Sem vložte zadání Vaší práce.

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

Bakalářská práce

Možnosti využití vlastních zařízení ve firemním prostředí (BYOD)

Lukáš Trnka

Vedoucí práce: Ing. Pavel Náplava

10. května 2015

Poděkování

Chtěl bych poděkovat panu Ing. Pavlu Náplavovi za jeho vstřícný přístup a cenné konzultace, ze kterých jsem si vždy odnášel užitečné rady a doporučení. Dále bych rád poděkoval Františku Mastnému a Tomáši Vosykovi, jejichž diplomové práce mi pomohly zorientovat se v problematice.

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, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 10. května 2015 .....

Odkaz na tuto práci

Trnka, Lukáš. *Možnosti využití vlastních zařízení ve firemním prostředí (BYOD)*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2015.

Abstrakt

Tato bakalářská práce seznamuje čtenáře s problematikou užívání soukromých zařízení zaměstnanců pro pracovní účely, označovanou pojmem BYOD. Firmy mohou podporou BYODu dosáhnout lepší produktivity svých zaměstnanců i finančních úspor v oblasti firemního IT. Přináší to ale také řadu možných potíží a rizik, jako je třeba hrozba zavirování firemní sítě nebo únik firemních dat ze špatně zabezpečeného zařízení. Práce přináší čtenáři potřebné znalosti, aby dokázal informovaně posoudit vhodnost nasazení BYODu do vlastní firmy. Informace získané z provedené analýzy tématu byly využity k vytvoření interaktivního dotazníku, který vypovídá o tom, nakolik by pro případného zájemce mohl být BYOD užitečný.

Klíčová slova BYOD, EMM, MDM, správa mobilních zařízení, mobilita, konzumerizace IT, mobilní zařízení, smartphone, tablet, notebook

Abstract

This thesis introduces the reader to the issue of the use of employees' private devices for work purposes. The practice is commonly abbreviated as BYOD. By supporting BYOD, businesses can achieve better productivity of

their employees and cost savings in corporate IT. However it brings a number of potential problems and risks, such as the threat of virus infection of the corporate network or corporate data leakage from poorly secured devices. This work provides readers with the necessary knowledge to be able to assess the appropriateness of deploying BYOD to their own businesses. Information obtained from the analysis of this topic have been used to create an interactive questionnaire, which can provide useful information to anyone interested in BYOD as to whether it could be beneficial in their respective case.

Keywords BYOD, EMM, MDM, mobile device management, mobility, consumerization of IT, mobile device, smartphone, tablet, notebook

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Je trendem dnešní doby obklopovat se různými hi-tech mobilními zařízeními, která se snaží být každým rokem ještě lepší a zákaznicky zajímavější. Zařízení jako chytré telefony, notebooky či tablety se staly běžnou součástí každodenního života mnoha lidí po celém světě, což je dáno jak velkou praktičností a univerzálností těchto zařízení, tak i tím, že nesou určitý punc luxusu a prestiže. Staly se fenoménem doby a proměnily podobu našeho fungování způsobem, který si ještě před deseti lety dokázal jen málokdo představit. Rozsah změn, které s tímto přišly, si teprve začínáme uvědomovat, včetně potíží a komplikací s tím souvisejících. Řada lidí až nyní začíná hledat vhodná řešení, která by jim pomohla vypořádat se s nastalou situací či z ní vytěžit maximum potenciálu, jež nabízí.

Ačkoliv jsou tato mobilní zařízení původně cílena na běžné zákazníky, stále větší pozornost jim je nucena věnovat i řada firem a organizací. Mobilní zařízení se totiž stala natolik populárními a užitečnými pomocníky, že se jich lidé nechtějí vzdát ani v zaměstnání, kde mají tendence využívat je jak k pracovně neproduktivním činnostem, tak ale i k zefektivňování a zrychlování své práce. Zaměstnanci takto mohou pro ně příjemným způsobem zvýšit svou produktivitu, z čehož následně profituje i instituce, pro niž pracují. Zařízení, která fungují ve firemním prostředí bez vědomí a dohledu firmy však mohou způsobit i značné škody. Příkladem může být zavlečení počítačových virů do podnikové infrastruktury či únik interních dokumentů.

Mnoho firem zvažuje, jak se ke konceptu využívání soukromých zařízení ve firemním prostředí postavit, zda to podporovat a když, tak jakým způsobem. Cílem této práce je analyzovat problematiku, tak aby na tyto otázky pomohla odpovědět. V následujícím textu budou popsány základní pojmy, klíčové parametry i dopady týkající se využití koncepce, na což bude navazovat metodologický rámec, který pomůže ke zhodnocení smysluplnosti u reálného zájemce.

Poznámka k citování zdrojů: Citace zdrojů, které jsou v této práci uvedeny na konci odstavců, se vztahují k celému odstavci, na jehož konci se nacházejí.

Poznámka k obrázkům: Grafy a obrázky jsou převzaty z uvedených zdrojů a jsou tedy nepřeloženy.

Kapitola 1

Historie

V následujících odstavcích bude popsán počátek a následný rozmach mobilních zařízení, zejména smartphonů a tabletů. Dále jejich pronikání do firemního prostředí, uvědomování si potíží a hrozeb, které to přináší a objevování výhod, které se z toho dají potenciálně vytěžit. Ve stručnosti budou zmíněny firemní nástroje na správu mobilních zařízení, tak jak postupně vznikaly. Ty budou podrobněji rozebrány v následujících kapitolách této práce. Nakonec bude zmíněno současné směřování vývoje problematiky mobilních zařízení ve firemním prostředí, včetně možného budoucího vývoje.

1.1 Na počátku

První malá přenosná zařízení, kterými si běžní uživatelé mohli vypomáhat v práci, se používala již v devadesátých letech minulého století. Pionýrem v této oblasti byla britská firma Psion se svým osobním digitálním asistentem. Ačkoliv se jednalo o první komerčně použitelný výrobek tohoto typu, celosvětově se příliš neprosadil.[1] Většího tržního úspěchu dosáhla až teprve americká společnost Apple, když v roce 1993 představila svůj Newton MessagePad. Od Applu také pochází obecné označení pro tato zařízení – PDA, tedy Personal Digital Assistant (osobní digitální asistent). Krátce po Applu se výrobě PDA zařízení začala věnovat i řada dalších výrobců. Jedním z nejpopulárnějších PDA byl Palm Pilot od firmy Palm. Ve své době byly PDA používány řadou zaměstnanců jako praktický pomocník. Širší popularity mezi běžnými zákazníky se jim však nikdy nedostalo. Dnes jsou PDA již považovány za zastaralé a lidé před nimi dávají přednost chytrým telefonům či tabletům.[2]

1.2 Revoluce zvaná iPhone

Ačkoliv o určité chytré telefony se výrobci pokoušeli již dříve, éra smartphonů naplno začala až teprve 9. 1. 2007, kdy společnost Apple představila světu

	iPhone	Samsung BlackJack	BlackBerry 8800	Treo 700p
Price	$499 or $599	$199	$299	$299
Weight	4.8 oz.	3.5 oz.	4.7 oz.	6.4 oz.
Dimensions	4.5 x 2.4 x 0.46″	4.5 x 2.3 x .5″	4.5 x 2.6 x .55″	4.4 x 2.3 x .9
Estimated battery life (hours)	Talk Time: 8 Standby: 250 Internet Use: 6 Video Playback: 7 Audio playback: 24	Talk time: 5.5 Standby: 264	Talk time: 5 Standby: 528	Talk time: 4.5 Standby: 300
Screen size	3.5″	2.2″	2.5″	2.6″

Obrázek 1.1: Porovnání prvního iPhonu s dalšími tehdejšími chytrými telefony.[4]

iPhone – svůj vlastní chytrý mobilní telefon s plně dotykovým ovládáním, elegantním designem a velmi intuitivním uživatelským prostředím. I přes to že první iPhony ze začátku nenabízely řadu funkcí, které už jejich konkurenti dávno měli, staly se brzy doslova hitem, na který museli reagovat i ostatní výrobci mobilních telefonů.[3]

1.3 Éra smartphonů

Už 5. listopadu 2007 přišla společnost Google s odpovědí na iPhone, když představila softwarovou platformu Android. Ve sdružení s dalšími firmami pak 23. září 2008 vypustila první verzi operačního systému Android do světa. Rozhodující bylo ale až uvedení mobilního telefonu T-Mobile G1 (HTC Dream) na trh (obrázek 1.2). Byl to totiž první smartphone vybavený tímto operačním systémem. Když byl pak 22. října stejného roku uživatelům zpřístupněn Android Market, kde si mohli kupovat různé aplikace a instalovat si je na své chytré telefony fungující na OS Android, začala popularita Androidu růst. Postupně vznikaly další a další aplikace. A stejně tak přicházely na trh i další a další modely chytrých telefonů od různých výrobců, které běžely převážně na systému Android.[5]

Nezahálel ani Apple, který postupně doplnil vše, co do té doby iPhonům oproti konkurenci chybělo a otevřel vlastní appstore s rozmanitými aplikacemi pro své zákazníky. Telefony od Applu a telefony fungující na OS Android

Obrázek 1.2: První smartphone užívající platformu Android.[6]

se sebou začaly konkurenčně bojovat, což hnalo vývoj smarthphonů dál a dál. Postupně se do tohoto souboje zapojily i další společnosti, které se snaží dohnat náskok Applu a Googlu, jako třeba firma Microsoft se svým operačním systémem Windows Phone nebo firma RIM[1] se svým BlackBerry OS.

Běžným zákazníkům se tak začaly nabízet různé smartphone jak ve vyšších, tak i v nižších cenových kategoriích. Společně s tím přišlo doslova nepřeberné množství aplikací, i dalších služeb přístupných přes mobilní telefony.

1.4 Někde mezi smartphony a notebooky

Jednou z hlavních výhod mobilních telefonů je jejich mobilita. Kvůli požadavku snadné přenosnosti ale nemohou nabídnout velkou obrazovku, pohodlnou klávesnici ani výkon rovnající se běžným PC. Mezi uživateli, toužícími především po konzumaci digitálního obsahu a ne už tak moc jeho tvorbě, vznikla tedy poptávka po zařízení pokud možno stejně mobilním a pohotovém jako smartphone, které by ale nabízelo především větší displej. Na tuto poptávku dokázala odpovídajícím způsobem zareagovat opět společnost Apple, když v lednu 2010 představila svůj nový výrobek pod názvem iPad, který se stal prvním novodobým tabletem.

Už v „dávných dobách digitální techniky“ byly pokusy o vytvoření tabletů. Nikdy však nebyly příliš komerčně úspěšné. Výrobci se totiž vždy snažili vytvořit v podstatě klasické notebooky vybavené navíc dotykovou obrazovkou a drobnými softwarovými doplňky v rámci operačního systému. Nikdy tedy vlastně nevytvořili operační systém, který by byl od základu vyladěný pro ovládání pomocí dotyků. Kvůli tomu byly používány, po připojení klávesnice a myši hlavně opět jako obyčejné notebooky. Až teprve iPad od Applu byl

[1]Společnost RIM se v roce 2013 přejmenovala na BlackBerry

vytvořen podle té správné koncepce a nabídl uživatelům především konzumaci multimediálního obsahu zpřístupněnou pomocí odladěného dotykového ovládání.[7]

I v oblasti tabletů mají nyní zákazníci široký výběr. Výhodou je i to, že řada tabletů nabízí uživatelům známé uživatelské prostředí, na které jsou zvyklí ze svých smartphonů. Nabídka všemožných aplikací, ať už určených pro zábavu či práci, se dále rozrůstá. A zájem o tablety podporují i různé internetové služby, které tak lidé mohou využívat kdekoliv a kdykoliv. Podle údajů analytické společnosti IDC vzrostly prodeje tabletů v roce 2013 o 52 % oproti předchozímu roku. Další závratný růst se ovšem v této oblasti už očekávat nedá. Alespoň ne v dohledné době. Loňské prodeje tabletů totiž vzrostly už jen o 7,2 % a i pro následující roky se očekává jen pozvolný růst. Důvodem však není ztráta zájmu uživatelů o podobná zařízení ani jejich nahrazení „zařízeními 2 v 1“ kombinující tablet a notebook. Za hlavní důvod se předpokládá mylný odhad délky životního cyklu tabletů, který se ukázal být výrazně delší než 2-3 roky, jako je to u smartphonů. Uživatelům zkrátka jejich staré tablety pořád stačí a díky pokračující softwarové podpoře je nepotřebují tak často měnit.[8]

1.5 Objevení BYODu

Jak rostl trh s mobilními zařízeními, zaměstnanci začali stále častěji využívat své soukromé smartphony a tablety i v práci, kde je částečně využívali k plnění svých pracovních povinností, připojovali je do firemní počítačové sítě (často bez vědomí podnikového IT oddělení) a práci si s nimi různě usnadňovali. Tento trend mezi svými zaměstnanci rozpoznal v roce 2009 Intel, který pro to následně i zavedl do širšího povědomí anglický termín „bring your own device“ (BYOD).[9]

Při myšlence na zaměstnance volně si do firemního prostředí přinášející své soukromé přístroje, řada firem instinktivně sahala po restrikcích a zákazech, kterými by tomuto jevu zamezila. Něco takového totiž firmám přináší různé problémy a rizika, jako třeba únik firemních dat ven z korporátního prostředí, snadnější zneužívání podnikového internetu pro soukromé účely či zavlečení virů a malwaru na firemní počítače. Firma Intel se nicméně rozhodla jít opačnou cestou a začali tento jev naopak podporovat s cílem zvýšit tak produktivitu svých zaměstnanců a snížit výdaje na firemní IT vybavení. Od začátku roku 2010 se počet zaměstnanci vlastněných mobilních zařízení používaných k práci zvýšil z 10 000 na 30 000 lidí a firma Intel očekává, že v budoucnu se do firemního BYOD programu zapojí většina z jejích přibližně 80 000 zaměstnanců.[9]

Popularita smartphonů a tabletů byla mezi zaměstnanci tak veliká, že firemní manažeři čelili narůstajícímu tlaku, aby ustoupili od blokování tohoto trendu a začali hledat jiné způsoby, jak se s ním vypořádat.

Před příchodem prvního iPhonu kralovaly firemním prostředím smartphony BlackBerry od firmy RIM. Tito předchůdci moderních smartphonů cílili přímo na využití v podnikovém prostředí, ke kterému byli uzpůsobeni, a řada firem je také podporovala a měla pro ně zavedenou potřebnou bezpečnostní infrastrukturu. Běžné uživatele však telefony BlackBerry příliš neoslovovaly. Potíží s ostatními smartphony bylo však to, že byly zacíleny pouze na běžného zákazníka a neumožňovaly téměř žádnou firemní kontrolu a zabezpečení.

1.6 Správa mobilních zařízení

Ještě v roce 2010, v rámci uvedení nové verze svého operačního systému iOS 4, poskytla společnost Apple první API, které umožňovalo firmám spravovat zaměstnanecká mobilní zařízení. Zároveň s tím se začaly objevovat první komerční řešení nabízející firmám vhodné softwarové nástroje pro správu zaměstnaneckých mobilních zařízení označované zkratkou MDM, tedy Mobile Device Management. Od roku 2011 začalo stále více firem zavádět BYOD politiky, které umožňovaly zaměstnancům využívat jejich mobilní zařízení v práci a stanovovaly pro to vhodná pravidla. Firmy Google, Apple i další menší výrobci mobilních OS pokračovali v uzpůsobování svých produktů potřebám podnikového prostředí, což jen podpořilo ústup telefonů BlackBerry z pozice hlavních firemních smartphonů.

Různé případy úniků firemních dat prostřednictvím soukromých telefonů a tabletů zaměstnanců se postupně začaly množit a okolo roku 2013 už bylo jasné, že samotné MDM nástroje nejsou dostatečné. A tak aby se problém vyřešil, byla vymyšlena nová třípísmenná zkratka – MAM pro Mobile Application Management, tedy správu mobilních aplikací. MAM umožňovalo mimo jiné dodávání firemních aplikací a jejich konfiguraci na zařízení zaměstnance.

Jelikož bylo zabezpečení dat stále tíživým tématem, přibyla brzy ještě jedna třípísmenná zkratka a to MCM, označující sadu nástrojů pro správu mobilního obsahu. Díky MCM bylo nyní možné zabalovat firemní aplikace a data do virtuálních kontejnerů, díky čemuž se tak spolehlivě a bezpečně oddělily od soukromých aplikací a dat uživatelů.[10]

1.7 Současnost řízení BYODu

Od svého zrození před teprve několika málo lety se možnosti BYODu i přístupy k jeho řízení hodně vyvinuly. Řešení, která postupně vznikla, jsou nyní sjednocena pod pojem Enterprise Mobility Management (EMM). Firmy si uvědomily význam zaměstnanecké mobility a proto se i snaží využívat dostupné technologie k tomu, aby jí podpořili. Ve výzkumu společnosti Gartner označili vedoucí pracovníci firemních IT oddělení mobilitu za jednu ze tří nejdůležitějších priorit. Kromě výzev týkajících se stále komplikovanějšího zabezpečení dat a podpory uživatelů, se podniky také snaží poskytovat například i firemní

nástroje pro spolupráci s ostatními zaměstnanci a to jak v rámci jednoho pracoviště, tak i na dálku.[11]

1.8 Budoucí vývoj

Vývoj technologií a postupů určených k řízení BYODu a zaměstnanecké mobility je nyní stále relativně na začátku, takže se dá očekávat řada dalších změn. Společnost Gartner odhaduje, že se jednotlivé společnosti v blízké době začnou více zabývat ochranou svých autorských práv u digitálního obsahu, pro což poskytnou výrobci EMM řešení potřebné technologie. Dále se předpokládá rozšíření spolupráce EMM technologií s technologiemi zabezpečujícími firemní správu identity a přístupu. Tak aby například při zjištění, že u nějakého ze zaměstnaneckých zařízení bylo prolomeno uzavření operačního systému a vzniklo tak potenciální riziko pro firmu, byla automaticky vyvolána reakce v systému správy přístupu a dané zařízení tak bylo okamžitě odříznuto od firemních služeb.[11]

V delším časovém horizontu pak Gartner předpovídá vznik jednotné technologie Unified Endpoint Management, která už nebude poskytovat řadu různých platforem pro správu zvlášť každého typu zařízení, ale nabídne jednotný nástroj. Prací firemních IT oddělení bude řídit zaměstnancovu osobní množinu komponent obsahující mobilní zařízení, PC a i další věci a služby, které by mohl potřebovat.[11]

V této kapitole byly popsány první PDA zařízení, které byly využívány zaměstnanci v prostředí jejich zaměstnání. Jak bylo řečeno, nebyly příliš masově rozšířeny a jejich užívání se omezovalo hlavně na firemní práci. S příchodem prvního iPhonu se však oblast chytrých mobilních zařízení zpopularizovala u běžných zákazníků a začala se překotně vyvíjet. Šíření těchto pro běžné uživatele určených zařízení brzy zasáhlo prostředí firem a organizací, kterým to způsobilo řadu nepříjemností a přinutilo je to hledat postupy a nástroje pro správu zaměstnanci vlastněných zařízení a jejich usměrnění v mezích pravidel firmy. Nástroje označované jako MDM se postupně rozšiřovaly a dnes bývají všechny sjednoceny pod pojem Enterprise Mobility Management. Je však zřejmé, že tento balík technologií a nástrojů se bude muset i do budoucna dále rozšiřovat, aby dokázal co nejlépe pojmout tuto stále se vyvíjející problematiku.

Kapitola 2

Základní pojmy

Pro správné pochopení problematiky BYOD, jejího působení ve firemním prostředí, způsobů jejího řízení a všech s tím souvisejících věcí, je třeba definovat základní pojmy. Tyto pojmy umožní čtenáři získat lepší orientaci v problematice a budou používány v dalších částech této práce.

2.1 Zaměstnanecká mobilita

Pro většinu běžných zaměstnanců v podstatě po celou dobu dvacátého století bylo nedílnou součástí jejich zaměstnání, že ráno vstali, vydali se ze svého domova na cestu do práce, tak aby v předem určeném čase byli na svém často pevně daném místě. Pracovních pozic, které by mohly fungovat nějak jinak, příliš velké množství nebylo. To je ovšem něco, co se v tomto století zásadně změnilo. Díky velkému pokroku v mobilních technologiích a službách poskytovaných přes Internet, už nejsou zaměstnanci nuceni být každý pracovní den přikováni ke svému psacímu stolu v budově svého zaměstnavatele. S využitím mobilních telefonů, počítačů a Internetu se jim otevírá více než kdy předtím cesta k teleworkingu, neboli práci a komunikaci online, práci přes Internet či práci na dálku. Zaměstnanci tak mohou ušetřit čas i stres spojený s cestováním, mohou pracovat z pohodlí svého domova, nebo třeba z míst, kde jsou právě v ten moment zapotřebí, jako třeba na schůzce se zákazníkem. S využitím videokonferencí a služeb na sdílení dat mohou dokonce na dálku spolupracovat s kolegy, kteří se mohou nacházet na mnoha různých místech po světě.[12]

Podle množství času, který zaměstnanec stráví prací mimo své stálé pracoviště, se dá teleworking rozdělit do tří kategorií[13]:

- **Příležitostný teleworking** – práce online na občasné služební cestě nebo pracovní dovolené. Práce nemusí být vykonávaná na počítači pracovníka, ale na pronajatém počítači např. v počítačové kavárně či hotelu. Příkladem může být firemní specializovaný IT odborník, který se z místa

své dovolené vzdáleně připojí na podnikový server, aby tak mohl vyřešit nečekaně nastalou krizi.

- **Částečný teleworking** – pravidelná práce online několik hodin až dnů v týdnu. Pracovníci mohou strávit část svého pracovního dne na vzdáleném místě a část v kanceláři. Do kategorie částečného teleworkingu lze řadit především obchodní zástupce, manažery na služebních cestách, ale třeba i studenty.
- **Plný teleworking** – pracovníci vykonávají práci trvale ze vzdáleného místa nebo se často přesunují mezi různými pracovišti. Může se jednat o pobočku firmy nebo o práci u dlouhodobého zákazníka. S centrálou firmy komunikují většinou online, fyzicky dojíždí do kanceláře pouze po předchozí dohodě. Tito zaměstnanci nemusí mít ve firmě trvale přiřazené pracovní místo. Tento styl práce mohou využívat například ženy na mateřské dovolené.

