diplomové práci byla provedena rešerše odborné literatury v teoretické části, v praktické pak proveden průzkum problematiky v reálných firmách, analýza dat a na jejich základě zkonstruován model popisující zákonitosti ve vztahu k různým typům firem. Teoretická část se skládala s částí věnovaných definici stínového IT, uspořádání jeho forem, příčinám jeho vzniku, rizikům a dopadům na podnik a způsobům řízení stínového IT. V další kapitole jsem pak provedl průzkum stínového IT v Čechách a získal ucelený pohled na jeho stav v praxi. Následně jsem měl možnost analyzovat data dodaná společností Safetica Technologies a na jejich základě sestavit model tří zajímavých firem z pohledu řízení stínového IT. V poslední kapitole jsem dosavadní poznatky použil při tvorbě souhrnného simulačního modelu popisujícího návod na řízení stínového IT a diskutoval jsem ověření hypotézy a finanční zákonitosti stínového IT.

Výsledkem této práce je ucelený soubor informací i praktický návod, jak přistupovat k této problematice pro vedení informatiky. Úvodní teoretická část je přínosná zejména z důvodu shrnutí informací z odborné literatury v rámci jednoho dokumentu a uspořádání těchto faktů v přehledné formě. Praktická část je přínosná při volbě způsobu řízení podnikové informatiky ve vztahu ke stínovému IT pro konkrétní firmu. Vedoucí informatiky si tak může na základě charakteristik, v jakém stavu je jeho firma (nebo v jakém stavu by chtěl, aby byla), zvolit strategii, podle které bude ke stínovému IT přistupovat. Pro mě osobně práce představuje přínos z pohledu rozšíření znalostí o problematice řízení podnikové informatiky a praktické zkušenosti s výzkumem težko měřitelné problematiky, kterou stínové IT beze sporu je.

V práci byly splněny téměř všechny v úvodu stanovené cíle. Znalosti o problematice stínového IT jsou uspořádány v kapitolách 1 až 5 do logických a navazujících celků, modely fungování firem ve vztahu ke stínovému IT jsou představeny v kapitolách 7 a 8. V kapitole 8 jsou identifikovány benefity a rizika. Částečně nesplněným cílem je ověření hypotézy, že proaktivní přístup ke stínovému IT může zvýšit elasticitu a flexibilitu firem za předpokladu mi-

nimálního růstu investic a rizik s ním spojených (z důvodu nemožnosti věrohodně posoudit rizika a investice). Hypotézu nelze potvrdit ani vyvrátit v plném znění, pokud však vypustím část týkající se investic a rizik, mohu ji na základě výsledků praktické části potvrdit.

Stínové IT je v literatuře často zmiňováno jako důležitý a nový fenomén. Jeho podstata je však stará už několik desetiletí a spíše se mění jeho význam s probíhajícím technologickým a společenským vývojem. Z provedeného průzkumu a analýzy dodaných dat vyplývá, že jeho význam v České republice není až tak zásadní, jako například v západních zemích. Zároveň se v průběhu práce potvrdilo několik zákonitostí, které bych rád znovu zmínil a zdůraznil: význam stínového IT bude v budoucnu stále větší, v boji proti němu se nedá vyhrát a je třeba ho přijmout a začít s ním aktivně pracovat jako další částí informatiky uvnitř podniku.

V rámci této práce jsem provedl základní průzkum na malém vzorku firem. Další práce by zde mohly navázat a provést rozsáhlejší průzkum, případně použít další metody a potvrdit nebo vyvrátit mnou nezachycené podoby stínového IT popisované v odborné literatuře. Stínové IT je také problém mezivědní a zasloužilo by si alespoň částečný průzkum pomocí psychologie a sociologie. Další oblastí, která by tuto práci dobře doplnila, by byla sofistikovanější analýza finančních charakteristik stínového IT. Zde je hlavní výzvou získání kvalitních dat, protože pro většinu firem budou buď citlivá, nebo jimi nebudou disponovat.

Literatura

[1] WALTERS, Richard. Bringing IT out of the shadows. *Network Security*. 2013, ročník 4, s. 5–11. DOI: 10.1016/S1353-4858(13)70049-7. ISSN 13534858. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1353485813700497

[2] SILIC, Mario a Andrea BACK. Shadow IT – A view from behind the curtain. *Computers & Security*. 2014, ročník 45, s. 274–283. DOI: 10.1016/j.cose.2014.06.007. ISSN 01674048. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S016740481400100X

[3] BEHRENS, Sandy a Wasana SEDERA. Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study. In: *PACIS 2004 Proceedings*. Taiwan: aisel.aisnet.org, 2004, s. 1713–1726.

[4] JAMCRACKER, INC. Shadow IT is not a new phenomenon [online]. 2015 [cit. 2015-10-07]. Dostupné z: http://www.jamcracker.com/blogs/shadow-it-not-new-phenomenon

[5] KING, Julia. THE UPSIDE OF Shadow IT. *Computerworld*. 2012, ročník 8, s. 18–23. ISSN 0010-4841.

[6] LEFEBVRE, Mojgan, Tom CULLEN a Ursula SORITSCH-RENIER. Me and My Shadow IT. *CIO*. 2014, ročník 27, s. 26–27. ISSN 0894-9301.

[7] CAPPUCCIO, Dave. Shine Some Light on Shadow IT [online]. 2013 [cit. 2015-10-08]. Dostupné z: http://blogs.gartner.com/david_cappuccio/2013/11/27/shine-some-light-on-shadow-it/

[8] JOHNSON, Steve. Bringing IT out of the shadows. *Network Security*. 2013, ročník 12, s. 5–6. DOI: 10.1016/S1353-4858(13)70134-X. ISSN 13534858. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S135348581370134X

[9] MCCAFFERTY, Dennis. How Shadow IT Transformed the Role of CIO. *CIO Insight*. 2015, ročník 1, s. 1–1. ISSN 1535-0096.

[10] BEHRENS, Sandy. Shadow systems. In: *Communications of the ACM*. Taiwan: aisel.aisnet.org, 2009, s. 124–129, DOI: 10.1145/1461928.1461960. ISSN 00010782. Dostupné z: http://portal.acm.org/citation.cfm?doid=1461928.1461960

[11] GYÖRY, Andreas, Anne CLEVEN, Falk UEBERNICKEL, et al. EXPLORING THE SHADOWS: IT GOVERNANCE APPROACHES TO USER-DRIVEN INNOVATION. In: *ECIS 2012 Proceedings*. 2012. Dostupné z: http://aisel.aisnet.org/ecis2012/222

[12] OLAVSRUD, Thor. CBS Interactive CIO Says Shadow IT Is an Opportunity [online]. 2014 [cit. 2015-10-11]. Dostupné z: http://www.cio.com/article/2690752/it-strategy/cbs-interactive-cio-says-shadow-it-is-an-opportunity.html

[13] KPC-GROUP, S.R.O. Gartner IT Leadership Trends [online]. 2012 [cit. 2015-10-11]. Dostupné z: http://www.cacio.cz/priloha/146

[14] MOORHEAD, Patrick. How Shadow IT gives CMOs more power. [online]. 2015 [cit. 2015-10-07]. Dostupné z: http://www.cio.com/article/2887137/cmo-role/shadow-it-driving-cmos-into-more-power.html

[15] FROST & SULLIVAN. The Hidden Truth Behind Shadow IT: Six trends impacting your security posture [online]. 2013 [cit. 2015-11-16]. Dostupné z: http://www.mcafee.com/cn/resources/reports/rp-six-trends-security.pdf

[16] MAHONEY, John. *How CIOs Should Deal With Shadow IT*. GARTNER, INC, 2011.