Pro podporu teleworkingu je v dnešní době možné využít velké množství různých nástrojů a služeb. Díky tomu je možné se vzdáleně domlouvat s kolegy či zákazníky, organizovat práci i podřízené nebo i společně tvořit. Zde je výčet těch nejběžnějších nástrojů, které lze využívat [13]:

- telefonování přes Internet – VoIP;
- telekonference / videokonference;
- chat – instant messaging;
- sdílení dokumentů online;
- sdílení pracovní plochy počítače;
- vzdálený přístup k počítači;
- online projektové řízení;
- online kalendáře a plánovače;
- firemní komunitní sítě, diskusní fóra a blogy;
- znalostní databáze ve stylu Wikipedie;
- online CRM (řízení vztahů se zákazníky);
- online fakturace;
- online marketing;
- online zálohování dat

Všechny tyto nástroje a možnosti jsou obvykle u zaměstnanců oblíbené, mohou zvyšovat jejich produktivitu i kvalitu práce. Pro podniky je ovšem nutné, aby měly vybudovanou správnou firemní infrastrukturu pro zaměstnaneckou mobilitu. Jinak může vzniknout řada nepříjemností a problémů, zatímco výhody se dostavit nemusí. Pro firmy je nutné, aby si uvědomily, že tato mobilita zasahuje prakticky do celého jejich fungování a dosavadní zaběhnuté procedury a pravidla už nemusí stačit. Zaměstnaneckou mobilitu je třeba zvažovat z hlediska práva, lidských zdrojů, bezpečnosti, identity a přístupu, podpory, obchodní infrastruktury a firemní politiky.[14]

2.2 Konzumerizace IT

S pojmem zaměstnanecká mobilita úzce souvisí i pojem Konzumerizace IT, tedy proces, kdy digitální zařízení a internetové služby původně určené pro běžné spotřebitele postupně pronikají do prostředí organizací a firem. Konzumeritace IT je hnána kupředu právě zaměstnanci těchto firem a organizací, kteří si kupují svá vlastní zařízení, přes své soukromé účty využívají online služby, sami si instalují různé aplikace na svá zařízení a pak tato zařízení připojují do podnikových sítí, často bez vědomí daných podniků.[15]

Zařízeními, která zaměstnanci nejčastěji přinášejí do své práce, jsou smartphony, tablety, notebooky či přenosná paměťová média. Ze služeb pak jde nejčastěji o online datová úložiště, webové e-mailové schránky a sociální služby jako Facebook či Twitter.[15]

Ačkoliv konzumerizace IT znamená pro podnikové IT značné komplikace, běžné zaměstnance to příliš netrápí. V dřívějších dobách mělo firemní IT oddělení vše celkem pevně v rukou a zaměstnanci neměli jinou možnost, než se přizpůsobit možnostem, které jim jejich IT oddělení poskytlo. Nyní si však zaměstnanci vytoužené služby a nástroje dokáží často zajistit sami. Obvykle se nezabývají tím, jestli nedostupnost žádané služby/zařízení nebyla třeba dána zákazem z bezpečnostních důvodů. IT oddělení tím pak ztrácí přehled o tom, jaké nástroje zaměstnanci využívají a není pak ani schopno garantovat bezpečnost firemní sítě. Konzumerizace IT je tak silným fenoménem, že si řada společností už uvědomila, že než aby proti tomu bojovaly, bude pro ně jednodušší a zároveň i užitečnější, když to začnou podporovat. Mohou z toho totiž pro sebe získat vyšší produktivitu zaměstnanců, větší flexibilitu a případně i finanční úspory (více viz kapitola 3). Proto dnes mnohé firmy zavádí BYOD politiky, kterými zaměstnancům umožňují využívat v práci jejich mobilní zařízení a to takovým způsobem, aby svým IT oddělením vrátili kontrolu nad situací.[15]

2.3 BYOD

Podle glosáře společnosti Gartner je BYOD *„alternativní strategií umožňující zaměstnancům, obchodním partnerům a dalším uživatelům používat jejich soukromně vlastněná zařízení ke spouštění podnikových aplikací a přístupu k podnikovým datům. Obvykle to zahrnuje smartphony a tablety, ale je možné do toho zahrnout i osobní počítače. Součástí strategie můžou být i firemní dotace na zaměstnanecká zařízení.“*[2][16]

Tato zkratka pro anglické sousloví Bring Your Own Device (česky: Přines si své zařízení) se používá jak pro označení situací, kdy má firma jasně definovaná pravidla jak nakládat se soukromými zařízeními, tak i pro situace, kdy firma jejich používání nijak neupravuje a jen je toleruje, či o jejich přítomnosti a užívání nemá vůbec povědomí.

Mezi zaměstnanci je typicky velká touha používat v práci svá vlastní zařízení, což bývá vyvoláváno například tím, že IT oddělením poskytované pracovní nástroje neodpovídají očekáváním zaměstnanců.[17] Nejdříve se používání vlastních zařízení může objevovat hlavně u manažerů a zaměstnanců IT oddělení, kteří mohou v rámci firemních pravidel fungovat na bázi jednorázových výjimek. Jakmile se ale počet používaných zařízení začne zvyšovat, začnou se výrazně projevovat i všechny jevy s tím související, což obvykle zasáhne fungování celé firmy.[18] Tyto jevy se určitě neomezují jen na firemní IT oddělení, zabývat se jimi musí například právní oddělení, lidské zdroje a řada dalších. Nejpalčivějším problémem bývají obvykle otázky bezpečnosti. Ty budou, společně s dalšími projevy BYODu podrobněji rozepsány v kapitole 4.

2.3.1 BYO*

Kromě termínu BYOD je možné občas narazit i na jeho různé varianty. Ty často označují určitou specifičtější část tohoto tématu. V zásadě každý, kdo chce mluvit o nějaké specifičtější části problematiky BYOD si může vymyslet vlastní variantu této zkratky. Je možné narazit i na varianty této zkratky, které už nesouvisejí s oblastí firemního IT, ale mají více „lidový význam“. Zde jsou příklady některých zkratek:

- BYOPC – Bring Your Own PC – přines si svůj vlastní osobní počítač.
- BYOL – Bring Your Own Laptop – přines si svůj vlastní laptop/notebook.
- BYOL – Bring Your Own Licence – zajisti si svou vlastní licenci (k nějaké aplikaci či službě).
- BYOC – Bring Your Own Computer – přines si svůj vlastní počítač.
- BYOC – Bring Your Own Cloud – zajisti si svou vlastní cloudovou službu.

[2] Přeloženo autorem ze zdroje: [16].

- BYOA – Bring Your Own Apps – přines si své vlastní aplikace.
- BYOT – Bring Your Own Technology – přines si svou vlastní technologii.
- BYOS – Bring Your Own Software – přines si svůj vlastní software.
- BYOS – Bring Your Own Support – zajisti si svou vlastní podporu.
- BYOB – *Bring Your Own Beer – přines si své vlastní pivo.*

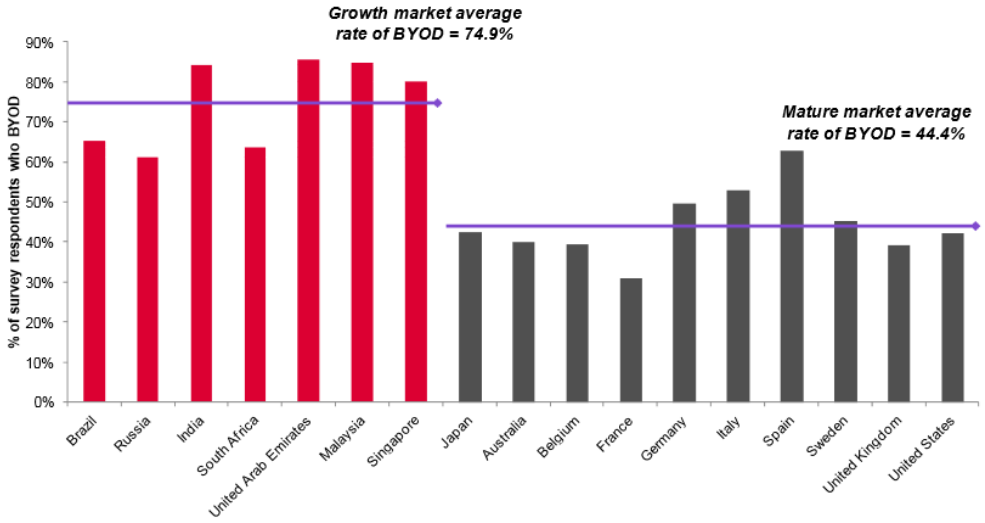
Další variantou této zkratky je CYOD, což znamená Choose Your Own Device, tedy Vyber si své zařízení. Jedná se o přístup, kdy společnost umožní zaměstnanci vybrat si zařízení z omezenější nabídky, kterou firma předtím schválila. Firma tak má možnost vybrat jen ta zařízení, která budou umožňovat dostatečnou míru kontroly a zabezpečení.[19]

2.3.2 Situace ve světě

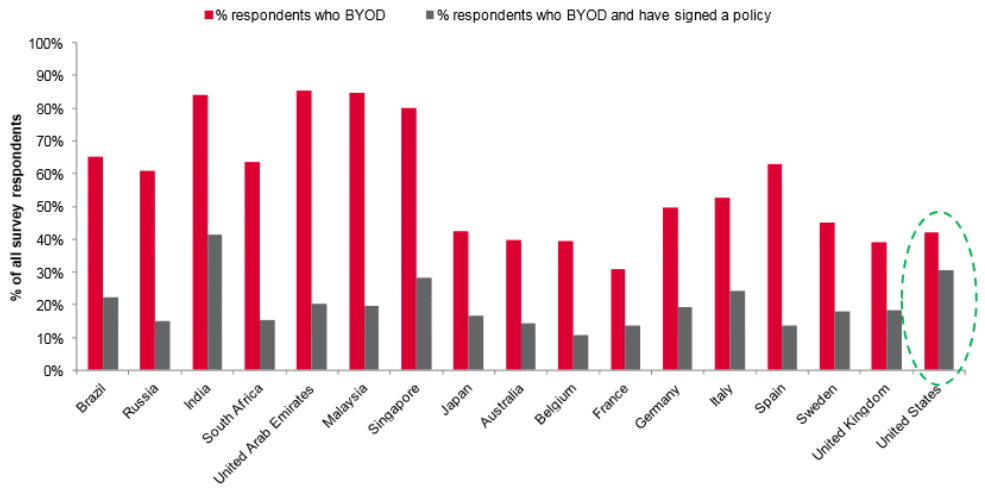
Postoje jak firem, tak i zaměstnanců k užívání vlastních zařízení pro pracovní účely se v různých částech světa liší. Analytická společnost Ovum provedla v roce 2012 průzkum mezi 3 796 respondenty ze 17 zemích světa, ze kterého vyplynulo, že možnost využívat k práci vlastní zařízení se jeví jako atraktivní pro 74,9 % zaměstnanců v rozvojových zemích, ale v rozvinutých zemích to je už jen 44,4 % zaměstnanců (viz obrázek 3.1).

Ve vyspělých zemích bylo dlouhou dobu zavedeným pravidlem, že firmy nakupovaly firemní notebooky, telefony, atd. a následně je distribuovaly mezi své zaměstnance. Firmy tomuto fungování byly přizpůsobeny technologicky i organizačně. Rozvíjející se země oproti tomu často nejsou schopny nabídnout svým zaměstnancům např. firemní telefon a jsou proto rády, když zaměstnanec začne využívat vlastní, soukromě koupené zařízení. Zaměstnanci z rozvojových zemí mývají také jiný přístup k práci. Jsou daleko ochotnější upřednostňovat zaměstnání před osobním životem a věnovat se pracovním úkolům i mimo pracovní dobu, než jak je to ve vyspělých zemích, kde si lidé drží práci a osobní život více oddělené. Postoj zaměstnanců k BYODu je však ovlivněn i otázkami ochrany soukromí a osobních údajů. Zejména pro evropské zaměstnance je toto téma velmi důležité, což je dáno historickými zkušenostmi. Lidé v rozvojových zemích toto téma tolik neřeší a nebo považují za marné se tím zabývat z přesvědčení, že jejich vlády a zaměstnavatelé si o nich jakékoliv informace tak jako tak zjistí.[20]

BYOD se světem šíří nezadržitelným tempem. Ač v různých regionech různě rychle, vždy je tlačen kupředu zaměstnanci a jejich touhou využívat oblíbená zařízení, na která jsou zvyklí k tomu, aby si usnadnili své pracovní úkony. Už dnes je BYOD součástí mnoha firem aniž o tom ty firmy třeba vůbec vědí. Zaměstnanci mají tendenci využívat svá mobilní zařízení jak ve firmách, které jejich používání neupravují, tak i v těch, které je přímo zakazují. Mnoho podniků si již uvědomila, že snaha blokovat BYOD je tak trochu jako boj



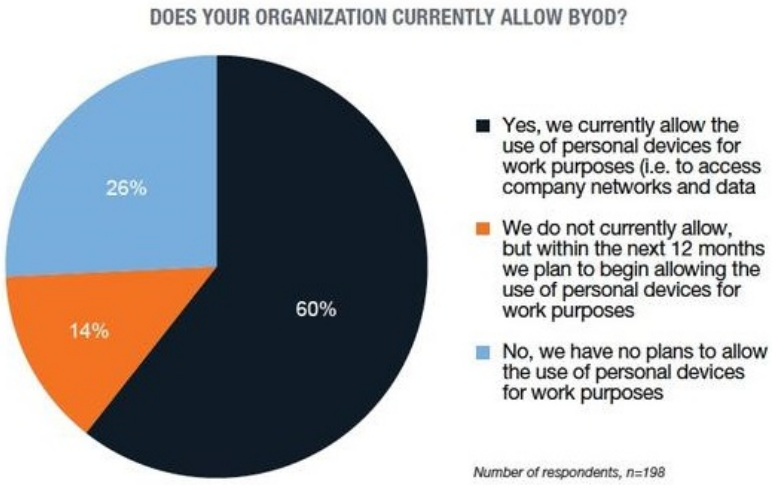
Obrázek 2.1: Rozdíl mezi průměrnou mírou adoptování BYODu v rozvojových zemích oproti vyspělým zemím.[20]



Obrázek 2.2: Nedostatek řízení BYODu ve firmách je celosvětový problém.[20]

s větrnými mlýny a zavedení pro jejich firmu vhodné BYOD politiky považují za důležité téma. V této oblasti je ovšem ještě potřeba dosáhnout většího pokroku, statistiky z roku 2012 ukazují, že průměrně jen 20 % zaměstnanců využívající BYOD, tak jednalo pod dohledem firemní BYOD politiky (viz obrázek 3.1).[20]

Údaje získané z výzkumu provedeného v listopadu 2014 říkají, že 74 % organizací již povolilo svým zaměstnancům využívání BYODu ve svém prostředí nebo se k tomu v dohledné době chystá. Jen přibližně čtvrtina firem

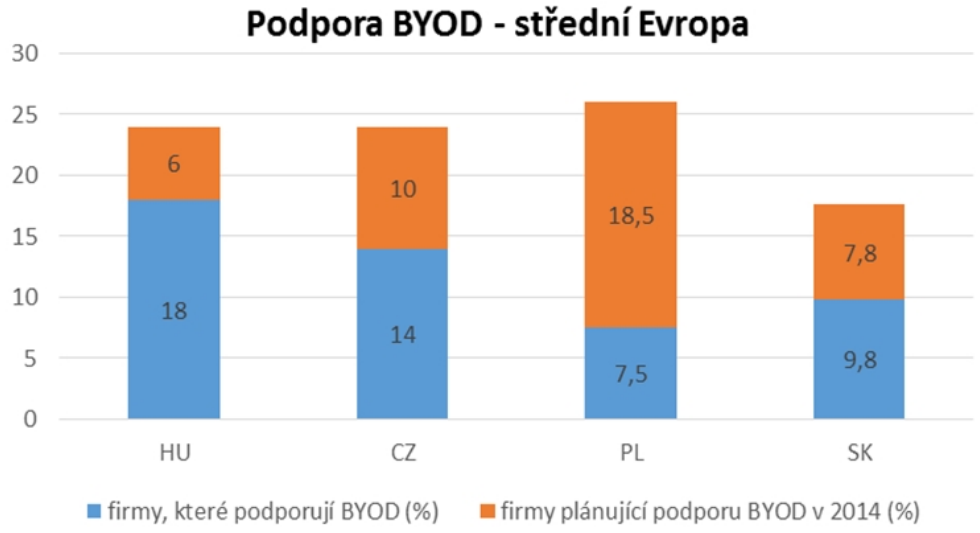


Obrázek 2.3: Jak se firmy staví k možnosti povolit ve svém prostředí BYOD.[22]

nemá vůbec v plánu BYOD povolit (viz obrázek 2.3). Výzkum také zjistil, že BYOD častěji povolují malé firmy (71 % již povolilo, 4 % plánují). Nejčastěji BYOD povolují technologické firmy a vzdělávací instituce.[21]

2.3.3 Situace v ČR

Nové IT trendy a postupy rozvíjející se nejvíce ve Spojených státech amerických se do Evropy a tedy i do Česka obvykle dostávají s několikaletým zpožděním. Chytrá mobilní zařízení určená pro běžné zákazníky se však šíří daleko rychleji. Je tedy potřeba s řešením problematiky BYODu neotálet, protože již nyní se projevuje i u nás. V roce 2013 vyšlo z výzkumu provedeném ve střední Evropě společností Intel, že jen 14 % českých firem BYOD podporuje a 10 % jich plánuje nasadit BYOD politiku do 12 měsíců (viz obrázek 2.4). Většina českých firem se stále příliš obává rizik a komplikací, které by to mohlo přinést a zřejmě ani nemají příliš velkou představu o tom, jaká pozitiva by jim to mohlo nabídnout.[23] To ostatně koresponduje s faktem, že na toto téma je v českém jazyce dostupné zatím jen málo informací a statistik.



Obrázek 2.4: Podpora BYODu ve firmách střední Evropy.[23]

Kapitola 3

Výhody a přínosy podporování BYODu

Mnoho zaměstnavatelů se tímto tématem začne zabývat až teprve v momentě, kdy jsou k tomu donuceni skutečností, že se jim BYOD proplížil do podniku. Na BYOD ale není nutné čekat. Naopak může být vhodné mu vyjít vstříc, podporovat ho a maximálně se snažit využít potenciál, který nabízí ke zlepšení výkonu firmy. Správně a pečlivě zavedená BYOD politika umožňující zaměstnancům využívat jejich vlastní mobilní zařízení může mít velký dopad na produktivitu a spokojenost zaměstnanců, díky čemuž se mohou podniku zvýšit zisky. Také bývá určitá příležitost ušetřit na výdajích, ale především bude mít firma větší kontrolu nad stále probíhající konzumerizací IT a bude tak připravena čelit potížím, které to může způsobit. Výhody a příležitosti, které přicházejí s BYODem jsou samozřejmě vyvažovány i řadou potíží a nutných změn, na něž ovšem existují řešení. Tyto potíže i jejich možná řešení budou zmíněna v kapitole 4. V této části budou popsány především důvody, proč by firma měla mít zájem na podpoře BYODu.

3.1 Vyšší produktivita a spokojenost zaměstnanců

Lepší výkony zaměstnanců při firemní podpoře BYODu mohou plynout v zásadě ze dvou složek – znalost zařízení a mobilita zaměstnance:

- **Znalost zařízení** – Vlastní zařízení, které zaměstnanec používá, si obvykle vybral sám podle svých vlastních kritérií, tak aby mu co nejvíce vyhovovalo. Dnešní spotřebitelská mobilní zařízení poskytují uživatelům spousty důvodů, proč by je měli sami chtít využívat, díky čemuž získávají lepší zkušenosti s ovládáním těchto zařízení a zároveň tím objevují i nové možnosti užití. A to vše dělají z vlastní vůle a radosti. Oproti tomu zařízení, která zaměstnancům poskytne jejich zaměstnavatel často neodpovídají požadavkům a tužbám svých přiřazených uživatelů. Zaměstnanci

tak nemají příliš pozitivní motivace, učit se s daným zařízením a objevovat jeho nové možnosti, a když to už dělají, tak spíše z nutnosti. Na svá vlastní soukromá zařízení jsou zaměstnanci zvyklí a je pro ně tedy jednodušší, rychlejší a i příjemnější využívat je i k pracovním činnostem.

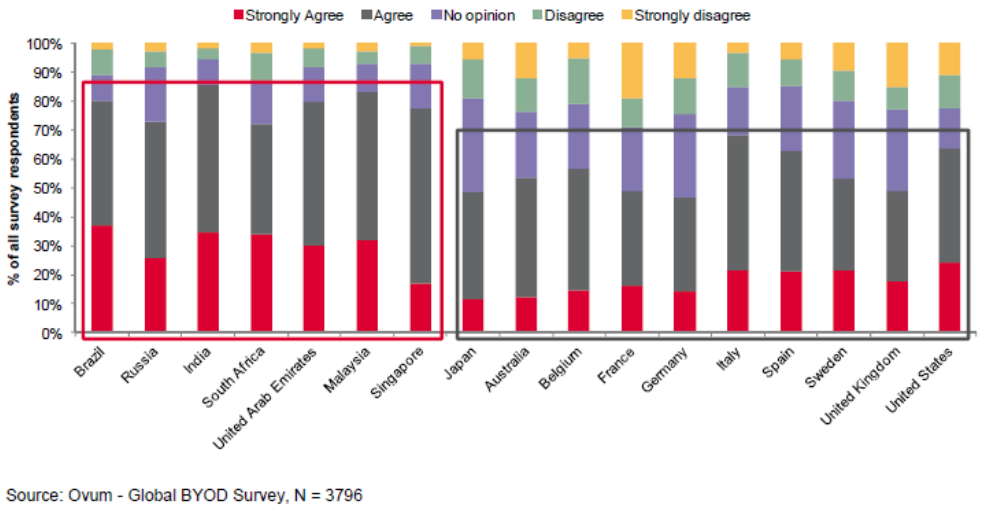
- **Mobilita zaměstnance** – Mohou-li zaměstnanci využívat vlastní zařízení i pro pracovní účely, často tak dělají i nad rámec pracovní doby. Typickým příkladem je psaní a odpovídání na pracovní e-maily po večerech či ráno před odchodem do práce nebo třeba čtení firemních dokumentů a zapisování si k nim poznámek, které pak zaměstnanec po příchodu do práce může hned zpracovat. Každý zaměstnanec, jehož zařízení je zapojené do firemního BYOD programu také může zůstávat v kontaktu se svými kolegy bez ohledu na to, kde se zrovna nachází a také může zužitkovat čas strávený například cestou vlakem k tomu, aby dohnal nějaké resty, či se připravil na nadcházející schůzku.