[17] DONNELLY, Caroline. Gartner: 25% of enterprises will use corporate app stores by 2017 [online]. 2015 [cit. 2015-10-11]. Dostupné z: http://www.itpro.co.uk/645640/gartner-25-of-enterprises-will-use-corporate-app-stores-by-2017

[18] PRICEWATERHOUSECOOPERS. 2015 Global Digital IQ Survey [online]. 2015 [cit. 2015-11-16]. Dostupné z: https://www.pwc.com/gx/en/advisory-services/digital-iq-survey-2015/campaign-site/digital-iq-survey-2015.pdf

[19] SYMANTEC. Avoiding The Hidden Costs of the Cloud [online]. 2013 [cit. 2015-11-16]. Dostupné z: https://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf

[20] NASUNI. Shadow IT in the Enterprise [online]. 2015 [cit. 2015-11-16]. Dostupné z: http://www6.nasuni.com/rs/nasuni/images/White_Paper-Shadow_IT_in_the_Enterprise.pdf

[21] MCKENDRICK, Joe. 6 reasons why shadow IT is emerging from the shadows: Guess who the biggest users of shadow IT are? IT employees themselves! [online]. 2014 [cit. 2015-11-04]. Dostupné z: http://www.zdnet.com/article/6-reasons-why-shadow-it-is-emerging-from-the-shadows/

[22] ParlamentníListy.cz. Safetica: 10 nejčastějších chyb zaměstnanců při práci s firemními daty [online]. 2013 [cit. 2015-11-16]. Dostupné z: http://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Safetica-10-nejcastejsich-chyb-zamestnancu-pri-praci-s-firemnimi-daty-276543

[23] PONEMON INSTITUTE, LLC. 2009 Annual Study: Cost of a Data Breach [online]. 2010 [cit. 2015-12-14]. Dostupné z: http://www.redteamusa.com/PDF/2009%20Cost%20of%20Cyber%20Crime%20pages%2037%20pages.pdf

[24] SAFETICA TECHNOLOGIES S.R.O. Cost of a Data Breach [online]. 2011 [cit. 2015-11-16]. Dostupné z: http://downloads.safetica.com/web/documents/Cost_of_a_Data_Breach.pdf

[25] FRENKEL, Karen A. 10 Ways to Take Control of SaaS Apps and Shadow IT. *CIOInsight*. 2015, ročník 1, s. 1–1. ISSN 1535-0096.

[26] GOODWIN, Bill. How to apply IT governance in the era of shadow IT. *Computer Weekly*. 2014, ročník 8, s. 18–20. ISSN 0010-4787.

[27] BUCKSTEEG, Martin. *ITIL 2011*. Brno: Computer Press, první vydání, 2012, ISBN 9788025137321.

[28] RENTROP, Christopher a Stephan ZIMMERMANN. *Shadow IT: Management and Control of unofficial IT*. Valencie, Španělsko: IARIA, 2012, ISBN 978-1-61208-176-2, 98-102 s.

[29] BARBEIRA, Francisco. Keynote. In: *CBI 2015*. Lisabon, Protugal, 2015.

Příloha **A**

Seznam použitých zkratek

BYOA Politika soukromých aplikací v podniku (angl. Bring Your Own Application)

BYOD Politika soukromých zařízení v podniku (angl. Bring Your Own Device)

BYOS Politika soukromých řešení v podniku (angl. Bring Your Own Stuff)

CD Kompaktní disk (angl. Compact Disc)

CEO Výkonný ředitel společnosti (angl. Chief Executive Officer)

CIO Vedoucí IT oddělení (Chief Information Officer)

CRM Systém pro řízení vztahů se zákazníky (angl. Customer Relationship Management)

DNS Systém doménových jmen (angl. Domain Name System)

DVD Digitální víceúčelový disk (angl. Digital Versatile Disc)

ERP Systém pro plánování podnikový zdrojů (angl. Enterprise Resource Planning)

HW Hardware

IT Informační technologie nebo též informatika (např. podniková)