3.2 Produktivita

Společnost Intel uvedla, že její zaměstnanci využívající k práci svá soukromá zařízení v rámci jejich BYOD programu zvýšili svou produktivitu v roce 2011 o téměř hodinu denně.[24] Podle zprávy *Evolving Workforce Research* téměř 60 % zaměstnanců prohlašuje, že jejich práce by pro ně byla příjemnější, kdyby mohli mít vliv na to, jaké technologie jim budou pro práci k dispozici a stejné množství zaměstnanců se domnívá, že by tím dokázali zvýšit svou produktivitu.[25] A podle zjištění společnosti Ovum (viz graf 3.1) přibližně 55 % zaměstnanců v rozvinutých státech a 79 % zaměstnanců v rozvíjejících se oblastech oceňuje možnost přistupovat k firemní elektronické korespondenci a k dalším podnikovým zdrojům i mimo svou pracovní dobu.[20]

V roce 2013 byla vydána studie nazvaná *The Total Economic Impact of IBM Managed Mobility for BYOD*, kterou pro IBM vypracovala analytická společnost Forrester. Cílem studie bylo prozkoumat celkový ekonomický dopad a potenciální návratnost investic, kterých mohou dosáhnout firmy, jež se rozhodnou využít mobilní řešení od IBM pro realizaci svého BYOD programu. Studie vycházela z údajů získaných od dvou zákazníků společnosti IBM. Jedním je velká evropská banka nabízející retailové, privátní a komerční bankovnictví klientům; zaměstnávající více než 25 000 zaměstnanců a spravující aktiva v hodnotě 150 miliard dolarů. Druhým je americká přepravní společnost s více než 30 000 zaměstnanci. Pro tvorbu finančního modelu v této studii byly využity informace jen od prvního zákazníka a to z důvodu, že druhý zmíněný byl v době tvorby této studie teprve v pilotní fázi zavádění svého BYOD programu.[26]

Z rozhovorů s těmito zákazníky vyplynulo, že zavedení BYOD programu s pomocí IBM vedlo k návratnosti investice měřeno ukazatelem ROI ve výši 108 % a době splatnosti dokonce menší než jeden měsíc. Zaměstnanecká pro-

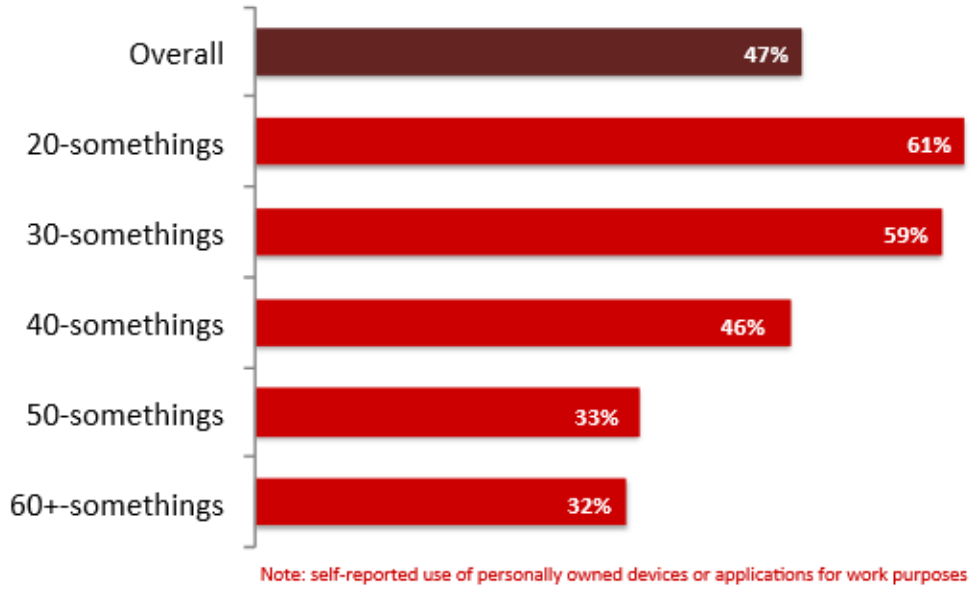


Obrázek 3.1: Jak moc oceňují zaměstnanci možnost přistupovat k firemnímu e-mailu a dalším firemním aplikacím i mimo pracovní dobu.[20]

duktivita se zvýšila o 45-60 minut na zaměstnance za týden. Z údajů za tři roky běhu programu bylo také zjištěno, že toto číslo pomalu klesá v důsledku toho, jak se program rozšiřuje i mezi zaměstnance, jež výhody BYOD programu tolik nevyužijí. To ostatně odpovídalo i původnímu očekávání. Z vyhodnocování také vyšlo, že ze všech zařízení, která se do programu zapojila je minimálně 90 % z nich pravidelně využíváno k pracovním záležitostem.[26]

Část tabletů zapojených do BYOD programu je využívána obchodníky, kteří za pomoci pro ně nově vyvinutých aplikací, jsou schopni provádět daleko rychleji obchodní transakce a mají i lepší možnosti prezentovat klientům nabízené bankovní produkty a to v nejaktuálnější podobě. Došlo tím ke zvýšení ročních příjmů o 7 500 až 11 500 dolarů na obchodníka užívajícího tablet, což jen v prvním roce běhu BYOD programu znamenalo zvýšení příjmů o 1 687 500 dolarů.[26]

Z rozsáhle studie pro společnost Panasonic provedené v druhé polovině roku 2014 ohledně užívání tabletů ve firmách nad 50 zaměstnanců vyšlo, že 70 % zaměstnavatelů hlásí podstatné zvýšení produktivity. Zaměstnavatelé i jejich zaměstnanci se v celkovém průměru shodli, že se produktivita zvýšila o cirka 30 %. Server BusinessWorld.cz, citující z této studie uvádí: *„Výrobní odvětví se ukázalo jako odvětví, získávající ze zavedení tabletů nejvíc. 77 % nákupčích v tomto odvětví hlásí zvýšení produktivity. Z oblasti telekomunikačních společností a společností veřejných služeb hlásí zvýšení produktivity 74 % dotázaných, 72 % v maloobchodě a velkoobchodě a 71 % ve finančních službách.“*[27]



Obrázek 3.2: Kolik procent zaměstnanců z různých věkových skupin užívá své soukromé zařízení nebo aplikaci pro pracovní účely.[29]

3.3 Spokojenost

V řadě případů je pro firmu důležitým faktorem i spokojenost zaměstnanců. Ta může jednak zvyšovat produktivitu, dále ale také může zvýšit loajalitu zaměstnance. To je důležité hlavně pro firmy opírající se o velké množství zaměstnanců s odbornými znalostmi. Odchod takového odborníka může pro firmu znamenat někdy i opravdu velkou ztrátu. Zejména pokud si sebou odnese i své know-how a nabídne ho nějakému novému zaměstnavateli.

Z grafu 3.1 je vidět, že tu je nezanedbatelné množství zaměstnanců, kteří o výhody BYODu stojí. Týká se to nejvíce mladších zaměstnanců ve věku 20-30 let (viz graf 3.2), kteří s chytrými telefony, notebooky a Internetovými službami vyrůstali a jsou zvyklí je naplno využívat.[28]

Je nutné zmínit, že podpora BYODu může být pro podniky také konkurenční výhodou v oblasti náboru nových zaměstnanců, zejména dnešních dvacátníků a třicátníků. Především v oblasti IT, kde je dlouhodobě nedostatek kvalifikovaných zaměstnanců, může být firemní BYOD program významným plusem ke zvýšení atraktivity pro případné zaměstnance. A jelikož se všemožná mobilní zařízení vyvíjejí stále dál a pronikají stále více do životů běžných lidí, bude zřejmě každá další generace na jejich přítomnost ještě více zvyklá a možnost jejich využití v práci pro ně bude stále významnější.[28]

3.4 Finanční úspory

Finanční úspory bývají často jednou z prvních výhod, nad kterými firmy zvažující zavedení podpory BYODu, začínají uvažovat. Skutečně je řada věcí, u kterých se dá zavedením BYOD programu, dosáhnout úspor. Firmy podporující zaměstnance, aby užívali svá zařízení, mohou ušetřit na financování firemních telefonů, notebooků a třeba i dalších podobných zařízeních, které by jinak musely zajišťovat a obhospodařovat ze svého rozpočtu.

3.4.1 Náklady na firemní HW

Ne všichni zaměstnanci začnou používat svá zařízení, ale čím víc bude firemní BYOD program uživatelsky příznivý, tím více zaměstnanců se do něj zapojí. Firmy tak mohou snížit vlastní výdaje za nákup a pravidelnou obnovu firemních notebooků, smartphonů, atp. Firmám navíc mohou odpadnout náklady za údržbu a opravy. Minimálně z části totiž tato starost přejde na zaměstnance a podniky jež jejich soukromým zařízením poskytují zákaznický servis. Studie *The Total Economic Impact of IBM Managed Mobility for BYOD* uvádí, že zkoumaná banka mimo jiné, dosáhla snížení počtu IT zaměstnanců potřebných pro údržbu firemní mobilní infrastruktury z pěti na dva a ušetřila ročně 1,5 milionů $ na placení licencí a služeb.[26]

3.4.2 Telefonní a datové služby

Řada firem ve světě se také snaží ušetřit na placení účtů za telefonní a datové služby, tím, že zaměstnanci užívající vlastní zařízení v práci, si také sami platí všechny běžné účty. Z ekonomické analýzy společnosti Cisco vyplývá, že zaměstnance obvykle příliš netrápí, že výdaje na jejich mobilní zařízení a související služby, které využívají i k práci, si hradí sami. Na dotaz jaká opatření by zvýšila jejich BYOD produktivitu, jen 20 % odpovědělo, že by to byly příspěvky zaměstnavatele na jejich BYOD zařízení. Zaměstnanci jsou tedy ochotni sami si platit zařízení a služby, u kterých věří, že jim zjednoduší jejich práci.[30]

Ačkoliv jsou zaměstnanci často ochotní sami si financovat svá BYOD zařízení, podniky nemají vždy a všude tu možnost přesunout tyto náklady na zaměstnance. V České Republice, z rozsudku Nejvyššího správního soudu 5 Afs 68/2007–121 z 28. 2. 2008 [3] vyplývá, že zaměstnavatelé mají povinnost platit svým zaměstnancům poměrnou část nákladů na užívání jejich soukromého zařízení k pracovním účelům. Je tedy třeba brát v úvahu zákony dané země, tuto otázku probrat se zaměstnancem a uzavřít s ním dohodu, která bude tyto příspěvky a náhrady upravovat.

[3] Dostupné z: http://www.ucetni-portal.cz/soubory/judikatura/633.pdf

3.4.3 Nový help-desk

Dalším zdrojem možných úspor je firemní help-desk. Zaměstnanci zapojení ve firemním BYOD programu jsou často schopni řešit potíže na vlastním zařízení svépomocí. Ostatně řada z nich to tak dělá i v soukromí, že hledají řešení problému se svým smartphonem po Internetu a ptají se na různých diskusních fórech. Podniky mohou nabídnout svým zaměstnancům alternativní způsoby podpory, jako jsou třeba právě diskusní fóra, na jejichž chodu se budou podílet i sami zaměstnanci svými radami ostatním kolegům. Navíc má-li zaměstnanec problém, jež byl na fóru řešen už v minulosti někým jiným, může si tak onen zaměstnanec toto řešení dohledat a není tedy ani potřeba, aby specialista IT podpory, či jiný kolega na daný problém znova odpovídali. Takovéto nové přístupy k podpoře zaměstnaneckých zařízení pak mají šanci vyjít levněji než klasický help-desk.[31]

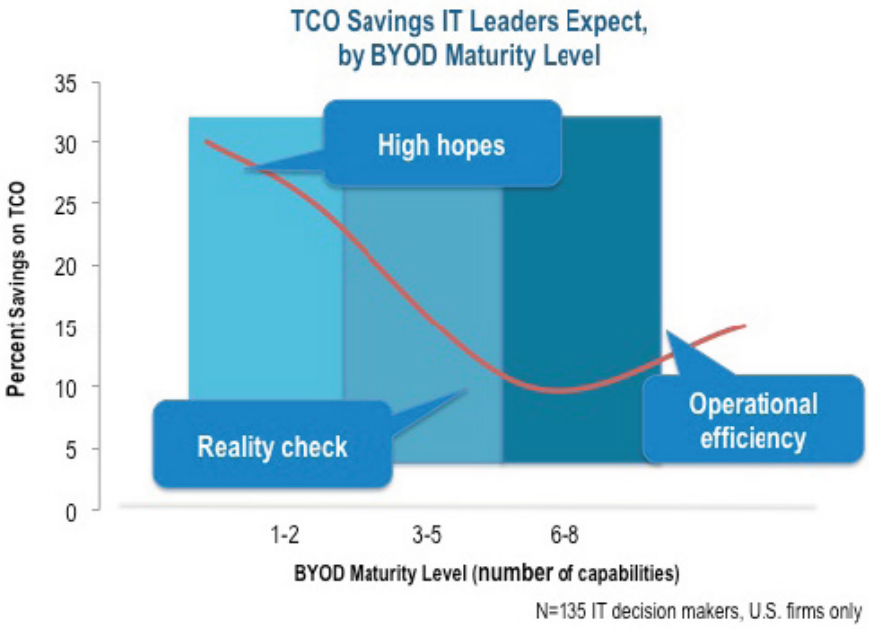
Navíc změna přístupu k poskytování IT podpory může vést i k tomu, že zaměstnanci podnikové IT podpory nebudou pouze zabraňovat snižování produktivity v případě nějakých poruch zařízení, ale mohou se přímo podílet na zvyšování zaměstnanecké produktivity. A to například tím, že na firemním diskusním fóru budou zveřejňovat rady a tipy jak lépe využívat zaměstnanecká zařízení a aplikace. Do toho se mohou zapojit i sami zaměstnanci a sdílet tak své zkušenosti nebo se také mohou přímo ptát firemních IT specialistů na to, co je v těchto souvislostech zajímá. Vznikne tak obousměrná komunikace mezi podnikovými IT specialisty a ostatními spolupracovníky, z čehož může firma získat jak užitečnou zpětnou vazbu, tak i třeba nové nápady na to jak by se co dalo vylepšit.[31]

3.4.4 Na úspory nemusí vždy dojít

Ačkoliv byla výše zmíněna řada věcí, na kterých se dá skutečně ušetřit, konečný výsledek z hlediska úspor může být všelijaký. Předně, určitá část nákladů se pouze přesune, jelikož kromě povolení BYODu je také potřeba zavést i nástroje na jeho správu a zabezpečení. Viceprezident společnosti Forrester Ted Schadler prohlásil, že celková cena BYODu je vyšší, než kdyby podporován nebyl.[32] Toto varovné tvrzení však neplatí vždy a bylo vyřčeno nejspíš proto, aby firmy zůstaly se svými očekáváními pevně nohama na zemi.

Například společnost Cisco dosáhla zavedením svého BYOD programu úspor na firemní podpoře o 25 %.[33] A i výše zmíněná studie o ekonomickém dopadu zavedení BYOD programu od IBM uvádí v případě daného zákazníka, že úspor bylo dosaženo i v situaci, kdy banka svým zaměstnancům přispívala měsíčně 85 $ na jejich účty za mobilní služby.[26]

Zavádění BYOD programu sebou přináší velké množství změn a dotkne se mnoha oblastí podniku. Je to tedy výzva, která aby přinesla výhody, musí být důkladně zvážena a připravena. Jak ukazuje graf 3.3 společnosti Cisco, firmy často při zavádění BYODu procházejí třemi různými fázemi očekávání



Obrázek 3.3: Očekávání celkových nákladů na firemní BYOD.[30]

celkových finančních úspor. Nejdřív mají příliš vysoká očekávání, v druhé fázi přichází určité vystřízlivění a nakonec, po vypořádání se s počátečními potížemi a vyladění systému teprve vidí skutečné úspory, které jim to přineslo či nepřineslo.

3.5 Shrnutí

Určit skutečné náklady na podporu BYODu je velmi obtížné a neexistuje na to jednotný postup. Je to dáno jednak specifickými vlastnostmi každé firmy a jejími prioritami při zavádění BYODu a dále důsledností a pečlivostí s jakou firma implementuje všechny potřebné systémy a firemní pravidla. Firmy jako Cisco či IBM dokazují, že dosáhnout úspor lze. Je však i řada firem, jimž zavedení BYODu náklady nesnížilo, ale třeba i naopak zvýšilo.[34] Celkově se ale i tak může zavedení BYODu stále vyplatit a to díky vyšší produktivitě, která tak může zvýšené náklady vyvážit většími zisky.

Z toho, že Intel uvádí zvýšení produktivity o hodinu denně zatím co IBM uvádí zvýšení produktivity o hodinu za týden je opět vidět, že i u produktivity je těžké zobecnit, jak velkých zvýšení se obvykle dosahuje. Je to opět dáno specifiky firmy a důsledností s jakou firma vytvořila svůj BYOD program. Statistiky se ale shodují v tom, že ke znatelnému zvýšení produktivity u těch, kteří se rozhodli BYOD zavést, skutečně dochází.

Kapitola 4

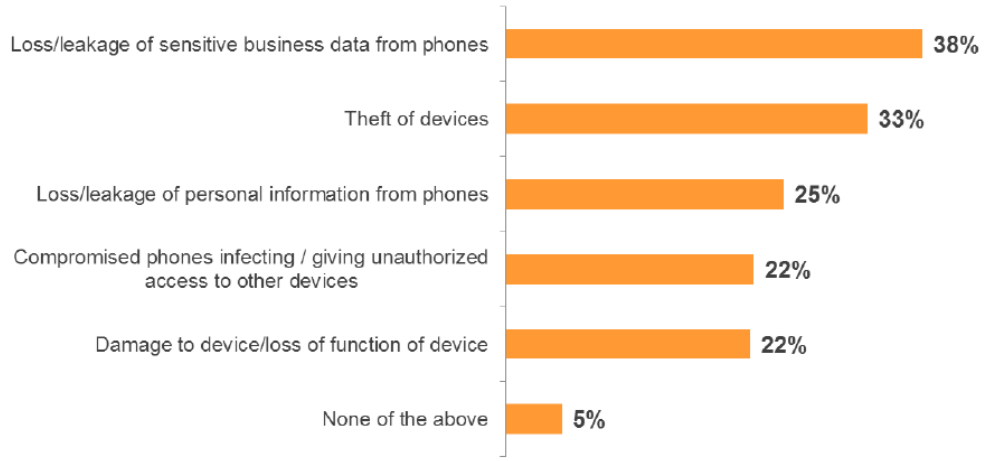
Výzvy, rizika a způsoby jejich řešení

Jak bylo již několikrát zmíněno v předchozích kapitolách, BYOD sebou přináší širokou škálu různých rizik a výzev. Tyto výzvy a rizika mohou zasáhnout jak společnosti, které hodlají BYOD mezi svými zaměstnanci podporovat, tak i společnosti, které BYOD ignorují, nebo i ty, které BYOD odmítají, ale nepřizpůsobily svá firemní pravidla současné podobě situace. V této kapitole budou stručně popsány výzvy i rizika BYODu, které považuji za významné a budou k nim uvedena jejich možná řešení. Pro přehlednost jsem, po prostudování souvisejících materiálů, vytvořil čtyři kategorie, do kterých jsem obsah této kapitoly rozdělil. Jsou to kategorie Bezpečnost, Technické zajištění, Legislativa&Politika a Zaměstnanci. V této kapitole vycházím jak ze zdrojů: [35], [36], [37], [38], [39], [40], [41], [42], [43], tak i z vlastních úvah.

4.1 Bezpečnost

Ochrana podnikových dat, ať už finančních, provozních, zákaznických či jiných, je pro každou firmu z pochopitelných důvodů zásadní téma, které musí řešit tak jako tak, nehledě na BYOD. Případný bezpečnostní incident, vedoucí ke ztrátě či úniku informací, může znamenat citelnou finanční újmu i poškození reputace v očích současných i možných budoucích zákazníků. BYOD sebou přináší řadu nových rizik pro informační bezpečnost, ale vrací na stůl i řadu věcí, jejichž dosavadní řešení se nyní stává nedostatečné či nepoužitelné. Například přístup k administrátorským právům u firemních notebooků může být omezen jen na zaměstnance IT oddělení, ale patří-li notebook přímo zaměstnanci, už na něj nelze aplikovat stejné restrikce.

Zavádění nových bezpečnostních opatření a pravidel i instalace potřebné infrastruktury může být nákladná, ale případné náklady na řešení bezpečnostních incidentů mohou být ve výsledku ještě dražší. Při rozhodování o tom,



Obrázek 4.1: Nejčastější hrozby na mobilních telefonech.[44]

jak se v rámci firmy postavit k otázce BYODu, je třeba zvážit dopady na bezpečnost informací a to jak v případě, že se společnost rozhodne BYOD podporovat, tak i v případě, že se k němu bude stavět odmítavě. Jak bylo uvedeno v předchozích kapitolách, zaměstnanci mají tendenci využívat svá soukromá zařízení na práci s firemními daty i v situaci, že žádná oficiální podpora BYODu u nich v práci neexistuje. Na rizika doprovázející BYOD tedy může dojít i u podniků, jež se tímto zatím nezabývaly a nepřizpůsobily tedy svá bezpečnostní pravidla stále probíhající konzumerizaci IT. Ať už se však daná společnost rozhodne BYOD podporovat či nakonec dospěje k rozhodnutí ho blokovat, je to v každém případě příležitost zrevidovat a aktualizovat firemní bezpečnostní pravidla tak, aby odpovídaly současným potřebám.