MS Office Microsoft Office

P2P Peer-to-peer

PDF Přenosný formát dokumentů (angl. Portable Document Format)

SaaS Software jako služba (angl. Software as a service)

SIT Stínové IT (angl. Shadow IT)

SLA Smlouva mezi poskytovatelem a uživatelem služby (angl. Service Level Agreement)

SMB Malé a střední podniky (angl. Small and Medium Business)

SW Software

VPN Univerzální sériová sběrnice (angl. Universal Serial Bus)

WiFi-AP Přístupový bod WiFi (angl. WiFi Access Point)

Příloha B

Interview použité pro průzkum stínového IT v českých firmách

V této příloze jsou podrobné informace týkající se interview, které bylo provedeno ve třech českých firmách s celkem 12 respondenty (průzkum je detailně popsán v kapitole 6).

B.1 Rozdělení na dvě skupiny respondentů

V každé firmě bylo interview provedeno s 1 pracovníkem z IT oddělení a dále se 3 respondenty z jiných než IT oddělení. Cílem bylo získání pohledu z obou stran, které mají odlišné zájmy a pohnutky. V následujících částech uvádím plné znění pokynů, které byly poslány respondentům s několikadenním předstihem.

B.1.1 Pokyny před interview - pracovník IT oddělení

Interview se bude týkat „stínového IT“ (používání zařízení, software a dalších informačních technologií bez vědomí IT oddělení uvnitř podniku).

Informace získané v tomto interview slouží pro výzkum v rámci diplomové práce, v jejím textu pak budou použity výhradně anonymně. Interview bude nahráváno pro účely následného přepisu a analýzy.

Interview bude zaměřeno na Vaše pracovní zkušenosti, které by se mohly týkat stínového IT. Není požadována odborná znalost této problematiky ani aktivní zkušenost.

Interview bude trvat přibližně 15 minut formou diskuze podle následující osnovy:

- Obecné informace o IT v podniku
- Vaše zkušenosti se stínovým IT

- Váš postoj ke stínovému IT
- Firemní směrnice a politiky

B.1.2 Pokyny před interview - pracovník mimo IT oddělení

Interview se bude týkat „stínového IT“ (používání zařízení, software a dalších informačních technologií mimo IT oddělení).

Informace získané v tomto interview slouží pro výzkum v rámci diplomové práce, v jejím textu pak budou použity výhradně anonymně. Interview bude nahráváno pro účely následného přepisu a analýzy.

Interview bude zaměřeno na Vaše pracovní zkušenosti, které by se mohly týkat stínového IT. Není požadována odborná znalost této problematiky ani aktivní zkušenost.

Interview bude trvat přibližně 15 minut formou diskuze podle následující osnovy:

- Obecné informace o IT v podniku
- Nástroje pro lepší produktivitu
- Váš postoj ke stínovému IT
- Firemní směrnice a politiky

B.2 Průběh interview

Samotné interview probíhalo tak, že jsem respondentům ještě jednou zopakoval téma interview a upozornil je, že z důvodů přepisu bude interview nahráváno. V průběhu interview jsem se respondentů doptával případně upřesňoval otázky tak, aby jim bylo zcela porozuměno. V případě, že se respondent sám rozhovořil, nepřerušoval jsem jej a snažil jsem doptat na případné podrobnosti (pokud se to týkalo předmětu kterékoliv otázky z interview). Z tohoto důvodu se často stalo, že respondent s předstihem odpověděl na některé otázky a bylo je tedy nutné přeskočit.

B.3 Otázky (témata)

V následujících částech jsou poznamenány otázky a témata. Otázky jsou znázorněny kurzívou, ostatní jsou poznámky týkající se kontextu. Interview bylo postaveno tak, aby kopírovalo strukturu teoretické části diplomové práce v kapitolách 1 až 5.

B.3.1 Pracovník IT oddělení

- Obecné
- *Stínové IT se týká informačních technologií používaných potají, setkal jste se s něčím takovým?*
- *Náplní Vaší práce je především dohled nad pracovními počítači zaměstnanců a servery, případně byste zmínil něco jiného?*
- Formy stínového IT
- Mobilní zařízení
  - *Je u Vás povolena politika BYOD, mohou zaměstnanci používat soukromé telefony? Děje se to případně bez souhlasu vedení?*
- WiFi AP, čtečky, vypalovačky, tiskárny, skenery.
  - *Přinesl Vám zaměstnanec do firmy např. vlastní WiFi AP, čtečku, vypalovačku...?*
- Cloudové aplikace, webové služby
  - *Máte představu, zda zaměstnanci používají občas úložiště (Dropbox, úschovna.cz...)?*
  - *Nebo jiné služby na webu (soukromý mail, vedení poznámek Evernote)?*
- Portable aplikace, kodeky, nastavení, čištění počítačů.
  - *Používají zaměstnanci portable aplikace?*
  - *Nebo další utility (kodeky, CCleaner apod.)?*
- Externí (nová zařízení)/interní (změny).
  - *Myslíte, že zaměstnanci ke stínovému IT používají firemní počítače/telefony, nebo si nosí vlastní zařízení?*
- Určení aplikace
  - *Myslíte, že zaměstnanci používají nějaké aplikace z následujícího seznamu?*
    - *Volný čas (soc. sítě)*
    - *Kancelářské balíky*
    - *Úložiště*
    - *Informační systémy*
    - *Komunikátory*

        - *Webové prohlížeče*
        - *Další?*

- Příčiny vzniku stínového IT (zjistit problémy v komunikaci)
    - Podnik motivátorem
        - *Proč to zaměstnanci dělají, chtějí mít novější verze prohlížečů, novější funkce programů, kancelářských balíků…?*
        - *Patří mezi takové programy něco, bez čeho by se těžko obešli?*
        - *Nesouvisí to s novou politikou (např. zavedením BYOD)?*
        - *Není problém v přístupu vedení (např. jiná oddělení to tolerují/sama vytvářejí)?*
- Zaměstnanec motivátorem
    - *Proč si myslíte, že si to zaměstnanec dovolí? Vede ho k tomu neznalost směrnic/pravidel?*
    - *Nebo se ospravedlňují („ale já to potřeboval“)?*
    - *Nebo prostě ignorují pravidla/nařízení?*
- Technologie motivátorem
    - *Myslíte, že tomu napomáhá vývoj informačních technologií (lepší zařízení, aplikace)?*
    - *Nebo také jednoduchost (za pár chvil si naklikám aplikaci v prohlížeči, nepotřebuji pomoci s instalací/nastavením...)?*
- Rizika a dopady na podnik
    - Negativní - Bezpečnost přístupu k datům
        - *Rizikem je přístup k datům. Bylo u Vás stínové IT někdy příčinou úniku, ztráty, nebo nedostupnosti dat?*
    - Negativní - Narušení fungování podniku
        - *Narušil nějaký incident spojený se stínovým IT chod firmy (nešlo plnit nasmlouvané služby/prodávat/vyrábět)?*
    - Pozitivní
        - *Myslíte, že se dá uspořit povolením soukromých zařízení a telefonů?*
        - *Myslíte, že budou zaměstnanci produktivnější na vlastních zařízeních?*
        - *Myslíte, že touto neoficiální cestou se dá rychleji reagovat na potřeby podniku?*

  - Způsoby řízení - Imperativní způsob, jaké jsou politiky
    * *Jakým způsobem se ke stínovému IT stavíte ve Vaší firmě?*
    * *Máte definované směrnice/politky? Poučujete o nich zaměstnance (jak)?*
  - Způsoby řízení - Motivace
    * *Jakou přikládáte důležitost existenci stínového IT (je pro Vás prioritou něco jiného?)? Sdílí tento postoj i vedení firmy, nebo má odlišný?*
    * *Jak posuzujete rozsah stínového IT?*