Průzkum společnosti Kaspersky Lab z roku 2013 provedený ve 24 zemích světa ukázal, že 91 % zkoumaných organizací zaznamenalo za posledních 12 měsíců alespoň jeden útok na jejich IT infrastrukturu vedený z vnějšku. Nejčastěji se jednalo o malware, spam, phishing, network intrusion a krádež mobilního zařízení. Pokud jde o bezpečnostní incidenty týkající se konkrétně mobilních zařízení, které byly v tomto průzkumu zkoumány jako samostatná kategorie, uvedlo 95 % dotazovaných organizací, že zaznamenali aspoň jeden takový případ v posledním roce. Z toho v 38 % šlo o únik důležitých dat (viz graf 4.1).[44]

4.1.1 End Node Problem

Pojmem *End Node*, tedy *koncový uzel* se rozumí periferní hardwarová jednotka v síti jako třeba stolní počítač, notebook, smartphone apod. Pro označení situace, kdy se takovýto koncový uzel připojuje do zabezpečené (např. firemní) sítě, ale sám neodpovídá požadovaným bezpečnostním standardům, se používá

anglický pojem *End Node Problem* (česky se dá přeložit jako *problém koncového uzlu*). Zranitelnost dané sítě může vzniknout, je-li připojovaný koncový uzel špatně nakonfigurovaný, má neaktualizovaný SW, špatnou antivirovou ochranu, či jiné nedostatky vytvářející riziko, že dojde k narušení zabezpečení sítě. Prostřednictvím nedostatečně zabezpečeného koncového uzlu může být firemní síť infikována viry či malwarem nebo může být třeba vystavena cílenému útoku z vnějšku. Pro IT odborníky zajišťující bezpečnost sítě bývá koncový uzel často tím nejslabším článkem z celého řetězu, který musí řešit.[45]

4.1.2 Škodlivý software

Škodlivý SW, běžně známý jako malware, je druh softwaru, který je vytvořený se záměrem způsobit nějakou újmu infikovanému počítačovému systému nebo jeho uživateli. Do kategorie malware se řadí počítačové červy, viry, trojské koně, spyware, adware a rootkity, atd. Takovýto SW může na zasaženém počítači mazat či šifrovat data, instalovat další nevyžádaný SW nebo třeba poškozovat funkčnost OS. Může se ale také chovat naopak zcela nenápadně, tak aby uživatel neměl vůbec tušení, že je něco špatně. Takto nenápadně pak může docházet k odesílání uživatelových souborů přes Internet na cizí počítač. Může být zaznamenáván internetový provoz na zasaženém počítači včetně zadávaných hesel, čísel kreditních karet atp. Škodlivý SW může ale také zneužít zranitelnost OS, k tomu, aby poskytl útočníkovi administrátorská práva na zasaženém zařízení a možnost ho ovládat.[46]

Malware se neomezuje jen na stolní počítače či notebooky. V podstatě jakékoliv inteligentní zařízení by mohlo být infikováno. V dnešní době je malware velmi rozšířený i na mobilních zařízeních jako jsou smartphony či tablety, přičemž nejčastěji vzniká malware pro zařízení běžící na některé z mnoha různých verzí platformy Android.[47]

Řešení:

- Antivirové programy zajišťují detekci a odstranění počítačových virů. Pro úplnou ochranu je ale třeba zajistit si produkt poskytující komplexní antimalwarovou ochranu ve kterém budou krom antivirového řešení i nástroje na ochranu před phishingem či spywarem.

- Kromě antimalwarových programů na klasické počítače dnes existují i podobné programy určené pro mobilní zařízení.

- Jako první (nikoli však poslední) obrannou linii je vhodné použít firewall. Ten hlídá datový provoz z i do výpočetního zařízení a blokuje podezřelé či zakázané datové služby. Firewally existují jako samostatné programy, ale často bývají i součástí komplexních antivirových programů.

- Mimo firewallů na počítače a smartphony je možnost mít firewall i jako součást datové sítě. Firewall může být totiž i součástí routeru, díky čemuž pak mohou organizace získat lepší možnosti jak kontrolovat datový provoz v jejich síti a blokovat tak nebezpečný datový provoz i ten, o němž bylo rozhodnuto, že nebude v síti povolen.

- Je také třeba zajistit, aby byla používána vždy ta nejaktuálnější verze OS a dalších programů. Pomocí technologie OTA (over-the-air) je možné bezdrátově zajistit pro mobilní zařízení automatické stahování a instalování jak aktualizací, tak i nového SW. Tato technologie může být součástí většího balíčku softwarových nástrojů určených ke správě mobilních zařízení.

4.1.3 Nedůvěryhodné a nevhodné aplikace a služby

Určité nebezpečí pro firmu může plynout z aplikací a služeb, které využívají jejich zaměstnanci na svých BYOD zařízeních. Aplikací i internetových služeb mají uživatelé k dispozici spoustu. Některé nabízejí různé praktické a užitečné funkce pro jak pracovní tak i soukromé účely, jiné zase poskytují zábavu a odpočinek. Ne každá aplikace či internetová služba ovšem pochází od důvěryhodného a spolehlivého zdroje. Zdánlivě neškodné aplikace v sobě mohou ukrývat zranitelnosti, přes které by pak případný útočník mohl propašovat na uživatelovo zařízení malware. Někdy tyto zranitelnosti vznikají neúmyslně chybou programátora, jindy záměrně za účelem škodit.

Výrobci mobilních zařízení, ve snaze ochránit uživatele před bezpečnostními hrozbami, integrují do svých operačních systémů různá omezení a na své oficiální appstory pouštějí pouze aplikace, které prošly určitou kontrolou. Uživatelé sami však mohou využít specializované programy na softwarovou úpravu operačních systémů svých zařízení a tato omezení překonat. V případě iOS od Applu se jedná o tzv. *jailbreak*, v případě platformy Android se tento proces označuje jako *rooting*. Uživatel pak na vlastní riziko získává v OS vyšší oprávnění a může tak instalovat aplikace a využívat funkcionality, které by mu byly za normálních okolností nepřístupné. Pro firemní prostředí znamená zařízení, jež si prošlo takovouto SW úpravou, potenciální hrozbu.

Riziko pro podnik může ale hrozit i z aplikací a služeb, které nejsou podvodné ani neobsahují žádnou bezpečnostní slabinu. Problémem může být už samotná skutečnost, že je zaměstnanec začne využívat. Příkladem může být třeba internetová služba Dropbox pro pohodlný přístup k dokumentům odkudkoliv. Dropbox je velmi praktická a zároveň populární služba. Potíž nastává, když tam začne zaměstnanec přes svůj soukromý účet nahrávat a sdílet firemní data. Nad takovýmto úložištěm nemá firma žádnou kontrolu, nemůže zajistit, že se ke sdíleným datům nedostane nepovolaná osoba ani je nemůže smazat, když zaměstnanec skončí svůj pracovní poměr.

Dalším rizikem může být to, že zaměstnanec bude využívat v průběhu pracovní doby aplikace či služby, které nesouvisí s jeho prací, což může vést k nižší produktivitě. Příkladem může být sociální síť Facebook či oblíbená hra Angry Birds. A potíže mohou působit i aplikace, které spotřebovávají velké množství dat a zatěžují tak firemní síť.

Řešení:

- Součástí firmou podporovaného BYODu obvykle bývají i firemní pravidla, která zaměstnancům omezují možnosti užití některých aplikací a služeb na svých zařízeních. Je potřeba, aby zaměstnanec podepsal, že byl s pravidly seznámen a že se jimi bude řídit.

- Rooting či jailbreak je třeba v rámci firemního BYOD programu zakázat. Schopnost detekovat a případně i rovnou zablokovat zařízení, jež si tímto procesem prošly, bývá často součástí specializovaných softwarových nástrojů na správu zaměstnaneckých zařízení.

- Podniky mohou vytvořit tzv. *blacklist*, na který uvedou vybrané aplikace, které nejsou pro zaměstnance povolené. Blacklisty mohou být vynucovány pomocí specializovaných softwarových nástrojů na správu zaměstnaneckých zařízení.

- Vedle blacklistu může existovat i *whitelist*, na kterém budou uvedeny aplikace, jež jsou naopak doporučovány. Podnik může na whitelist uvést třeba bezpečnou alternativu aplikace, která byla blacklistem zakázána.

- To, jestli bude nějaká aplikace či služba zakázána či doporučena si musí každý podnik zvážit na základě rizik a přínosů, ke kterým by to mohlo vést. Tabulka 4.1 nabízí příklady aplikací, které podle firmy Fiberlink bývají často na blacklistech a whitelistech. Je vidět, že třeba služba Dropbox bývá různými firmami řazena jak do kategorie zakázaných, tak i povolených.

- Někdy se může vyplatit, aby si firma vytvořila vlastní aplikaci či internetovou službu, kterou bude mít sama pod kontrolou a poskytla jí zaměstnancům. Takovou službou může být třeba firemní datové úložiště, které by zaměstnanci mohli užívat namísto Dropboxu a dalších veřejných úložišť.

- Ke kontrolování či přímo blokování různých aplikací a služeb lze využít i síťové firewally, které mohou monitorovat a identifikovat data proudící po síti.

Tabulka 4.1: Příklady aplikací často zařazovaných do blacklistů i whitelistů různých firem. Zdrojová data z: [48].

Blacklist		**Whitelist**	
iOS	**Android**	**iOS**	**Android**
Dropbox	Dropbox	iBooks	NITDroid
SugarSync	Facebook	Adobe Reader	Adobe Reader
BoxNet	Netflix	Google	Lookout
Facebook	Google+	Citrix Receiver	Google
Google Drive	Angry Birds	Numbers	Skype
Pandora	Google Play Movies & TV	Dropbox	Citrix Receiver
SkyDrive	Google Play Books	Pages	Android Translator
Angry Birds	Sugarsync	itunes U	Antivirus
HOCCER	Google Play Music	Keynote	ZXing
Netflix	Google+ Hangouts	WebEx	Google Mapsa
Dropbox	Dropbox	iBooks	NITDroid
SugarSync	Facebook	Adobe Reader	Adobe Reader

4.1.4 Připojení z nedůvěryhodné sítě

Občas se zaměstnanec na svém soukromém mobilním zařízení může potřebovat připojit k síti, která se nedá považovat za důvěryhodnou. Může jít například o internetovou kavárnu, přes jejíž síť se chce zaměstnanec připojit do firemního systému. Provoz v takovéto nedůvěryhodné síti může být monitorován třetí osobou, která tak může odposlechnout přístupová hesla nebo třeba přesměrovat přicházející/odcházející data na svůj počítač.

Řešení:

- Pro takovéto případy je potřeba, aby byla data proudící mezi zaměstnancovým zařízením a firemním systémem šifrována.
- Přístup k firemním datům a službám je třeba povolit až teprve poté, co zaměstnanec zadá své uživatelské jméno a přístupové heslo.
- VPN (Virtual Private Network) umožňuje v prostředí nedůvěryhodné sítě vytvořit uzavřené a šifrované spojení mezi několika počítači, tedy vlastní privátní síť.
- Nedůvěryhodnou sítí by se případně mohla stát i samotná firemní wi-fi síť a to v situaci, kdy se do ní budou volně připojovat jak zaměstnanci, tak i firemní zákazníci a návštěvníci. Nechce-li podnik přestat poskytovat

bezdrátový internet i libovolným návštěvníkům, může vytvořit druhou wi-fi síť, k níž budou mít přístup pouze zaměstnanci.

4.1.5 Ztráta/krádež/odchod

Ať už nastane situace, že bude zaměstnancovo mobilní zařízení ztraceno, ukradeno, nebo s ním zaměstnanec přejde k jinému zaměstnavateli, pro firmu to znamená riziko úniku dat. Krom toho, že se podniková data mohou dostat do nepovolaných rukou, tak může dojít i na situaci, kdy o daná data přijdete úplně a to v případě, že nejsou nikde zazálohována.

Řešení:

- Aby se ztížil přístup ke ztraceným či ukradeným zařízením, je nutné po zaměstnancích zapojených v BYOD programu požadovat, aby na svých zařízeních měli nastavené heslo nebo PIN. Při opakovaném nesprávném zadání hesla či PINu by pak mělo dojít k zablokování či smazání daného zařízení.

- Minimalizovat únik dat se dá i tím, že ne každý zaměstnanec bude mít plný přístup ke všemu. Je tedy třeba vytvořit různé uživatelské role, kterými bude určeno kdo má přístup k čemu. Tyto role je pak třeba přidělovat konkrétním zaměstnancům tak aby každý měl přístup jen k tomu co potřebuje.

- V případě ztráty či krádeže je užitečné, aby u daného zařízení bylo možno sledovat jeho polohu. Pokud je zařízení touto funkcí vybaveno, dá se pak zjistit jeho současná, nebo alespoň poslední zaznamenaná poloha.

- Ne vždy je však možné zařízení získat zpět. Potom je třeba zajistit, aby se alespoň jeho obsah nedostal k někomu cizímu. Existují různé programy a funkce, které umožňují dané mobilní zařízení na dálku zamknout či vymazat data v něm obsažená (*remote lock/wipe*).

- Aby mohlo firemní IT oddělení podniknout kroky k ochraně pohřešovaného zařízení, musí se o něm napřed dozvědět. Proto je třeba, aby měli zaměstnanci povinnost hlásit ztrátu svých BYOD zařízení neprodleně.

- Ochranu dat na mobilním zařízení lze zvýšit šifrováním jeho úložného prostoru.

- Velmi účinným způsobem jak zajistit, aby se data z mobilního zařízení neztratila, je vůbec je tam neukládat. Pomocí virtualizace je možné na mobilním zařízení spustit aplikaci nebo třeba další operační systém, který běží odděleně od OS daného zařízení. Na mobilním zařízení stačí

mít nainstalovaný virtuální stroj, který si po spuštění stáhne vše potřebné, pracuje s tím v operační paměti mobilního zařízení a před ukončením odešle zase všechny provedené změny zpět na firemní server.

- Ať už se přes mobilní zařízení přistupuje k jakýmkoliv službám na podnikovém serveru, je třeba, aby byl přístup podmíněn zadáním uživatelského jména a hesla. Ke zvýšení bezpečnosti u pro firmu kritických služeb může posloužit nějaký pokročilý bezpečnostní systém, jako třeba 2FA (Two-Factor Authentication), takže pak k přihlášení může být krom hesla nutno navíc zadat čerstvě vygenerovaný jednorázový kód, který uživatel obdrží například pomocí SMS zprávy.

4.2 Technické zajištění

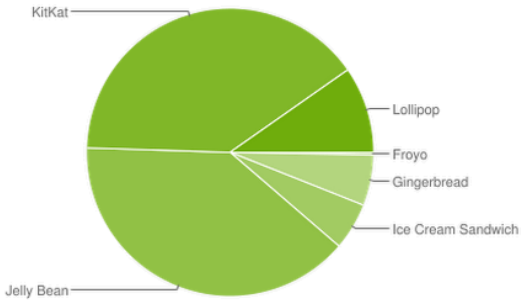
Když organizace povolí ve svém prostředí BYOD, musí být i připravena unést zátěž, kterou to bude působit na její infrastrukturu. Pokud firma již dříve poskytovala zaměstnancům firemní mobilní zařízení, potom již možná má nějaký balík softwarových nástrojů na správu mobilních zařízení, firemní wi-fi, či zaměstnance zajišťující mobilním zařízením servis. Příchod mnoha různých mobilních zařízení vlastněných zaměstnanci si ale obvykle vyžaduje velké změny oproti době, kdy se v podnikovém prostředí pohybovaly pouze firemní zařízení stejného typu, nebo alespoň zařízení od jediného výrobce. Aby se výhody BYODu mohly projevit a firma z nich mohla mít užitek, musí být připravena investovat nemalé množství úsilí i finančních prostředků do nové podoby infrastruktury, která bude reagovat i na nové výzvy, jež přicházejí s využíváním soukromých zařízení na práci.

4.2.1 Diverzifikace zařízení

Nabídka trhu s mobilními zařízeními pro běžné uživatele je široká a kromě zavedených výrobců jako jsou Apple, Samsung, Lenovo, Blackberry a mnoho dalších, se průběžně pokoušejí prosadit i různí noví hráči. Jedním takovým je třeba čínská společnost Xiaomi, která již uspěla na svém domovském trhu a nyní expanduje do světa. I v operačních systémech těchto mobilních zařízení je nemalá rozmanitost. Zatímco třeba u iOSu jsou uživatelé firmou Apple vcelku důsledně vedeni k pravidelným aktualizacím (momentálně nejnovější verzi 8 mělo v květnu 2015 nainstalováno 81 % zařízení [49]), v případě platformy Android je situace docela jiná. Existuje mnoho verzí, jež jsou stále značně rozšířeny a uživatelé nejsou motivováni přecházet vždy na nejnovější verzi OS a často jim výrobce novou verzi OS vyladěnou pro jejich přístroj už ani nenabízí (viz graf 4.2). Vedle toho i tady průběžně vznikají nové operační systémy, které bojují o možnost se trvale prosadit vedle už zavedené konkurence. Příkladem takového systému může být třeba Firefox OS od Mozilly.

Version	Codename	API	Distribution
2.2	Froyo	8	0.3%
2.3.3 - 2.3.7	Gingerbread	10	5.7%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.3%
4.1.x	Jelly Bean	16	15.6%
4.2.x		17	18.1%
4.3		18	5.5%
4.4	KitKat	19	39.8%
5.0	Lollipop	21	9.0%
5.1		22	0.7%

Data collected during a 7-day period ending on May 4, 2015.
Any versions with less than 0.1% distribution are not shown.



Obrázek 4.2: Rozšířenost jednotlivých verzí OS Android mezi uživateli.[50]

Podniku, který se rozhodne u svých zaměstnanců podporovat BYOD, hrozí, že bude zahlcen obrovským množstvím různých zařízení od různých výrobců a nebude schopen zajistit jejich bezpečné fungování.

Řešení:

- Snaha podporovat ve firemním BYOD programu jakékoliv zařízení, které si může zaměstnanec přinést, by byla neúnosně nákladná i složitá. Proto bývá potřeba určit, která zařízení budou a která nebudou podporována. Nepodporovaná zařízení mohou mít přístup k firemním datům jen částečný (např. přístup k pracovnímu e-mailu přes webové rozhraní) a nebo mohou mít přístup k datům zcela zakázaný, je-li to potřeba např. z bezpečnostních důvodů. Tabulka 4.2 ukazuje celkové prodeje chytrých telefonů předních výrobců za rok 2014.
- Zpravidla bývají podporovány zařízení s operačnímy systémy od Applu, Androidu a Microsoftu, které jsou nejrozšířenější.
- Kromě softwaru, který by uměl konfigurovat a dohlížet na všechna podporovaná zařízení, je potřeba změnit help-desk, tak aby se dokázal vypořádat s touto rozmanitostí zařízení. Je třeba určit, v jakém rozsahu bude podnik poskytovat BYOD zařízením podporu, tak aby zaměstnanci zůstali co nejproduktivnější.

Tabulka 4.2: Celosvětová velikost prodejů smartphonů za rok 2014 podle jednotlivých výrobců. Zdrojová data z: [51]. [4]

Společnost	**2014 Množství (tisíce ks.)**	**2014 - Podíl na trhu (%)**	**2013 Množství (tisíce ks.)**	**2013 - Podíl na trhu (%)**
Samsung	307,597	24.7	299,795	30.9
Apple	191,426	15.4	150,786	15.5
Lenovo*	81,416	6.5	57,424	5.9
Huawei	68,081	5.5	46,609	4.8
LG Electronics	57,661	4.6	46,432	4.8
Others	538,710	43.3	368,675	38.0
Total	**1,244,890**	**100.0**	**969,721**	**100.0**

4.2.2 Správa zařízení, aplikací a služeb

Aby mohlo být běžné mobilní zařízení bezpečně užíváno při práci, zaměstnavatel potřebuje mít možnost na něm provést určitou konfiguraci vyplývající hlavně z jeho bezpečnostních požadavků. Aby mohlo spolupracovat s podnikovou IT infrastrukturou, musí existovat způsob, jak na zařízení nainstalovat potřebný software nebo licenci. Zejména v počátcích BYODu, tedy u prvních moderních chytrých telefonů na toto nebylo ještě myšleno. Proto byla jejich konfigurace pro firemní prostředí velmi obtížná. V dnešní době již výrobci chytrých zařízení reagují na potřeby podniků a postupně vybavují svá zařízení funkcemi umožňující lepší konfigurovatelnost.

Kromě samotných zařízení je však často potřeba konfigurovat i jednotlivé aplikace, které zaměstnanci využívají. Tady je problém složitější kvůli tomu, že existuje nespočet různých vývojářů po celém světě a zejména pokud jejich aplikace nebyla primárně určena pro podnikové účely, nedá se příliš doufat, že by k nim doplnili potřebné konfigurační funkce.

Zařízení, aplikace ale i služby, které k firemnímu BYODu zaměstnavatel poskytuje, mohou být užívány v rozporu s bezpečnostními pravidly nebo mohou být užívány nežádoucím způsobem. Zaměstnanec může například v pracovní době zatěžovat firemní datovou síť sledováním streamovaného videa. Nebo naopak třeba své BYOD zařízení vůbec k práci nevyužívá a při tom dostává od svého zaměstnavatele příspěvky na jeho provoz.

Řešení:

- Správa mobilních zařízení se řešila už před příchodem BYODu u firemních notebooků a telefonů. Už tehdy vznikly softwarové nástroje pro

[4]* Lenovo je nyní vlastníkem společnosti Motorola, jejíž prodeje mobilních telefonů jsou započítány do prodejů Lenova

jejich správu známé jako Mobile Device Management (MDM). Firmy poskytující MDM spolupracují s výrobci mobilních zařízení a kromě možnosti lépe konfigurovat dané zařízení také umožňují spravovat zařízení od různých výrobců pomocí jednoho softwaru.

- Kromě MDM vznikl i softwarový nástroj určený ke správě samotných aplikací. Označuje se jako Mobile Application Management (MAM). Pomocí MAM lze kontrolovat aplikace na zaměstnancově zařízení, dohlížet tak na jejich správné užívání a případně je na dálku překonfigurovat či smazat.

- Dodavatelé MAM často poskytují i vlastní aplikace určené pro firmy, které odpovídají jejich potřebám na funkčnost, bezpečnost a konfigurovatelnost.

- Pokud podniku nestačí žádná z nabízených aplikací, může se rozhodnout pro vytvoření vlastní aplikace. K tomu si může opatřit platformu pro vývoj mobilních aplikací, nebo může využít služeb firem, jež se tvorbou aplikací na zakázku přímo živí.

- Aby se zabránilo nežádoucímu či nehospodárnému užívání mobilních zařízení ve firmě, bývají softwarové nástroje pro jejich správu vybaveny i funkcemi pro monitorování a vyhodnocování. Díky takovýmto sledovacím funkcím může mít podnik nejen přehled o nevhodném užívání mobilních zařízení, aplikací a služeb, ale může hodnotit produktivitu a chování svých zaměstnanců. Díky tomu se pak dají snižovat náklady za firemní BYOD program i vyhodnocovat jeho účinnost. Jedná se však i o zásah do soukromí zaměstnanců. Proto je třeba nastavit oboustranně přijatelná pravidla, která budou zakotvena například v pracovní smlouvě.

- Zásah do soukromí zaměstnance může být, i pokud bude celý obsah jeho soukromého BYOD zařízení na dálku smazán firemním MDM. To může být povoleno firemními BYOD pravidly, které zaměstnanec podepsal, ale pro zaměstnance je daleko žádanější, pokud mohou být na jeho zařízení zvlášť odděleny osobní a firemní data. Toho bývá v praxi obtížně dosaženo a je to nejen o konfiguraci mobilního zařízení a poskytnutí firemního SW, ale je to také hodně o chování daného zaměstnance. Třeba předpoklad, že fotografie jsou vždy soukromými daty, je mylný. Zaměstnanci totiž občas fotí třeba tabule s pracovními nákresy a poznámkami.

- Řešením může být třeba tzv. *geo-fencing*, který může zablokovat fotoaparát na mobilním zařízení vždy, když zaměstnanec vstoupí do budovy zaměstnavatele. Podobně je možné ve vybraných aplikacích třeba znepřístupnit funkci *copy-paste*. Pokud si zaměstnanec ale vezme klasický fotoaparát a vyfotí obrazovku svého BYOD zařízení, těžko se tomu lze nějak bránit.

- Nakonec je tedy otázka smazávání celého zařízení či jen firemních dat o tom, do jaké míry je podnik ochoten riskovat určitou ztrátu dat a jak moc chce svého zaměstnance odrazovat od zapojení do BYOD programu. Zmírněním tohoto problému mohou být rozdílná pravidla pro různé zaměstnance v závislosti na tom, s jak citlivými daty pracují.

4.2.3 Downtime

Podpora a servis BYOD zařízení bývá daleko složitější než je tomu u firmou vlastněných zařízení. Ne s každým zařízením, které si zaměstnanec může přinést, budou mít firemní technici stejně velké zkušenosti, aby ho dokázali rychle uvést zpět do provozu. A někdy znalosti a zkušenosti s daným zařízením ani nestačí. Firemní technici mohou sice pomoci například s resetem SW do továrního nastavení, ale třeba výměnu vadného displeje, provést už kvůli záruce na zaměstnancově zařízení nemohou. Firemní technickou podporu při zavedení BYODu je potřeba významným způsobem změnit. I tak ale mohou být problémy, které podnikový IT zaměstnanec nebude schopen řešit.

Řešení:

- Nová technická podpora může být z části realizována tak, že bude podporovat zaměstnance, aby dokázali řešit problémy na svých zařízeních svépomocí. Vhodným pomocníkem může být firemní diskuzní fórum či wiki-stránky s radami a tipy na řešení obvyklých problémů. Více viz podkapitola 3.4.3.

- Některé problémy si zaměstnanci sami vyřešit nedokážou, či ani nemohou. Pro takové případy musí firma zajistit zaměstnance, kteří budou schopni poskytnout všem ve firmě podporovaným zařízením určitou technickou podporu.

- V případě závažnějších problémů či HW poruch, musejí obvykle IT zaměstnanci odkázat svého kolegu k výrobci či prodejci, u kterého zařízení koupil. Po dobu, než bude vyřízena reklamace, může firma zaměstnanci zapůjčit firemní zařízení.

- Zaměstnanci nemusí samotné náhradní zařízení vždy stačit. Pro to, aby mohl pokračovat v práci může potřebovat i přístup ke svým telefonním kontaktům, či jiným datům, jež má na svém momentálně nefunkčním BYOD zařízení. Pokud firma využívá virtualizaci, je možné nahrát ze serveru uživatelův image v poslední uložené verzi na nové zařízení. Zaměstnanec tak má neustále přístup ke všem datům i aplikacím a jeho práce může nerušeně pokračovat na jakémkoliv zařízení.

4.2.4 Výkon firemní sítě

Zavedení BYOD programu sebou obvykle nese častější využívání mobilních zařízení ve firmě a tedy vyšší zátěž na firemní síť. Přetížená datová infrastruktura může místo zvýšení pracovní produktivity způsobit naopak její snížení. Původní datová síť mohla být designována jen tak, aby unesla zátěž pracovních stanic a několika málo firemních notebooků, které musely být nakoupeny pro klíčové zaměstnance. Pokud ale začne většina zaměstnanců připojovat k datové síti i své soukromé smartphony, notebooky či tablety, může to vést ke snížení datové propustnosti sítě a může to přetěžovat i firemní servery. A v budoucnu s příchodem *Internetu Věcí* (Internet of Things) může být problém ještě větší. Zaměstnanci mohou začít chtít k firemní síti zapojovat zařízení jako chytré hodinky, chytré brýle a další podobné tzv. *Wearable computers*.

Řešení:

- Tento problém lze řešit investicí do nové infrastruktury.
- Zátěž je možné zmírnit i tím, že do BYOD programu nebudou zapojováni ti zaměstnanci, kteří to ze své pracovní pozice nemají jak využít.
- Zajistit, aby se k síti připojovala jen konkrétní povolená zařízení, lze například na úrovni síťových routerů pomocí filtrování MAC adres. Tedy tím, že router připojí k síti jen ta zařízení jejichž MAC adresu má na svém seznamu povolených zařízení.
- Pomohou i pravidla regulující užívání firemní datové infrastruktury a nástroje na monitorování datového provozu a provozu na BYOD zařízeních, tak aby se zajistilo, že zaměstnanci nebudou zatěžovat síť soukromým datovým provozem.

4.3 Legislativa & politika

Zavádění BYOD programu sebou nepřináší pouze technické a bezpečnostní otázky. Týká se i zákonů a zaměstnaneckých pravidel. Realizace BYODu ve firmě je tedy úkolem, na kterém se musejí podílet i firemní právníci a zástupci oddělení lidských zdrojů. Zejména otázka vlastnictví je v souvislosti s BYODem dost ošemetnou záležitostí. Je nutné naformulovat taková pravidla, která budou řešit všechny okolnosti užívání zaměstnancova soukromého zařízení ve firemním prostředí a s firemními daty, tak aby nehrozilo, že firma ztratí kontrolu. Zároveň je třeba, aby daná pravidla nejen respektovala zaměstnancova zákonná práva, ale také aby nepůsobila poněkud nepřátelsky a nebrala zaměstnanci příliš svobody při užívání jeho oblíbeného zařízení.

4.3.1 Otázka vlastnických práv

Zařízení, které zaměstnanec zapojí do firemního BYOD programu je jeho. Data, která na něm má už ale nemusí být vždy jeho, některá mohou patřit jeho zaměstnavateli. Může se stát, že zaměstnanec nebude tento vlastnický rozdíl řešit a i k firemním datům se bude chovat tak jak je zvyklý, tedy stejně jako ke svým soukromým.

Zvláštním případem je pak vlastnictví telefonního čísla. U běžného zaměstnance to obvykle nehraje roli, ale například u obchodních zástupců, kteří poskytují firemním klientům svá telefonní čísla, na kterých jsou k zastižení, už to může znamenat vážný problém. Pokud přestane být takový obchodní zástupce zaměstnancem firmy a přejde i se svým telefonem a telefonním číslem ke konkurenční firmě, zákazníci budou pořád volat jemu a on je tak může přetáhnout ke konkurenci.

Řešení:

- Je třeba jasně určit pravidla a povinnosti jak pro zaměstnance, tak i pro firmu. Zároveň s právem používat své oblíbené zařízení pro pracovní účely, musí zaměstnanec akceptovat určitou míru omezení, které mu na jeho zařízení stanoví zaměstnavatel.
- Důležité je, aby každý zaměstnanec, jehož se to týká, byl podrobně seznámen s obsahem a i konkrétním významem firemních BYOD pravidel a jejich akceptování stvrdil podpisem. Zaměstnanci by mělo být umožněno ještě před podpisem, aby dostal odpovědi na jakékoliv nejasnosti, které by u toho mohl mít.
- Při získávání práva monitorovat a řídit zaměstnancovo BYOD zařízení, firma nesmí zapomenout, že zaměstnanec má stále právo na ochranu osobních informací.
- Problém telefonního čísla je možno řešit prostřednictvím přesměrování telefonního hovoru v rámci podnikového telefonního systému, podobně jako to dříve fungovalo u pobočkových ústředen.
- Další možností řešení problému telefonního čísla je používání telefonů s dvěmi SIM-kartami, díky čemuž zaměstnanec může přijímat hovory na dvě různá telefonní čísla v jednom mobilu Navíc každá SIM-karta může být vedena u jiného operátora. Při odchodu zaměstnance z podniku pak stačí, aby vrátil jen firemní SIM-kartu.

4.3.2 Užívání soukromého SW pro pracovní účely

Zaměstnanci bývají zvyklí využívat programy či služby, které jsou dostupné běžným uživatelům. Potíž je v tom, že licenční podmínky takového programu

často vylučují komerční užití. Chce-li firma umožnit svým zaměstnancům práci na vlastních zařízeních, může být potřeba dodat jim některé programy, jako je třeba Photoshop nebo MS Office s komerční licencí.

Řešení:

- Obvyklou praxí je, že podniky nakupují licence na zařízení. Chce-li ale zaměstnanec využívat určitý program na více svých zařízeních, může vyjít levněji, pokud firma nakoupí licence na uživatele. Takovouto licenci pak lze přiřadit konkrétnímu uživateli, který jí pak může využívat na více zařízeních, včetně těch vlastních.
- Existují i další licence jako třeba licence *plus 1*, která umožňuje, aby měl zaměstnanec daný SW nainstalovaný na firemním počítači, plus ještě na jednom libovolném zařízení.
- Nejrozumnějším řešením může být opatření různých licencí, tak aby byly pokryty všechny firemní potřeby.

4.3.3 Hrazení nákladů na BYOD zařízení

Jak bylo popsáno v jedné z podkapitol kapitoly Finanční úspory (3.4.2), zákony některých zemí, včetně České republiky, vyžadují, aby zaměstnavatel přispíval zaměstnancům na jejich BYOD zařízení. Příspěvky se mohou týkat jak nákladů na telefonní a datové služby, tak i na opotřebení daného přístroje.

Řešení:

- Konkrétní podmínky hrazení těchto nákladů je třeba popsat například v pracovní smlouvě či jejím dodatku. Je třeba, aby byla jasně označena zařízení, která jsou v BYOD programu zaměstnancem užívána a firma na ně bude tedy přispívat.
- Protože je zaměstnancovo zařízení užíváno i k soukromým účelům, firma může přispívat jen na poměrnou část nákladů odpovídající užívání daného zařízení k pracovním účelům.

4.4 Zaměstnanci

BYOD znamená významnou změnu nejen pro fungování firmy, ale i pro fungování samotného zaměstnance. Získává nové možnosti, ale také nové povinnosti. Zde zmíněná rizika se netýkají výhradně BYODu. Pokud se ovšem podniku dosud nijak nedotýkala, při zavádění BYOD programu by na ně mělo být také myšleno.

4.4.1 Work/life balance

Možnost využívat pro práci i svá vlastní zařízení a tedy pracovat v podstatě kdekoliv a kdykoliv znamená nejen možnost zvýšit svou produktivitu, ale i další možnost způsobit si přepracování. Pokud zaměstnanec nedokáže najít zdravou rovnováhu mezi prací a svým soukromým životem, může si v krajním případě způsobit tzv. Syndrom vyhoření.

Syndrom vyhoření: *„... se týká zejména oblasti práce a je typické citovým a mentálním vyčerpáním. Často jde o důsledek dlouhodobého stresu a týká se nejvíce lidí, kteří pracují s jinými lidmi. Od deprese nebo prosté únavy se syndrom vyhoření liší hlavně tím, že se vztahuje výhradně na onu krizovou oblast a jeho součástí jsou pochybnosti o smyslu dané práce.“*[52]

Přepracovanost a syndrom vyhoření není radno podceňovat, protože vede ke snížení produktivity a zvýšení chybovosti. Nástup syndromu vyhoření je plíživý proces, proto je běžné, že si člověk neuvědomí vznikající problém včas. Léčba syndromu vyhoření trvá dlouho a může i vyžadovat, aby firma snížila nároky na daného zaměstnance.

Řešení:

- Zaměstnance je třeba jasně upozornit na tato rizika. Vhodné je, aby si zaměstnanci pro sebe stanovili pravidla, kterými se budou sami řídit, jako třeba nekontrolovat firemní e-mail po deváté hodině večer.
- Striktní zákaz všech aplikací a služeb nesouvisející s prací může být ve výsledku kontraproduktivní. Pro udržení produktivity na rozumné úrovni může být naopak užitečnější některé aplikace a služby neblokovat (např. přehrávání hudby, YouTube) a pokud zaměstnanec odvádí dobrou práci, tolerovat mu, že menší část své pracovní doby věnuje i něčemu jinému.
- Pokud podnik zjistí zvýšený výskyt přepracovanosti u svých zaměstnanců, může případně sám nastavit některá omezení, kterými svým zaměstnancům přímo omezí možnost pracovat nad rámec své pracovní doby. Takovým omezením může být třeba znepřístupnění vzdáleného připojení k firemním systémům přes víkendy a svátky.

4.4.2 Nedodržování firemních pravidel

Kromě záměrného porušování firemních pravidel může daleko častěji docházet k zapomínání na pravidla, zejména pokud je zaměstnanci nebudou vnímat jako důležitá. Zaměstnanci také mohou pravidla obcházet z lenosti například tím, že budou používat na svých zařízeních slabá hesla nebo že si budou svá hesla psát na papírek nalepený na monitoru.

Řešení:

- Kromě podrobného školení na začátku zapojení do BYOD programu je vhodné pravidelně zaměstnance informovat ohledně aktuálních hrozeb. K tomu lze využít oběžníky, intranet či se o tom zmiňovat na poradách. Příkladem takové aktuální hrozby byl v roce 2014 tzv. *Heartbleed Bug*, který ohrozil bezpečnost šifrovaných dat na Internetu. Běžný zaměstnanec si nemusí vůbec dokázat uvědomit, jak se takováto chyba může dotknout i jeho a jeho BYOD zařízení.

- Zaměstnavatelé by po zaměstnancích měli vyžadovat používání silných hesel, která si ale budou pamatovat. Jako prevence proti zapisování si hesel na papírky může pomoci, když firma zaměstnancům doporučí mnemotechnické tipy, jak si heslo zapamatovat.

- Klasická hesla mohou být případně nahrazena biometrickou autentizací, jako je třeba čtečka otisků prstů, která po uživateli nevyžaduje, aby si něco pamatoval.

- Na tabletech a smartphonech s dotykovou obrazovkou bývá možnost využívat k odemykání displeje takzvaný *Pattern Screen Lock*, který po uživateli vyžaduje zapamatovat si místo číselného hesla sérii pohybů prstu po displeji. Jde o vcelku populární alternativu, která však není bezpečnější než zadávání číselného hesla. Může však zmírnit problém se zapomínáním hesla a jeho psaním si na papírky.

- Aby byla pravidla dodržována, musí být jasně definovány sankce a pokuty za jejich porušení. Pravidla, u jejichž porušování se sankce neuplatňují, mohou vést zaměstnance k pocitu, že se vlastně nejedná o důležité pravidlo. Soupis pravidel se pak stává jen zbytečně popsaným kusem papíru.

Jednotlivé výzvy a rizika popsané v této kapitole mohou mít pro každou firmu jinak velkou důležitost a z toho vyplývá i to jaká řešení by ta která firma měla využít. Některá rizika není možno nikdy úplně eliminovat, takže snaha investovat do všech myslitelných opatření může být zbytečně drahá a přinášet více komplikací než užitku. Aby se podnik mohl správně rozhodnout, musí si napřed ujasnit, které věci jsou pro jeho činnost důležité a jak moc. Pak teprve lze vybrat taková řešení, která budou odpovídat potřebám a přitom budou finančně i technicky únosná.

Kapitola 5

Řešení správy mobilních zařízení, aplikací a jejich obsahu

V předchozí kapitole byla popsaná řešení jednotlivých výzev a komplikací, které mohou nastat při vpuštění BYODu do firemního prostředí. Zmíněná řešení bývají často už součástí specializovaných softwarových balíků. Tyto balíky se skládají z nástrojů a funkcí zaměřených na správu mobilních zařízení, správu samotných aplikací, správu datového obsahu, nebo kombinují vše do jednoho produktu. Výrobci těchto balíků často zákazníkům nabízí kromě svých produktů i pomoc s jejich výběrem a integrováním do podnikového fungování.

5.1 Mobile Device Management

Mobile device management (MDM) je termín používaný v souvislosti se správou mobilních zařízení (jako jsou smartphony, tablety a notebooky) užívaných ve firemním prostředí. Obvykle to zahrnuje jejich nasazení, zabezpečení, monitorování, integrování a řízení.[53]

MDM je obvykle řešeno softwarovým balíkem, který nabízí všechny potřebné funkce. Tento software získává nad mobilním zařízením velký díl kontroly, s cílem nastavit ho a zabezpečit tak, aby mohlo být připojeno k firemní síti. Pomocí MDM je možno spravovat jak firemní zařízení tak i zařízení vlastněná samotnými zaměstnanci. Uživatelé jsou obvykle nuceni pro přístup k danému zařízení a na něm obsažených citlivých dat zadávat bezpečnostní kód. V případě ztráty či krádeže mobilního zařízení, umožňuje MDM jeho vzdálené smazání. Firma může užíváním MDM softwaru snížit své náklady, zkrátit čas řešení technických potíží na mobilních zařízeních a zmírnit bezpečnostní rizika pro celou firemní síť.[36]

Ideální software pro správu mobilních zařízení (MDM) by měl [53]:

- Poskytovat plnou kompatibilitu s operačními systémy a aplikacemi všech běžných mobilních zařízení.

- Umožňovat fungování s více různými poskytovateli služeb.
- Nabízet možnost okamžité implementace skrze službu over-the-air na jakékoliv vybrané zařízení.
- Umožňovat co nejrychlejší nasazení nejnovějšího hardwaru i softwaru dostupného na trhu.
- Být schopen přidávat či odebírat zařízení ze systému podle potřeby, aby se zaručilo optimální fungování firemní sítě.

Samotné MDM sebou obvykle přináší pro uživatele znatelná omezení v možnostech užívání daného mobilního zařízení, což může být uživateli zejména na jím vlastněném zařízení nepříjemné. MDM bylo prvním přístupem k řešení problematiky mobilních zařízení. Později začaly vznikat i další přístupy, které reagovaly na nedostatky původního MDM. V současné době, když se hovoří o MDM, bývají často jeho součástí i funkce cílící na správu mobilních aplikací a obsahu.

5.2 Mobile Application Management

Termín Mobile application management (MAM) se týká dodávání a správy firemního softwaru na koncové zařízení uživatele. Software zajišťující MAM funkcionalitu obvykle obstarává celý životní cyklus mobilní aplikace. Dokáže zajistit její dodání na cílové zařízení, obstarat potřebné licence, konfiguraci, aktualizace a poskytnout i informace o jejím užívání. Důležitou funkcí je vzdálené smazání firemních aplikací a dat z uživatelova zařízení. Na rozdíl od MDM je MAM pro uživatele méně omezující. Nesnaží se ovládat celý přístroj, ale soustředí se na kontrolu zaměstnavatelem dodaných aplikací. Dodavatelé MAM řešení často svým zákazníkům nabízejí i aplikace na míru vytvořené pro firemní potřeby.[54]

5.3 Mobile Content Management

Software pro správu obsahu mobilních zařízení (Mobile content managemet) poskytuje technologie pro zabezpečený přístup k firemním datům na smartphonech, tabletech a dalších koncových zařízení. Základní částí MCM softwaru je datové úložiště a služba na sdílení dat. Některá řešení jsou založena čistě na technologii cloudu zatímco jiná umožňují připojení koncového zařízení k firemnímu datovému úložišti. MCM často umožňuje firmám přidat nástroje pro podporu týmové spolupráce, například v podobě možnosti komentovat data sdílená mezi několika kolegy.[55]

5.4 Enterprise Mobility Management

Enterprise mobility management (EMM) je dalším krokem ve vývoji řešení problematiky mobilních zařízení ve firemním prostředí. Představuje sjednocení funkcí poskytovaných nástroji na správu mobilních zařízení (MDM), mobilních aplikací (MAM) a mobilního obsahu (MCM). Užíváním softwarového balíku EMM mohou firmy zajistit podporu svých zaměstnanců užívajících mobilní zařízení i udržet v maximální účinnosti firemní bezpečnostní pravidla.[11]

EMM software by měl poskytovat tyto klíčové funkce [11]:

- inventář zařízení;
- inventář aplikací;
- nástroje na konfiguraci operačních systémů mobilních zařízení;
- dodávání, aktualizování a smazávání mobilních aplikací;
- konfiguraci a správu pravidel na mobilních aplikacích;
- vzdálené připojení a dohled pro účely technické podpory;
- provádění vzdálených akcí jako je třeba smazání zařízení;
- správu obsahu mobilních zařízení

5.5 Přední dodavatelé EMM řešení

Na trhu existuje řada dodavatelů řešení pro problematiku mobilních zařízení ve firemním prostředí. Jejich řešení nabízejí různý stupeň komplexnosti a úplnosti. Ne všichni dodavatelé nabízejí stejné funkce a rozdíly mohou být i v tom, která mobilní zařízení jejich softwarová řešení podporují. Při výběru vhodného dodavatelé EMM řešení je tedy potřeba hledat takového, který nejvíce odpovídá požadavkům konkrétního zákazníka na podobu firemní mobility.

Analytická společnost Gartner provedla v roce 2014 hodnocení čtrnácti předních dodavatelů EMM řešení a zanesla je do svého *Magic Quadrant* grafu (viz obrázek 5.1). Firmy v něm jsou hodnoceny podle následujících dvou měřítek [11]:

- **Ability to Execute** (schopnost realizace) – měří schopnost dodavatele dosáhnout podílu na trhu a odpovídat svými službami a produkty současným požadavkům zákazníků.
- **Completeness of Vision** (kompletnost vize) – shrnuje pravděpodobnost budoucího úspěchu daného dodavatele na tomto trhu v závislosti na jeho prohlášeních o směřování produktu, úrovni jak moc jeho schopnosti vyhovují budoucí poptávce a jeho soustředění na požadavky na EMM produkty.

Z toho vychází zařazení do jednoho ze čtyř kvadrantů, kterými jsou [11]:

- **Leaders** (lídři) – Dosahují nejvyšších tržeb na trhu EMM řešení, mají za sebou řadu úspěšných implementací a dobré renomé u zákazníků. Jejich EMM produkt nabízí největší kompletnost a odpovídá trendům trhu. Mají strategii, díky níž mohou doufat i v budoucnu v úspěch na trhu.

- **Challengers** (vyzyvatelé) – Jsou schopni oslovit velkou základnu zákazníků a dosahovat vysokých tržeb. Jejich notné zdroje jim zajistí dlouhou životaschopnost na trhu. Nabízejí solidní produkty, které ovšem nepředstavují nutně to nejlepší na trhu a postrádají plán do budoucna jak se odlišit od konkurence.

- **Visionaries** (vizionáři) – Mají jedinečné schopnosti v určitých aspektech EMM. Přicházejí s inovativními přístupy k řešení zásadních problémů jako je třeba podpora platformy Android či ochrana před ztrátou dat. Jsou vhodní pro zákazníky, jež kladou velký důraz na vybrané oblasti EMM. Jejich produkty nemusí dosahovat stejné úplnosti, výkonnosti či podpory jako je tomu u lídrů trhu.

- **Niche Players** (specializovaní hráči) – Bývají dobrou volbou pro organizace. Jejich produkty nenabízejí stejnou úroveň kompletnosti ani nedosahují stejných tržeb a zákaznického renomé jako je tomu u lídrů a vyzyvatelů. Jejich strategií bývá spíše držet krok s trhem než ho vést, což může být způsobeno nedostatkem jejich zdrojů. Jejich EMM produkty bývají často rozšířením jiného jejich produktu. Pokud případný zákazník nepožaduje ty nejlepší dostupné schopnosti a funkce, mohou pro něj být specializovaní hráči vhodnou volbou oproti dražším a rozsáhlejším produktům lídrů a vyzyvatelů.

Z grafu 5.1 je vidět, že společnost BlackBerry, která byla kdysi lídrem trhu s nástroji pro správu mobilních zařízení je nyní výrazně pozadu za svými konkurenty. Společnost Gartner vyhodnotila jako současné lídry trhu firmy AirWatch, IronMobile a Citrix. K těmto firmám a jejich produktům sepsala následující stručné hodnocení [11]:

5.5.1 AirWatch

AirWatch, jež byl v roce 2014 koupen společností VMware, funguje i nadále jako oddělená obchodní jednotka s označením AirWatch by VMware. VMware plánuje využít AirWatch k vybudování agregátoru pracovního prostředí, doplňujíc svou desktop virtualizaci a technologii řízení aplikací poskytovanou jako

Obrázek 5.1: Graf Magic Quadrant porovnává přední poskytovatele EMM řešení.[11]

SaaS[5]. Soubor produktů, v nabídce přes SaaS nebo on-premises[6], se skládá ze standardních komponent produktu EMM navíc se službou application reputation a základním řízením pro PC a Mac počítače. Nabídka AirWatch má všestrannou EMM funkcionalitu, která jim umožňuje častá vítězství ve výběrových řízeních. Má dobrou administrativní konzoli se zabudovanými výukovými videi, linky a pro nové administrátory přístup podobný wizardu, který jim umožní rychle se s ním naučit pracovat. Protože komponenty mobile ap-

[5]SaaS - Software as a Services - model nabízení softwarových produktů, kdy je produkt hostován a spravován na serveru výrobce, zákazník jej využívá vzdáleně přes Internet a platí za to pravidelné poplatky.

[6]On-premises - tradiční model nabízení softwarových produktů, kdy je produkt nainstalován a provozován na vlastní HW infrastruktuře zákazníka.

plication management a mobile content management jsou někdy nestabilní a jejich použitelnost je obtížná, zákazníci často využívají především vlastnosti MDM. AirWatch nadále tlačí na inovaci a je jedním ze dvou vedoucích dodavatelů, kteří poskytují podporu nejnovějším verzím iOSu už ve stejný den, kdy jsou zveřejněny, a byl jedním z prvních, kdo podporoval klíčové technologie jako Apple Volume Purchase Program a Samsung Knox. AirWatch se hodí pro organizace, které potřebují EMM s všestranným souborem vlastností na širokou škálu platforem.

5.5.2 Citrix

Citrix vstoupil do světa EMM po akvizici Zenprise v lednu 2013. Zenprise byl přidán k technologii řízení mobilních aplikací Citrixu, stejně jako k Citrix ShareFile a Citrix NetScaler. Citrix ShareFile je jedním z nejucelenějších a nejlépe vybavených produktů s MCM funkcemi mezi dodavateli EMM. V květnu 2014 Citrix oznámil uvedení Workspace Suite, který kombinuje desktopovou virtualizaci a EMM, pro poskytnutí přístupových aplikací a obsahu jakémukoli zařízení skrze kombinaci fyzických a virtuálních mechanizmů. XenMobile je dostupný přes obchodní model on-premises nebo přes SaaS model. XenMobile MDM podporuje iOS, Android, Windows Phone, BlackBerry a Windows 8. Citrix MDX Toolkit podporuje iOS a Android. Existuje jen menší množství velkých nasazení produktu XenMobile (tj. přes 10 000 uživatelů) v porovnání s ostatními vedoucími dodavateli EMM. Citrix je vhodnou volbou pro organizace, které potřebují získat bezpečné pracovní prostředí zahrnující Windows, webové a mobilní aplikace, ale také pro organizace, které používají pomocné technologie, jako jsou XenApp, XenDesktop a NetScaler.

5.5.3 MobileIron

Strategie MobileIron je, nabízet takové EMM, které je agnostické k aplikacím a zařízením, které organizace užívá. Tím se liší od těch dodavatelů EMM, kteří kombinují proprietární Secure PIM[7] a EFSS [8] produkty s nástroji EMM. Společnost pokračuje v inovaci své EMM nabídky a usiluje o získávání patentů pro svou mobilní technologii. MobileIron je dostupný buď skrze nabídku on-premises nebo SaaS model. Produkt MDM podporuje iOS, Android, Windows Phone, Windows 8 a Mac OS X. Jejich modul řízení mobilních aplikací podporuje iOS a Android. MobileIron je jediným dodavatelem EMM na trhu, který demonstruje možnosti remote-view v reálném čase na iOS. MobileIron uvedli svůj Form S-1 v dubnu 2014, se záměrem provést první veřejnou nabídku akcií (IPO). To je důležité, vzhledem ke skutečnosti že se MobileIron

[7]PIM - Personal information management - typ softwaru určený ke správě kontaktů, kalendáře, schůzek a dalších osobních dat.

[8]EFSS - Enterprise cloud file sync & share - typ softwaru pro sdílení a synchronizování dokumentů napříč různými koncovými zařízeními.

snaží konkurovat větším a zavedeným dodavatelům. MobileIron je vhodný pro organizace, které uplatňují strategii best-of-breed na mobilní aplikace – jako je file share and sync, email a app reputation. Infrastruktura MobileIron je appliance-based[9] a má horší možnosti monitorování dostupnosti a výkonu než je tomu u mnoha ostatních konkurenčních produktů. Zákaznická podpora dostává ty nejvyšší známky v téměř všech referenčních pohovorech s odkazem na fakt, že společnost přes svůj rozvoj nabízí vnímavost a dialog týkající se vylepšení produktů, typické pro společnost v začátcích. Strategie MobileIron je integrovat se s dodavateli a produkty, které jsou těmi nejlepšími v daných oblastech.

Na rozdíl od dřívější doby, dnešní možnosti správy zaměstnanecké mobility jsou dost rozsáhlé. Firmy mají možnost zajistit si obsáhlý balík EMM nástrojů, který jim umožní spravovat různá mobilní zařízení, aplikace i data nebo mohou zvolit úžeji zaměřený produkt, jež bude více odpovídat strategii zaměstnanecké mobility, kterou chtějí podporovat. Protože neexistuje jedno univerzální řešení, je velmi důležité udělat si už na začátku dobrou představu o tom, jakou podobu zaměstnanecké mobility vlastně firma chce a potřebuje a podle toho vybírat dodavatele. Všichni dodavatelé nenabízejí to samé. Produkty některých dodavatelů mohou být v určitých oblastech rozvinutější než v jiných a někteří se zaměřují na řešení konkrétních potíží. Jít tedy za tím dodavatelem, který je momentálně označován za toho nejlepšího, nemusí vždy znamenat nejlepší volbu.

[9]Appliance Computing - SW architektura, kdy jsou zákazníkovi poskytnuty pracovní stanice v podobě tenkého klienta a které pak přistupují k objednaným SW službám přes Internet.

Kapitola 6

Metodologický rámec hodnocení BYODu u reálného zájemce

V rámci této bakalářské práce vznikl i metodologický rámec, který má pomoci reálnému zájemci zhodnotit smysluplnost podpory BYODu v jeho podniku. Rámec je ve formě dotazníku, který má případnému zájemci, o zavedení BYODu do vlastní firmy, poradit, nakolik by toto mohla být vhodná odpověď na potřeby jeho podniku a zda o ní tedy má smysl začít uvažovat. Dotazník nicméně nemůže dát jasnou odpověď na to, zda se zavedení BYOD programu případnému zájemci skutečně vyplatí. Situace každé firmy je velmi odlišná. Liší se jejich potřeby, možnosti i očekávání. A stejně tak i BYOD program je možné realizovat řadou různých způsobů. Pro získání jasné odpovědi si každá firma musí zhodnotit svou konkrétní situaci více do hloubky a k ní vybrat takové řešení, které bude nejvíce odpovídat jejím očekáváním a možnostem.

6.1 Proces vzniku dotazníku

Po té, co jsem prostudoval celé téma a vytvořil si obecnou představu, jsem se začal zamýšlet nad podobou metodického rámce. Z konzultací s vedoucím práce vyplynulo, že by rámec měl mít formu dotazníku. Potřeboval jsem tedy vymyslet otázky i způsob jejich vyhodnocení. Protože v koncepci BYOD je velké množství proměnných, jak na straně firem, tak i na straně způsobu a rozsahu užívání soukromých zařízení, první co jsem zvažoval, bylo zobrazení výsledku do třírozměrného grafu, kde bych měřil velikost možného užitku z BYODu, míru jeho využívání a to, jak velkou část firmy ovlivní. Tuto prvotní myšlenku jsem ale zavrhl. Trojrozměrný graf by byl obtížnější na zobrazování a pro uživatele by mohl být hůře pochopitelný. Navíc ani takto rozsáhlý graf by zřejmě nebyl dostatečný, aby obsáhnul všechny možné podoby BYODu. Postupně jsem tedy došel ke zjednodušenému dvourozměrnému diagramu, kde měřím užitečnost BYODu a komplikace.

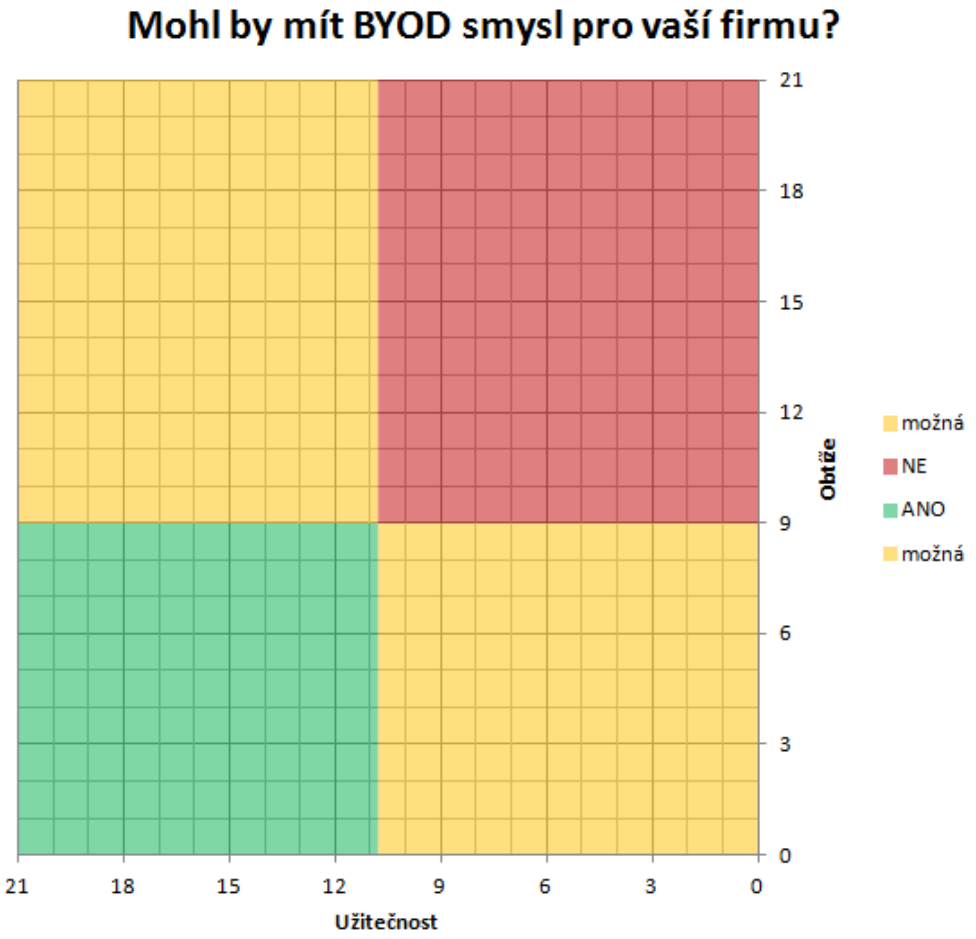
Při vymýšlení otázek do dotazníku jsem přemýšlel o různých firmách a zvažoval, co by pro takové firmy bylo ohledně BYODu důležité. Protože je možné BYOD využít ve skoro jakémkoliv typu firmy, najít otázky, které by byly obecně použitelné, nebylo jednoduché. Mým úkolem nebylo vytvořit popis zavedení BYODu u konkrétní firmy, takže i vymýšlené otázky jsem musel tvořit tak, aby byly víceméně univerzální. Navíc, má-li být dotazník určen možným zájemcům o BYOD, kteří jsou teprve na začátku zvažování a hlavně si teprve zjišťují informace, je pravděpodobné, že zatím nebudou schopni odpovídat na příliš konkrétní otázky.

Pro lepší utřídění otázek, jsem je začal rozdělovat do kategorií. Při tom jsem vycházel z kapitol 3 a 4. Otázky jsem si dělil do kategorií: Produktivita, Spokojenost, Náklady, Bezpečnost, Technické zajištění, Legislativa&Politika a Zaměstnanci. A dále pak podkategorie Užitečnost a Komplikace. Takto jsem mířil k velkému množství otázek podle jednotlivých kategorií. Řada otázek se mi ale překrývala a opakovala napříč různými kategoriemi. Odstraňováním duplicitních otázek se mi nakonec jejich rozdělení do kategorií téměř zrušilo a zbylo tak nakonec 18 otázek, dělících se do kategorií *Užitečnost* (10 otázek) a *Obtíže* (8 otázek). Výsledné otázky se snaží pojmout celou šíři tématu a při tom uživatele nezahltit, nevyžadovat po něm podrobné znalosti tématu a ani konkrétní rozhodnutí, jak řešit jednotlivé výzvy BYODu.

6.2 Popis dotazníku a jeho použití

Na začátku je stručné uvedení do problematiky BYODu, vysvětlení smyslu dotazníku a informace jak dotazník použít. Následuje formulář s osmnácti otázkami. U každé otázky je uvedeno několik možných odpovědí. Vedle otázek pak mohou být vysvětlující komentáře buď k celé otázce nebo k jednotlivým odpovědím. Poslední část obsahuje vyhodnocení uživatelových odpovědí. Ze zaškrtnutých odpovědí se vypočítají dva parametry, které pak určí pozici bodu v diagramu 6.1.

Jedním parametrem je *Užitečnost*, která vypovídá o potenciální velikosti užitku, který by daná firma mohla podporou BYODu získat. Druhý parametr je pojmenován slovem *Obtíže* a říká, jak moc náročná by podpora BYODu ve firmě mohla být. Samotný diagram se skládá ze čtyř kvadrantů. Zelený kvadrant je vymezen vysokou mírou užitečnosti a nízkými obtížemi. Pokud výsledek dotazníku ukáže do tohoto kvadrantu, potom je vysoká šance, že by se podpora BYODu ve firmě mohla vyplatit. Červený kvadrant je naopak určován vysokými obtížemi a nízkou užitečností. Pokud výsledek ukáže sem, potom pro firmu pravděpodobně nebude BYOD příliš vhodný. Dva žluté kvadranty pak značí, že buď je vysoká potenciální užitečnost ale zrovna tak i s tím související obtíže, nebo jsou obtíže nízké ale je nízká i potenciální užitečnost. Ukazuje-li výsledný bod do některého ze žlutých kvadrantů, potom, aby se BYOD vyplatil, bude si to žádat důkladné zvážení a plánování.



Obrázek 6.1: Podoba diagramu, na který se zobrazuje výsledek vyplněného dotazníku.

V případě, že situace v jednotlivých odděleních firmy se hodně liší, může být dotazník vyplněn zvlášť pro každé oddělení či skupinu několika oddělení ve firmě, což může poskytnout možnost přesnějšího zhodnocení. Jednotlivé výsledky vyšlé z dotazníku je možno zapsat do tabulky pod diagramem. Zapsané výsledky se pak budou také zobrazovat v diagramu a budou tak umožňovat vzájemné porovnání.

6.3 Popis aplikace

Dotazník byl vytvořen v programu Microsoft Excel 2007. Vzniklá aplikace se skládá ze tří hlavních vrstev (listů), které dohromady umožňují interaktivní fungování dotazníku. List Zdrojová data obsahuje především otázky, k nim

patřící odpovědi a u každé odpovědi je ještě uvedena její hodnota. V listu Výpočet se pak u každé otázky zjistí, jaká byla zvolena odpověď a napíše se její číselná hodnota. Tyto hodnoty se sečtou tak, aby vznikly dva parametry, které následně určí bod na diagramu, který je umístěn v dolní části listu Dotazník. List Dotazník obsahuje vše, co je pro uživatele potřeba k tomu, aby mohl tuto aplikaci použít. Ostatními listy se tedy nemusí zabývat.

V listu Dotazník jsou na konci části s otázkami dvě tlačítka. Jedno slouží pro reset dotazníku, druhé pomáhá s návratem na začátek dotazníku. Funkce obou tlačítek jsou vytvořeny jako makro v programovacím jazyku Visual Basic for Application (VBA), který je standardní součástí kancelářského balíku MS Office. Pokud uživatel nepovolí spouštění maker v tomto dokumentu, potom nebudou tlačítka funkční. Dotazník samotný bude ale stále použitelný, protože k jeho vyhodnocování jsou použity jen běžné funkce programu MS Excel.

Vzniklý metodologický rámec je poměrně obecný, což je dáno šířkou zpracovávaného tématu. Pro vytvoření metodologického rámce, který by dokázal dát jasnou odpověď, zda se u nějakého zájemce BYOD skutečně vyplatí, by bylo nutné podrobně zkoumat firmu daného zájemce a znát jeho konkrétní možnosti a představy. Takovýto úzce zaměřený rámec by ale pak nemusel být univerzálně použitelný. Rámec, který zde vznikl, si dává za cíl pomoci zájemci zorientovat se v problematice užívání vlastních zařízení zaměstnanců ve firemním prostředí a dát mu informaci o tom, jestli by toto téma pro něj mohlo být zajímavé.

Kapitola 7

Použití metodologického rámce na ukázkovém příkladu

Použití vzniklého rámce je zde ukázáno na dvou fiktivních firmách, které se zajímají o možnost využití BYODu ve svém provozu.

7.1 Ukázkový příklad 1 - ExpertBank

Fiktivní banka operující v několika evropských státech, zaměstnává 10 000 lidí a specializuje se na bankovní služby pro fyzické osoby a podnikatelské subjekty. V každé ze zemí, kde operuje má celou řadu poboček rozprostřenou ve větších i menších městech. Část zaměstnanců běžně pracuje i mimo svá pracoviště, často jde o obchodní zástupce jednající s klienty.

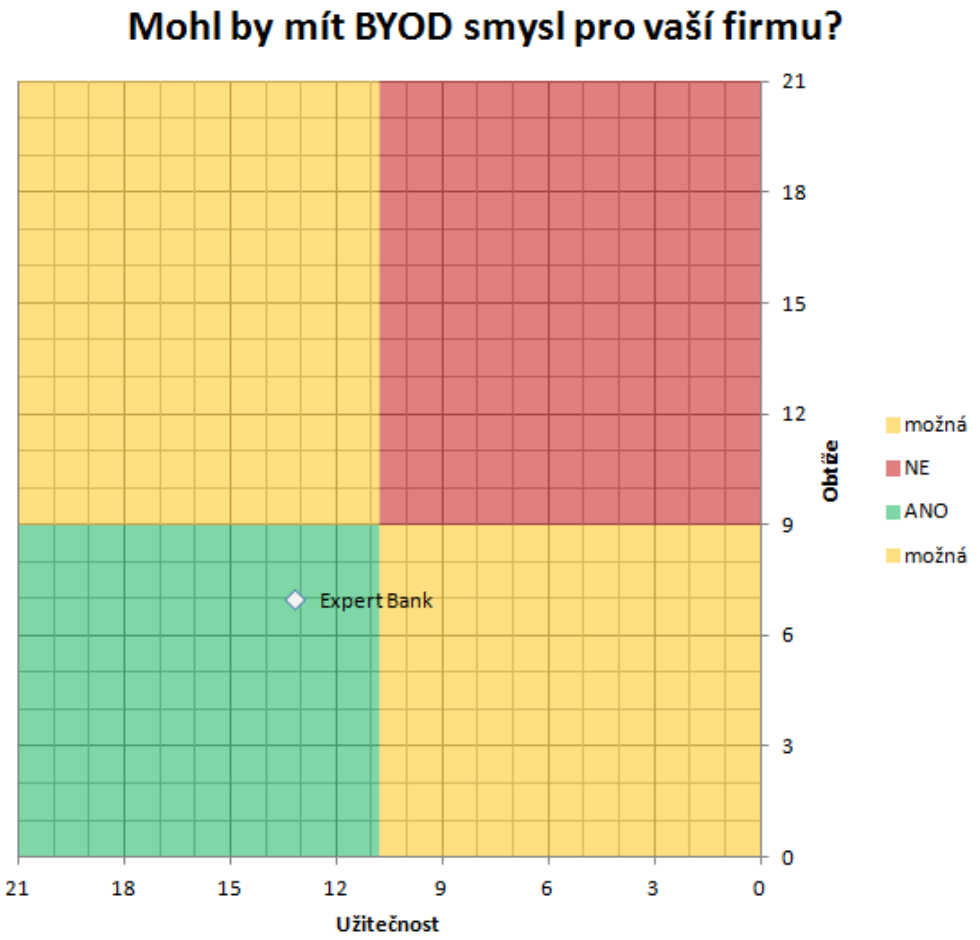
Firemní mobilní zařízení (především notebooky a tablety) banka obnovuje přibližně každé 4 roky a pro jejich správu užívá nástroje MDM. Banka klade veliký důraz na informační bezpečnost. Vedení banky by rádo využilo BYOD pro zvýšení produktivity a mobility svých zaměstnanců.

Výsledek:

Z dotazníku vyšlo, že pro tuto banku by zavedení firemního BYOD programu mohlo mít velký význam (viz diagram 7.1), především díky ochotě investovat do změny od které si slibují zlepšení svého podnikání. Užitečná je také předchozí zkušenost s nástroji na správu mobilních zařízení. Pro tuto banku má tedy rozhodně smysl, aby se BYODem zabývala více do hloubky a zvažovala konkrétní možnosti jeho realizace. Vyplněný dotazník viz příloha A.

7.2 Ukázkový příklad 2 - SiliconCzech s.r.o.

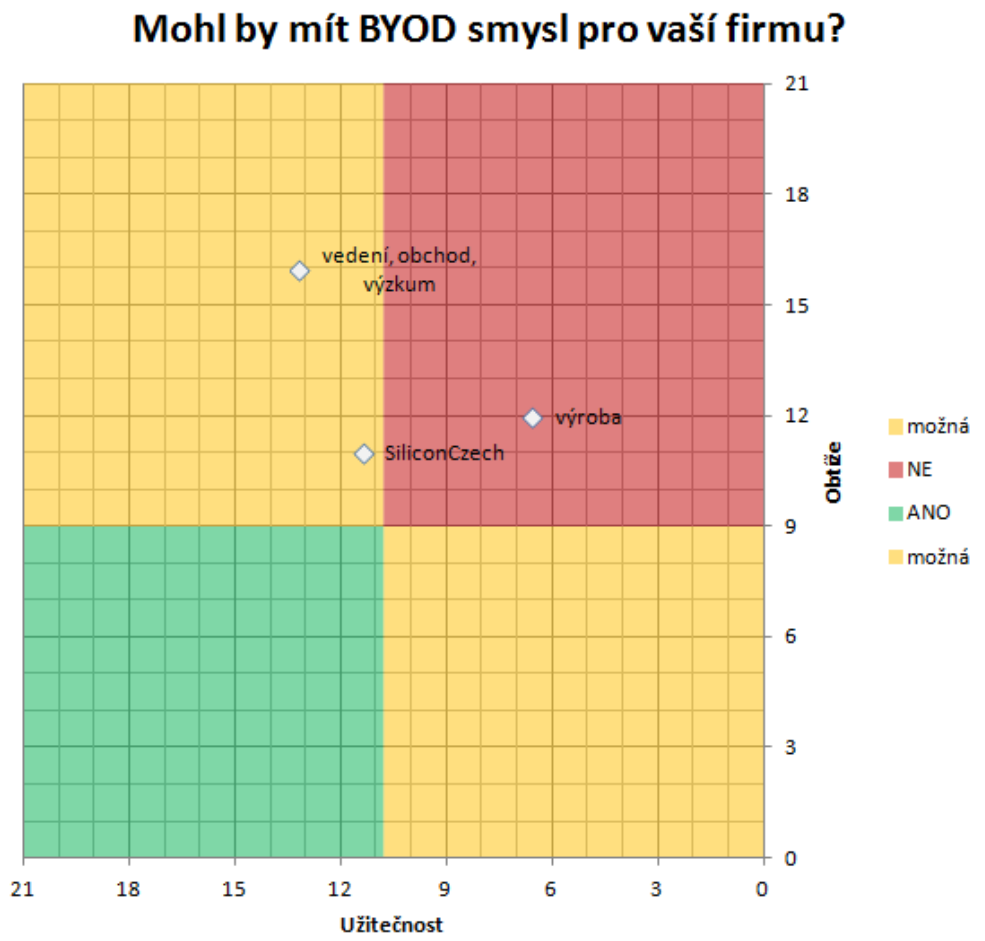
Fiktivní český výrobce mikrokontrolerů a elektronických součástek, zaměstnávající 500 lidí, vlastní několik budov, ve kterých má svou obchodní centrálu,



Obrázek 7.1: Zkoumaná banka se podle vyplněného dotazníku umístila do zeleného kvadrantu.

výrobní továrnu a výzkumné oddělení. Kromě standardních typů mikrokontrolerů a součástek, také ve svém výzkumném oddělení vyvíjí specializované typy součástek podle požadavků konkrétních zákazníků.

Největší část zaměstnanců pracuje ve výrobě, kde užívají specializované výrobní a měřící nástroje. Firma podle potřeby poskytuje zaměstnancům především z managementu, obchodníkům a lidem z výzkumu firemní mobilní zařízení. Tato zařízení (především notebooky) jsou už ve firmě užívány delší dobu a firma není příliš ochotná investovat do nových zařízení. Firemní management zvažuje podporu BYODu ve své firmě jednak z důvodu, aby vyslyšel dlouhodobé požadavky zaměstnanců na lepší techniku a pak také, aby nemusel zvyšovat současné výdaje na firemní IT a případně dosáhl i úspor.



Obrázek 7.2: Zkoumaná firma se podle vyplněného dotazníku jako celek umístila ve žlutém kvadrantu. Její výrobní část se umístila jasně v červeném kvadrantu.

Výsledek:

Firma se umístila v kvadrantu „Možná“ (viz diagram 7.2), ukazatel užitečnosti ovšem není příliš vysoký, a protože jsou poměrně velké rozdíly ve fungování různých oddělení firmy, vyhodnotíme dotazník znovu zvlášť pro výrobní část firmy a zvlášť pro obchodní, řídící a výzkumnou část firmy. Vyplněný dotazník viz příloha B.

Výrobní část firmy: Z diagramu jasně vyplývá, že pro výrobní část firmy nemá BYOD příliš velký smysl. Míra užitečnosti je totiž poměrně malá a velmi pravděpodobně by nestála za obtíže s tím spojené. Vyplněný dotazník viz příloha C.

Management, obchodníci a výzkum: Druhá část firmy by z podpory BYODu mohla mít užitek. Ovšem jeho realizace by byla vcelku náročná. Po-

kud by tedy firma chtěla BYOD pro část svých zaměstnanců zavést, je velká šance, že by ve výsledku vzniklé obtíže převážily význam možného užitku. Vyplněný dotazník viz příloha D.

Kapitola 8

Celkové shrnutí tématu

V této kapitole budou stručně shrnuty důležité body této práce.

8.1 Trend

V posledních letech řada firem řešila otázky zaměstnanecké mobility a konzumerizace IT. Mezi zaměstnanci je zájem nebýt upoután na jedno pevně dané místo, z nějž jediného je možné vykonávat úkony související s jejich prací. Ačkoliv to neznamená, že by se snad většina chtěla stát plně mobilními zaměstnanci, mít k dispozici určitou flexibilitu je žádané. A mobilní zařízení určená původně pro běžné spotřebitele jsou ve firemním prostředí zaměstnanci také poměrně žádanou věcí. Přinejmenším je tu sklon zaměstnanců upřednostňovat populární spotřebitelská mobilní zařízení před omezenými prostředky poskytovanými jejich zaměstnavateli. To jen zvyšuje zájem o BYOD a vytváří to další tlak na společnosti, aby se těmito tématy zabývaly. Je zřejmé, že zaměstnanecká mobilita, konzumerizace IT i BYOD budou důležitými tématy i v následujících letech.

8.2 Výhody

Největšími výhodami plynoucími z podpory mobility a konzumerizace IT, především je-li to realizováno povolením BYODu jsou vyšší produktivita zaměstnanců a jejich spokojenost. Zaměstnanci získávají nové možnosti, jak lépe vykonávat svou práci, z čehož těží i sám zaměstnavatel. Aby se výhody co nejvíce projevily, je třeba je správně podporovat a využít možností na zlepšení vnitrofiremního fungování, které BYOD přináší. Bez cíleného rozvoje těchto nových možností budou výhody BYODu vyplývat pouze z kreativity zaměstnanců fungujících v nezměněném pracovním prostředí.

8.3 Náklady

BYOD na jednu stranu znamená, že firma může omezit náklady na nákup a obnovu firemních zařízení a při tom využívat výhod nejmodernějších mobilních zařízení, na druhou stranu ale musí řešit nové požadavky na správu zaměstnaneckých zařízení a zajištění potřebné úrovně bezpečnosti a podpory. Na úspory, přinejmenším v počátcích zavádění BYODu často nemusí dojít. Pro vytvoření úspěšného BYOD programu je zpravidla potřeba důkladné plánování, školení zaměstnanců i nákup softwaru na správu a zabezpečení mobilních zařízení. Poskytovatelé softwarových řešení mohou pomoci přípravou firemního BYODu, což zvyšuje šanci, že firemní náklady budou vynaloženy účelně. V každém případě je lepší vynaložit náklady na kvalitní BYOD program, než pak nést náklady za jeho nefungování.

8.4 Bezpečnost

Zaměstnanecká zařízení ve firemní síti bezesporu představují potenciální nebezpečí pro bezpečnost firemních dat. Naštěstí na tuto hrozbu existuje řada různých řešení, která mohou vést ke zmírnění rizik. Zavedení těchto bezpečnostních řešení sice vyžaduje vynaložení často nemalých nákladů a také důsledné dodržování bezpečnostních pravidel, na druhou stranu ale počítačové viry ani podvodníci se neomezují jen na soukromá zařízení a firmy tak jako tak musí otázku bezpečnosti řešit. Požadavky na bezpečnost jsou u každé firmy trochu jiné. Je tedy nutné, aby si každá firma identifikovala klíčové oblasti své bezpečnosti a podle toho volila odpovídající zabezpečení. Některá rizika ovšem nejde nikdy zcela eliminovat, takže snaha investovat do všech myslitelných opatření muže být zbytečně drahá a přinášet více komplikací než užitku.

8.5 Podpůrný SW

Od doby, kdy se BYOD začal objevovat ve firmách, došlo k velkému posunu v oblasti nástrojů na jeho správu. O zavedení BYODu tedy nyní mohou uvažovat i firmy, pro které byly dřívější nástroje na správu mobilních zařízení nedostatečné. Firmy nabízející svá řešení zaměstnanecké mobility mohou zájemci pomoci s vytvořením dobrého BYOD programu. Protože ale produkty některých dodavatelů mohou být v určitých oblastech rozvinutější než v jiných, je důležité, aby případný zájemce už od začátku měl přibližnou představu, jaké oblasti jsou pro něj důležité, a vybral podle toho dodavatele. Obecně tedy nelze doporučit jednoho konkrétního dodavatele či software. Tato práce čtenáři přináší obecný přehled o tom, jaké typy softwaru existují. To čtenáři pomůže udělat si lepší představu o tom, co by se jemu konkrétně mohlo více hodit.

Závěr

V rámci této práce vznikla analýza problematiky označované pojmem BYOD, tedy užívání soukromých mobilních zařízení zaměstnanců ve firemním prostředí. Čtenáře seznamuje s trendy a významnými milníky, které stály na počátku a formovaly další vývoj této problematiky. Dále jsou zde popsány základní pojmy, jmenovitě: zaměstnanecká mobilita, konzumerizace IT a samotný BYOD. V následujících částech práce je pak čtenář seznámen s konkrétními aspekty těchto základních pojmů. Je zřejmé, že tyto pojmy mají zásadní vliv na fungování firem a i v dohledné budoucnosti se jimi budou firmy muset zabývat.

Zaměstnanecká mobilita dává firmám nové možnosti fungování a minimálně pro některé firmy bude nutným krokem pro umožnění jejich dalšího rozvoje. Firemní IT vybavení je již dnes významně ovlivněno trendem konzumerizace IT a firmy i v následujících letech budou tlačeny svými zaměstnanci, aby na tento trend nějak reagovaly. Spontánní reakcí na konzumerizaci IT se ukázal být BYOD. Při zkoumání této problematiky bylo zjištěno, že BYOD je natolik silným jevem, že většina společností raději hledá způsoby, jak se mu přizpůsobit, než aby se mu pokoušely bránit.

Vytvoření úspěšného firemního BYOD programu je ovšem velmi náročný úkol. Vedle prospěchu, který to může přinést, tu jsou i potíže a rizika, se kterými je třeba se vypořádat. Tyto potíže přesahují oblast informačních technologií a zasahují do fungování zaměstnanců i celé firmy. Důležitým zjištěním je, že pokoušet se plně eliminovat všechna rizika, jež s BYODem přicházejí, by bylo nadlidským úkolem. Je tedy třeba zhodnotit si závažnost a pravděpodobnost jednotlivých rizik, přijmout rozumnou míru opatření a akceptovat skutečnost, že jisté riziko bude vždy existovat.

Na řešení rizik a potíží týkajících se BYODu ale i maximalizování možného užitku, se specializuje řada firem. Ty nabízejí případným zájemcům jak softwarové nástroje na správu zaměstnanecké mobility, tak často i své zkušenosti s vytvářením vhodných firemních strategií. Čtenář z této práce získá základní představu o těchto firmách i typech produktů, které nabízejí.

K této bakalářské práci vzniknul i interaktivní dotazník, jehož vyplněním se firma může dozvědět, nakolik by jí mohl BYOD přinést užitek a zda-li tedy pro ní má smysl se jím blíže zabývat. Použití dotazníku je ukázáno na příkladech dvou jednoduchých fiktivních firem.

Stanovené cíle této práce se mi podařilo splnit. V budoucnu by mohlo být na tuto práci navázáno analýzou dalších přístupů k řešení zaměstnanecké mobility, jako je třeba povolení užívání firemních zařízení pro soukromé účely zaměstnanců. Z analýzy by mělo vyplynout, pro jaké firmy a v jakých situacích jsou tyto další přístupy vhodnější než podpora BYODu.

Věřím, že má práce bude sloužit jako užitečný a obsažný úvod do problematiky BYODu pro všechny zaměstnavatele i zaměstnance, kteří o tomto zatím příliš neslyšeli, nebo mají pouze kusé informace.

Literatura

[1] SPENCE, E.: For The Record, Apple's Newton Was Not The First PDA. [online], Březen 2012, [cit. 2015-1-13]. Dostupné z: http://www.forbes.com/sites/ewanspence/2012/06/03/for-the-record-apples-newton-was-not-the-first-pda/

[2] BEAL, V.: PDA - personal digital assistant. [online], [cit. 2015-1-13]. Dostupné z: http://www.webopedia.com/TERM/P/PDA.html

[3] YAROW, J.: The iPhone was revealed eight years ago today — look how terrible the first one was. [online], Leden 2015, [cit. 2015-1-13]. Dostupné z: http://business.financialpost.com/2015/01/09/the-iphone-was-revealed-eight-years-ago-today-look-how-terrible-the-first-one-was/

[4] YAROW, J.: Look How Unbelievably Awful The First iPhone Was. [online], Prosinec 2013, [cit. 2015-1-13]. Dostupné z: http://www.businessinsider.com/the-first-iphone-2013-12?op=1

[5] SMRČEK, J.: Google Android – velký výlet do historie. [online], Březen 2011, [cit. 2015-1-13]. Dostupné z: http://www.cnews.cz/google-android-velky-vylet-do-historie

[6] RIESEL, M. S.: Review HTC Dream (T-Mobile G1) novo celular da Google com Android. [online], Únor 2009, [cit. 2015-1-13]. Dostupné z: http://www.riesel.com.br/tecnologia/review-htc-dream-t-mobile-g1/

[7] JANEČEK, V.: Cesta do pravěku: jak se zrodil tablet. [online], Srpen 2010, [cit. 2015-1-13]. Dostupné z: http://www.zive.cz/clanky/cesta-do-praveku-jak-se-zrodil-tablet/sc-3-a-153583/

[8] IDC: Worldwide Tablet Growth Expected to Slow to 7.2% in 2014 Along With First Year of iPad Decline, According to IDC. [on-

line], Listopad 2014, [cit. 2015-1-13]. Dostupné z: http://www.idc.com/getdoc.jsp?containerId=prUS25267314

[9] HARKINS, M.: Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices. [online], [cit. 2015-1-13]. Dostupné z: http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264

[10] LAIRD, J.: A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. [online], Listopad 2014, [cit. 2015-1-13]. Dostupné z: http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore

[11] COSGROVE, T.; aj.: Magic Quadrant for Enterprise Mobility Management Suites. [online], Červen 2014, [cit. 2015-1-13]. Dostupné z: http://www.gartner.com/technology/reprints.do?id=1-1UWW5XX&ct=140603&st=sb

[12] BEAL, V.: teleworking. [online], [cit. 2015-1-13]. Dostupné z: http://www.webopedia.com/TERM/T/teleworking.html

[13] MARTOCH, M.: Teleworking – práce přes Internet přináší úspory nákladů. [online], Leden 2009, [cit. 2015-1-13]. Dostupné z: http://www.itbiz.cz/teleworking-prace-pres-internet

[14] FONTANA, J.: Mobility; it's not a device, it's an IT architecture. [online], Srpen 2012, [cit. 2015-1-13]. Dostupné z: http://www.zdnet.com/article/mobility-its-not-a-device-its-an-it-architecture/

[15] BEAL, V.: consumerization of IT. [online], [cit. 2015-1-13]. Dostupné z: http://www.webopedia.com/TERM/C/consumerization_of_it.html

[16] Gartner: Bring Your Own Device (BYOD). [online], [cit. 2015-1-18]. Dostupné z: http://www.gartner.com/it-glossary/bring-your-own-device-byod

[17] Intel: Insights on the Current State of BYOD. [online], Říjen 2012, [cit. 2015-1-18]. Dostupné z: http://www.intel.com/content/www/us/en/mobile-computing/consumerization-enterprise-byod-peer-research-paper.html

[18] MASTNÝ, F.: *Vliv využívání mobilních zařízení v činnosti podniku.* Diplomová práce, České vysoké učení technické v Praze, Fakulta elektrotechnická, 2014, [cit. 2015-1-18].

[19] BENDER, A.: BYOD vs CYOD: Bring or choose your own device? [online], Duben 2013, [cit. 2015-1-18]. Dostupné z:

http://www.computerworld.com.au/article/456899/byod_vs_cyod_bring_choose_your_own_device_/

[20] Adrian DRURY, R. A.: BYOD: an emerging market trend in more ways than one. Technická zpráva, Ovum Ltd., 2012, [cit. 2015-1-18]. Dostupné z: http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf

[21] HAMMOND, T.: Research: BYOD booming with 74% using or planning to use. [online], Leden 2015, [cit. 2015-1-18]. Dostupné z: http://www.techproresearch.com/article/research-byod-booming-with-74-using-or-planning-to-use/

[22] HAMMOND, T.: Research: 74 percent using or adopting BYOD. [online], Leden 2015, [cit. 2015-1-18]. Dostupné z: http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/

[23] ČÍŽEK, J.: BYOD je pro české firmy stále exotika. [online], Leden 2014, [cit. 2015-1-20]. Dostupné z: http://www.zive.cz/bleskovky/byod-je-pro-ceske-firmy-stale-exotika/sc-4-a-172168/

[24] TWILLEY, R.: With BYOD, Employee Productivity Surges. [online], Duben 2013, [cit. 2015-1-21]. Dostupné z: http://www.forbes.com/sites/centurylink/2013/04/26/byod-employees-bring-their-own-efficiency-to-work/

[25] BALDWIN, C.: BYOD increases productivity, but IT departments need to be prepared. [online], Srpen 2012, [cit. 2015-1-21]. Dostupné z: http://www.computerweekly.com/news/2240160757/BYOD-increases-productivity-but-IT-departments-need-to-be-prepared

[26] Forrester: Forrester - The Total Economic Impact of IBM Managed Mobility for BYOD. Technická zpráva, IBM, Květen 2013, [cit. 2015-1-21]. Dostupné z: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=AZW03003USEN#loaded

[27] Businessworld.cz: Tablety: revoluce v produktivitě. [online], Leden 2015, [cit. 2015-1-24]. Dostupné z: http://businessworld.cz/mobilita/tablety-revoluce-v-produktivite-12087

[28] KANESHIGE, T.: CIOs Need to Push BYOD Policies to Lure Millennials. [online], Říjen 2013, [cit. 2015-1-21]. Dostupné z: http://www.cio.com/article/2383561/byod/cios-need-to-push-byod-policies-to-lure-millennials.html

[29] CompTIA: Generational Research on Technology and its Impact in the Workplace. Technická zpráva, CompTIA, 2013, [cit. 2015-1-20]. Dostupné z: http://www.unify.com/~/media/internet-2012/documents/report/CompTIA-Generational-Study.pdf

[30] MEDCALF, R.; aj.: The Financial Impact of BYOD - A Model of BYOD's Benefits to Global Companies. Technická zpráva, Cisco IBSG, 2013, [cit. 2015-1-25]. Dostupné z: http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf

[31] KANESHIGE, T.: Killing the Help Desk Softly - or Blowing It Up. [online], Březen 2013, [cit. 2015-1-24]. Dostupné z: http://www.cio.com/article/2387321/byod/killing-the-help-desk-softly---or-blowing-it-up.html

[32] SARAN, C.: Forrester: The costs and benefits of BYOD. [online], Červen 2012, [cit. 2015-1-25]. Dostupné z: http://www.computerweekly.com/news/2240158445/Forrester-The-costs-and-benefits-of-BYOD

[33] KERNER, S. M.: Cisco Reduces Support Costs with BYOD. [online], Květen 2013, [cit. 2015-1-25]. Dostupné z: http://www.enterprisenetworkingplanet.com/netsysm/cisco-saves-support-costs-with-byod.html

[34] KANESHIGE, T.: BYOD: If You Think You're Saving Money, Think Again. [online], Duben 2012, [cit. 2015-1-25]. Dostupné z: http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html

[35] HERTZ, I.: 3 BYOD Costs Companies Often Overlook. [online], Duben 2013, [cit. 2015-4-5]. Dostupné z: http://www.techopedia.com/2/29282/it-business/it-management/3-byod-costs-companies-often-overlook

[36] MILLS, H.: Mobile Device Management vs. Mobile Application Management: The Big Fight Continues. [online], Listopad 2013, [cit. 2015-4-5]. Dostupné z: http://www.techopedia.com/2/29672/it-business/it-management/mobile-device-management-vs-mobile-application-management-the-big-fight-continues

[37] JANSSEN, C.: Advanced Business Application Programming Workbench (ABAP Workbench). [online], [cit. 2015-4-5]. Dostupné z: http://www.techopedia.com/definition/25322/advanced-business-application-programming-workbench-abap

[38] KANESHIGE, T.: Dual-Persona Smartphones Not a BYOD Panacea. [online], Květen 2013, [cit. 2015-4-5]. Dostupné z:

http://www.cio.com/article/2385747/byod/dual-persona-smartphones-not-a-byod-panacea.html

[39] KANESHIGE, T.: BYOD Security Concerns: Does IT Protest Too Much? [online], Červen 2012, [cit. 2015-4-5]. Dostupné z: http://www.cio.com/article/2394572/byod/byod-security-concerns--does-it-protest-too-much-.html

[40] KANESHIGE, T.: BYOD's Phone Number Problem. [online], Květen 2012, [cit. 2015-4-5]. Dostupné z: http://www.cio.com/article/2395549/byod/byod-s-phone-number-problem.html

[41] VERNER, M.: How to Confront Today's Bring Your Own Device Challenges. [online], Září 2013, [cit. 2015-4-5]. Dostupné z: http://www.utgsolutions.com/how-to-confront-todays-bring-your-own-device-challenges/

[42] BRAUE, D.: Aussie workers bypassing IT organisations for BYOD: survey. [online], 2013, [cit. 2015-4-5]. Dostupné z: http://www.govtechreview.com.au/aussie-workers-bypassing-it-organisations-for-byod-survey/

[43] SHACKLETT, M.: 10 BYOD concerns that go beyond security issues. [online], Srpen 2012, [cit. 2015-4-5]. Dostupné z: http://www.techrepublic.com/blog/10-things/10-byod-concerns-that-go-beyond-security-issues/

[44] KasperskyLab: Global Corporate IT Security Risks: 2013. Technická zpráva, Cisco IBSG, Květen 2013, [cit. 2015-3-4]. Dostupné z: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[45] JANSSEN, C.: End Node. [online], [cit. 2015-3-4]. Dostupné z: http://www.techopedia.com/definition/26122/end-node

[46] JANSSEN, C.: Malicious Software (Malware). [online], [cit. 2015-3-5]. Dostupné z: http://www.techopedia.com/definition/4015/malicious-software-malware

[47] JANSSEN, C.: Mobile Malware. [online], [cit. 2015-3-5]. Dostupné z: http://www.techopedia.com/definition/29477/mobile-malware

[48] Kingsley-Hughes, A.: Top 10 banned apps on iOS and Android BYOD devices. [online], Červen 2013, [cit. 2015-3-6]. Dostupné z: http://www.zdnet.com/article/top-10-banned-apps-on-ios-and-android-byod-devices/

[49] Apple: App Store Distribution. [online], Duben 2015, [cit. 2015-4-3]. Dostupné z: https://developer.apple.com/support/appstore/

[50] GooglePlayStore: Platform Versions. [online], Květen 2015, [cit. 2015-4-3]. Dostupné z: https://developer.android.com/about/dashboards/index.html

[51] Gartner: Gartner Says Smartphone Sales Surpassed One Billion Units in 2014. [online], Březen 2015, [cit. 2015-4-3]. Dostupné z: http://www.gartner.com/newsroom/id/2996817

[52] PETERKOVÁ, M.: Syndrom vyhoření – úvod. [online], [cit. 2015-3-24]. Dostupné z: http://www.syndrom-vyhoreni.psychoweb.cz/

[53] ROUSE, M.: mobile device management (MDM). [online], Červen 2013, [cit. 2015-4-21]. Dostupné z: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[54] ROUSE, M.: mobile application management (MAM). [online], Červen 2014, [cit. 2015-4-21]. Dostupné z: http://searchconsumerization.techtarget.com/definition/mobile-application-management

[55] ROUSE, M.: mobile content management. [online], Duben 2014, [cit. 2015-4-21]. Dostupné z: http://searchconsumerization.techtarget.com/definition/mobile-content-management

Příloha **A**

Vyplněný dotazník

Ukázka vyplněného dotazníku pro fiktivní firmu Expert Bank - celá firma:

1. **Jak moc ve vašem podniku využívají zaměstnanci ke své práci výpočetní techniku?**

   c) Výpočetní technika je klíčovým nástrojem činnosti zaměstnanců.

2. **Jak často se musejí vaši zaměstnanci přesouvat kvůli pracovním povinnostem na různá místa mimo budovu, ve které obvykle pracují?**

   c) Zaměstnanci alespoň jednoho oddělení běžně vykonávají část své práce mimo svá stálá pracoviště.

3. **Vyžaduje si pracovní náplň vašich zaměstnanců užívání nějakých mobilních zařízení?**

   b) Někteří zaměstnanci k plnění svých povinností potřebují mít k dispozici i mobilní zařízení.

4. **Jsou vaši zaměstnanci spokojeni s výpočetní technikou, kterou mají k dispozici?**

   b) Technika, kterou mají k dispozici, převážně odpovídá jejich potřebám, ale s jejím užíváním nejsou zcela spokojeni.

5. **Objevuje se mezi vašimi zaměstnanci tendence pomáhat si při práci jejich soukromými mobilními zařízeními?**

   b) Mezi zaměstnanci je určitý zájem mít možnost užívat k pracovním účelům i svá soukromá zařízení.

6. **Mělo by pro vaši firmu smysl umožnit zaměstnancům být více časově a místně flexibilní?**

   a) Ano

7. **Jak často se stává, že se zaměstnancem užívané firemní mobilní zařízení poškodí/ztratí?**

   b) Středně často

8. **Má vaše firma potřebu poskytovat přístup k firemním IT zdrojům i osobám, jež nejsou stálými zaměstnanci?**

   c) Převážně ne.

9. **Jak moc jsou pro vaši firmu důležití zaměstnanci patřící do tzv. generace Y?**

   b) Takovíto zaměstnanci jsou vítaným doplňkem k pracovnímu kolektivu.

10. **Máte sjednané poskytování a servis firemních zařízení u dodavatele, který je schopen poskytnout vašim zaměstnancům taková mobilní zařízení, která co nejvíce odpovídají jejich potřebám a touhám?**

    b) Ne

11. **Jak rozsáhle chcete BYOD zapojit do fungování vaší firmy?**

    c) Rádi bychom s využitím BYOD programu provedli změny ve fungování různých firemních oddělení, abychom dosáhli konkrétních cílů.

12. **Jak moc hodláte zapojit do přípravy BYOD programu své zaměstnance napříč různými odděleními?**

    a) Zajistíme maximální potřebnou součinnost jednotlivých oddělení, aby mohlo být dosaženo nejlepšího výsledku.

13. **Jak moc jste ochotni investovat do nové IT infrastruktury?**

    a) Poskytneme dostatečně velké množství peněz, aby bylo možné nakoupit veškeré potřebné vybavení.

14. **Využívá váš podnik nějaké IT technologie, které by se daly využít při zavádění BYOD programu?**

    a) Ano

15. **Jak důležité je pro vaše podnikání zajištění bezpečnosti firemních dat?**

    a) Kriticky důležité

16. **Jak moc důležitá pro práci vašich zaměstnanců je spolehlivost a dostupnost mobilních zařízení?**

    b) Nedostupnost zaměstnancova zařízení není stěžejní překážkou a obvykle bývá dostatek času tento stav napravit.

17. **Jak moc jste ochotni přispívat zaměstnancům na jejich BYOD zařízení?**

    a) V minimální nutné míře, jak vyžaduje zákon.

18. **Mohlo by vlivem firemní podpory BYODu, u vašich zaměstnanců častěji docházet k jejich přepracovanosti?**

    b) Ne, povaha povinností a pracovního prostředí nesvádí naše zaměstnance k tomu, aby pravidelně věnovali pracovním povinnostem i svůj volný čas.

Příloha **B**

Vyplněný dotazník

Ukázka vyplněného dotazníku pro fiktivní firmu SiliconCzech s.r.o. - celá firma:

1. **1. Jak moc ve vašem podniku využívají zaměstnanci ke své práci výpočetní techniku?**

   b) Zaměstnanci v alespoň některých odděleních mají počítače jako jeden z nástrojů, které užívají k práci.

2. **Jak často se musejí vaši zaměstnanci přesouvat kvůli pracovním povinnostem na různá místa mimo budovu, ve které obvykle pracují?**

   c) Zaměstnanci alespoň jednoho oddělení běžně vykonávají část své práce mimo svá stálá pracoviště.

3. **Vyžaduje si pracovní náplň vašich zaměstnanců užívání nějakých mobilních zařízení?**

   a) Ne, valná většina zaměstnanců ke své práci mobilní zařízení nepotřebuje.

4. **Jsou vaši zaměstnanci spokojeni s výpočetní technikou, kterou mají k dispozici?**

   c) Technika, kterou mají k dispozici, jim umožňuje splnit pracovní povinnosti, ale nepovažují ji za zcela optimální či dostatečně výkonnou.

5. **Objevuje se mezi vašimi zaměstnanci tendence pomáhat si při práci jejich soukromými mobilními zařízeními?**

   c) Zaměstnanci mají značný zájem užívat k práci i svá mobilní zařízení.

6. **Mělo by pro vaší firmu smysl umožnit zaměstnancům být více časově a místně flexibilní?**

   b) Ne

7. **Jak často se stává, že se zaměstnancem užívané firemní mobilní zařízení poškodí/ztratí?**

   b) Středně často

8. **Má vaše firma potřebu poskytovat přístup k firemním IT zdrojům i osobám, jež nejsou stálými zaměstnanci?**

   b) Ano, příležitostně.

9. **Jak moc jsou pro vaši firmu důležití zaměstnanci patřící do tzv. generace Y?**

   b) Takovíto zaměstnanci jsou vítaným doplňkem k pracovnímu kolektivu.

10. **Máte sjednané poskytování a servis firemních zařízení u dodavatele, který je schopen poskytnout vašim zaměstnancům taková mobilní zařízení, která co nejvíce odpovídají jejich potřebám a touhám?**

    b) Ne

11. **Jak rozsáhle chcete BYOD zapojit do fungování vaší firmy?**

    b) Budeme provádět jen menší změny ve fungování jednotlivých firemních oddělení, abychom umožnili využití BYODu, neplánujeme žádné zásadní změny fungování.

12. **Jak moc hodláte zapojit do přípravy BYOD programu své zaměstnance napříč různými odděleními?**

    b) Firemní IT oddělení bude aktivně spolupracovat jen s právním oddělením a oddělením lidských zdrojů, ostatní oddělení budou do tvorby zapojeny jen okrajově.

13. **Jak moc jste ochotni investovat do nové IT infrastruktury?**

    c) Nemáme v úmyslu zvyšovat výdaje na IT.

14. **Využívá váš podnik nějaké IT technologie, které by se daly využít při zavádění BYOD programu?**

    b) Ne

15. **Jak důležité je pro vaše podnikání zajištění bezpečnosti firemních dat?**

    b) Důležité

16. **Jak moc důležitá pro práci vašich zaměstnanců je spolehlivost a dostupnost mobilních zařízení?**

    c) Mobilní zařízení nejsou pro práci zaměstnance nutné a zaměstnanec může plnit své povinnosti i bez nich.

17. **Jak moc jste ochotni přispívat zaměstnancům na jejich BYOD zařízení?**

    a) V minimální nutné míře, jak vyžaduje zákon.

18. **Mohlo by vlivem firemní podpory BYODu, u vašich zaměstnanců častěji docházet k jejich přepracovanosti?**

    b) Ne, povaha povinností a pracovního prostředí nesvádí naše zaměstnance k tomu, aby pravidelně věnovali pracovním povinnostem i svůj volný čas.

Příloha C

Vyplněný dotazník

Ukázka vyplněného dotazníku pro fiktivní firmu SiliconCzech s.r.o. - výrobní část:

1. **Jak moc ve vašem podniku využívají zaměstnanci ke své práci výpočetní techniku?**

   b) Zaměstnanci v alespoň některých odděleních mají počítače jako jeden z nástrojů, které užívají k práci.

2. **Jak často se musejí vaši zaměstnanci přesouvat kvůli pracovním povinnostem na různá místa mimo budovu, ve které obvykle pracují?**

   b) Určitá část zaměstnanců musí alespoň párkrát měsíčně z pracovních důvodů cestovat i mimo své běžné pracoviště.

3. **Vyžaduje si pracovní náplň vašich zaměstnanců užívání nějakých mobilních zařízení?**

   a) Ne, valná většina zaměstnanců ke své práci mobilní zařízení nepotřebuje.

4. **Jsou vaši zaměstnanci spokojeni s výpočetní technikou, kterou mají k dispozici?**

   b) Technika, kterou mají k dispozici, převážně odpovídá jejich potřebám, ale s jejím užíváním nejsou zcela spokojeni.

5. **Objevuje se mezi vašimi zaměstnanci tendence pomáhat si při práci jejich soukromými mobilními zařízeními?**

   a) Mezi zaměstnanci není žádná větší touha užívat k práci svá vlastní mobilní zařízení.

6. **Mělo by pro vaší firmu smysl umožnit zaměstnancům být více časově a místně flexibilní?**

   b) Ne

7. **Jak často se stává, že se zaměstnancem užívané firemní mobilní zařízení poškodí/ztratí?**

   a) Málo často

8. **Má vaše firma potřebu poskytovat přístup k firemním IT zdrojům i osobám, jež nejsou stálými zaměstnanci?**

   c) Převážně ne.

9. **Jak moc jsou pro vaši firmu důležití zaměstnanci patřící do tzv. generace Y?**

   c) Nejedná se o rozhodující faktor.

10. **Máte sjednané poskytování a servis firemních zařízení u dodavatele, který je schopen poskytnout vašim zaměstnancům taková mobilní zařízení, která co nejvíce odpovídají jejich potřebám a touhám?**

    b) Ne

11. **Jak rozsáhle chcete BYOD zapojit do fungování vaší firmy?**

    a) Vycházíme vstříc hlavně našim zaměstnancům, nemáme v plánu provádět žádné změny ve fungování jednotlivých firemních oddělení.

12. **Jak moc hodláte zapojit do přípravy BYOD programu své zaměstnance napříč různými odděleními?**

    b) Firemní IT oddělení bude aktivně spolupracovat jen s právním oddělením a oddělením lidských zdrojů, ostatní oddělení budou do tvorby zapojeny jen okrajově.

13. **Jak moc jste ochotni investovat do nové IT infrastruktury?**

    c) Nemáme v úmyslu zvyšovat výdaje na IT.

14. **Využívá váš podnik nějaké IT technologie, které by se daly využít při zavádění BYOD programu?**

    b) Ne

15. **Jak důležité je pro vaše podnikání zajištění bezpečnosti firemních dat?**

c) Méně důležité.

16. **Jak moc důležitá pro práci vašich zaměstnanců je spolehlivost a dostupnost mobilních zařízení?**

    a) Zaměstnanci nemohou naplno plnit své povinnosti, pokud je mobilní zařízení nespolehlivé a není možné jeho okamžité nahrazení.

17. **Jak moc jste ochotni přispívat zaměstnancům na jejich BYOD zařízení?**

    a) V minimální nutné míře, jak vyžaduje zákon.

18. **Mohlo by vlivem firemní podpory BYODu, u vašich zaměstnanců častěji docházet k jejich přepracovanosti?**

    b) Ne, povaha povinností a pracovního prostředí nesvádí naše zaměstnance k tomu, aby pravidelně věnovali pracovním povinnostem i svůj volný čas.

Příloha D

Vyplněný dotazník

Ukázka vyplněného dotazníku pro fiktivní firmu SiliconCzech s.r.o. - management, obchodníci, výzkum:

1. **Jak moc ve vašem podniku využívají zaměstnanci ke své práci výpočetní techniku?**

   c) Výpočetní technika je klíčovým nástrojem činnosti zaměstnanců.

2. **Jak často se musejí vaši zaměstnanci přesouvat kvůli pracovním povinnostem na různá místa mimo budovu, ve které obvykle pracují?**

   c) Zaměstnanci alespoň jednoho oddělení běžně vykonávají část své práce mimo svá stálá pracoviště.

3. **Vyžaduje si pracovní náplň vašich zaměstnanců užívání nějakých mobilních zařízení?**

   b) Někteří zaměstnanci k plnění svých povinností potřebují mít k dispozici i mobilní zařízení.

4. **Jsou vaši zaměstnanci spokojeni s výpočetní technikou, kterou mají k dispozici?**

   c) Technika, kterou mají k dispozici, jim umožňuje splnit pracovní povinnosti, ale nepovažují ji za zcela optimální či dostatečně výkonnou.

5. **Objevuje se mezi vašimi zaměstnanci tendence pomáhat si při práci jejich soukromými mobilními zařízeními?**

   c) Zaměstnanci mají značný zájem užívat k práci i svá mobilní zařízení.

6. **Mělo by pro vaší firmu smysl umožnit zaměstnancům být více časově a místně flexibilní?**

   b) Ne

7. **Jak často se stává, že se zaměstnancem užívané firemní mobilní zařízení poškodí/ztratí?**

   b) Středně často

8. **Má vaše firma potřebu poskytovat přístup k firemním IT zdrojům i osobám, jež nejsou stálými zaměstnanci?**

   b) Ano, příležitostně.

9. **Jak moc jsou pro vaši firmu důležití zaměstnanci patřící do tzv. generace Y?**

   b) Takovíto zaměstnanci jsou vítaným doplňkem k pracovnímu kolektivu.

10. **Máte sjednané poskytování a servis firemních zařízení u dodavatele, který je schopen poskytnout vašim zaměstnancům taková mobilní zařízení, která co nejvíce odpovídají jejich potřebám a touhám?**

    b) Ne

11. **Jak rozsáhle chcete BYOD zapojit do fungování vaší firmy?**

    b) Budeme provádět jen menší změny ve fungování jednotlivých firemních oddělení, abychom umožnili využití BYODu, neplánujeme žádné zásadní změny fungování.

12. **Jak moc hodláte zapojit do přípravy BYOD programu své zaměstnance napříč různými odděleními?**

    b) Firemní IT oddělení bude aktivně spolupracovat jen s právním oddělením a oddělením lidských zdrojů, ostatní oddělení budou do tvorby zapojeny jen okrajově.

13. **Jak moc jste ochotni investovat do nové IT infrastruktury?**

    c) Nemáme v úmyslu zvyšovat výdaje na IT.

14. **Využívá váš podnik nějaké IT technologie, které by se daly využít při zavádění BYOD programu?**

    b) Ne

15. **Jak důležité je pro vaše podnikání zajištění bezpečnosti firemních dat?**

    a) Kriticky důležité

16. **Jak moc důležitá pro práci vašich zaměstnanců je spolehlivost a dostupnost mobilních zařízení?**

    b) Nedostupnost zaměstnancova zařízení není stěžejní překážkou a obvykle bývá dostatek času tento stav napravit.

17. **Jak moc jste ochotni přispívat zaměstnancům na jejich BYOD zařízení?**

    a) V minimální nutné míře, jak vyžaduje zákon.

18. **Mohlo by vlivem firemní podpory BYODu, u vašich zaměstnanců častěji docházet k jejich přepracovanosti?**

    a) Ano, naši zaměstnanci by mohli mít sklony věnovat až příliš velkou část svého volného času na práci.

Příloha E

Seznam použitých zkratek

API Application Programming Interface

HW Hardware

OS Operační systém

SW Software

Příloha F

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `apl` ..... složka obsahující aplikaci
  - `thesis` ..... složka obsahující zdrojovou formu práce ve formátu LaTeX
- `text` ..... text práce
  - `BP_Trnka_Lukáš_2015.pdf` ..... text práce ve formátu PDF