B.3.2 Pracovník mimo IT oddělení

- Obecné
- *Je součástí Vaší pracovní agendy práce s počítačem?*
- *Máte služební nebo soukromý chytrý telefon?*
- Formy stínového IT
- Mobilní zařízení
  - *Mohl by Vám být telefon při práci užitečný (kromě volání)? Např. jako úložiště, navigace...?*
- Wifi AP, čtečky, vypalovačky, tiskárny, skenery.
  - *Nebo jiné zařízení (čtečka, skener, externí disk)?*
- Cloudové aplikace, webové služby
  - *Potřebujete někdy použít úložiště Dropbox, úschovna.cz?*
  - *Nebo jiné služby (soukromý mail – při výpadku firemního serveru)?*
  - *Používáte aplikaci na poznámky (např. Evernote)?*
- Portable aplikace, kodeky, nastavení, čištění počítačů.
  - *Nemáte problém s kodeky při přehrání videa?*
  - *Není Váš počítač občas pomalý, zanesený (a chtělo by ho přeinstalovat/přenastavit)?*
- Externí (nová zařízení)/interní (změny).
  - *Stačí Vám pro práci zařízení na pracovišti, nebo občas musíte donést soukromé?*
- Určení aplikace

  - *Jaké používáte aplikace z následujících oblastí?*
    - *Kancelářské balíky (MS Office)*
    - *Úložiště (USB disky, externí disky, cloudová úložiště - Dropbox)*
    - *Informační systémy (SAP, účetnictví)*
    - *Komunikátory (Skype)*
    - *Webové prohlížeče*
    - *Další?*

- Příčiny vzniku stínového IT (zjistit problémy v komunikaci)
  - Podnik motivátorem
    - *Máte v podniku aktualizované verze prohlížečů a jiných programů, nebo na nejnovější verze můžete chvíli čekat?*
    - *Chybí Vám ve firmě nějaký program, který by se Vám opravdu hodil?*
    - *Jak to bylo s politikou soukromých zařízení ve firmě – neprovádělo vedení podniku nějaké přehodnocení postoje?*
    - *Mohou jiní zaměstnanci/jiná oddělení používat soukromá zařízení více než ostatní?*
- Zaměstnanec motivátorem
  - *Jsou u Vás ve firmě nějaká omezení/pravidla pro používání informačních technologií?*
  - *Jsou užitečná, nebo Vám naopak spíše nepomáhají (a byrokraticky svazují ruce)?*
  - *Jak vnímáte důležitost těchto pravidel/směrnic?*
- Technologie motivátorem
  - *Vnímáte v podniku změnu postoje k pracovním zařízením v souvislosti s technologickým vývojem (firma např. vstřícnější)?*
  - *Použil(a) jste někdy (i např. doma soukromě) aplikaci formou předplatného (např. měsíční poplatek za Office 365, Spotify...)?*
- Rizika a dopady na podnik
  - Pozitivní
    - *Myslíte, že je pro firmu výhodné povolení soukromých zařízení?*
    - *Dovedl(a) byste si představit práci na soukromém počítači/telefonu? Byla by pro Vás práce na vlastním zařízení pohodlnější, případně produktivnější?*

    - *Potřebujete někdy provést úpravu nastavení pracovního počátače a čekáte na ni poměrně dlouho?*

- Negativní - Bezpečnost přístupu k datům
    - *Napadají Vás nějaká rizika, pokud například instalujete vlastní aplikaci na pracovní počítač (Únik, ztráta/nedostupnost)?*
- Negativní - Narušení fungování podniku
    - *Mohla by instalace vlastního programu nebo použití soukromého telefonu narušit chod celé firmy? Napadá Vás konkrétní scénář, co by se mohlo stát?*
- Způsoby řízení - Imperativní způsob, jaké jsou politiky
    - *Jaký je postoj vedení k soukromým zařízením a programům ve Vaší firmě?*

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF