EKONOMICKÁ UNIVERZITA V BRATISLAVE

FAKULTA HOSPODÁRSKEJ INFORMATIKY

Evidenčné číslo: 103004/I/2014/1541437786

Vybrané problémy bezpečnosti informačného systému v konkrétnom ekonomickom prostredí

Diplomová práca

2014 **Bc. Martin Karas**

EKONOMICKÁ UNIVERZITA V BRATISLAVE

FAKULTA HOSPODÁRSKEJ INFORMATIKY

Vybrané problémy bezpečnosti informačného systému v konkrétnom ekonomickom prostredí

Diplomová práca

Študijný program: Manažérske rozhodovanie a informačné technológie

Študijný odbor: 6258 Kvantitatívne metódy v ekonómii

Školiace pracovisko: Katedra aplikovanej informatiky

Vedúci záverečnej práce: Dr. Ing. Miroslav Hudec

Bratislava 2014 **Bc. Martin Karas**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Martin Karas
Študijný program: Manažérske rozhodovanie a informačné technológie (Jednoodborové štúdium, inžiniersky II. st., externá forma)
Študijný odbor: 3.3.24 Kvantitatívne metódy v ekonómii
Typ záverečnej práce: Inžinierska záverečná práca
Jazyk záverečnej práce: slovenský

Názov: Vybrané problémy bezpečnosti informačného systému v konkrétnom ekonomickom prostredí

Anotácia: Komparatívna analýza vybraných ukazovateľov bezpečnosti s návrhom opatrení na odstránenie nedostatkov v bezpečnosti IS v konkrétnom podniku so zameraním na BYOD

Vedúci: Dr. Ing. Miroslav Hudec
Katedra: KAI FHI - Katedra aplikovanej informatiky FHI

Dátum zadania: 06.11.2011

Dátum schválenia: 21.11.2011

doc. Ing. Gabriela Kristová, CSc.
vedúci katedry

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú prácu som vypracoval samostatne a že som uviedol všetku použitú literatúru.

Dátum: **.....**

Poďakovanie

Chcel by som poďakovať všetkým, ktorí mi pomohli pri spracovaní tejto diplomovej práce. Moje poďakovanie patrí najmä vedúcemu diplomovej práce, Dr. Ing. Miroslavovi Hudecovi a tiež doc. Ing., Anne Kvietkovej, PhD., ktorá viedla moju prácu v prvom roku, za vedenie a cenné pripomienky pri spracovaní témy. Samostatné poďakovanie patrí Ing. Miroslavovi Kažimírovi za ochotu a konzultácie v oblasti korporátnej bezpečnosti. Osobitné poďakovanie za podporu a pomoc patrí mojej manželke Katke.

ABSTRAKT

KARAS, Martin: *Vybrané problémy bezpečnosti informačného systému v konkrétnom ekonomickom prostredí.* – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra aplikovanej informatiky. – Vedúci záverečnej práce: Dr. Ing. Miroslav Hudec. – Bratislava: FHI EU, 2014, 72 strán.

Cieľom záverečnej práce je popísať bezpečnosť informačného systému, postupy a riziká pri jeho tvorbe. Tieto poznatky následne rozpracovať na prehľad bezpečnostných charakteristík a porovnať ich implementáciou prijatej stratégie v konkrétnom prostredí. Práca je rozdelená do 6 kapitol a obsahuje 8 obrázkov a 2 tabuľky. V prvej kapitole popisujeme všeobecné postupy tvorby informačných systémov a bezpečnostné hrozby. V druhej kapitole nasledujú ciele práce a metodiky skúmania. Štvrtá časť popisuje implementáciu bezpečnosti a porovnáva ju so všeobecnými odporúčaniami. V posledných dvoch častiach hodnotíme zistené poznatky z pohľadu adekvátnosti a sumarizujeme dosiahnuté výsledky. Výsledkom riešenia danej problematiky je množina odporúčaní a návrhov na zlepšenie informačnej bezpečnosti.

Kľúčové slová:
Informačná bezpečnosť, IS, informačný systém, BYOD

ABSTRACT

KARAS, Martin: *Selected problems of information system security in a specific economic environment.* – The University of Economics in Bratislava. Faculty of Business Informatics, Department of Applied Informatics. – Final thesis supervisor: Dr. Ing. Miroslav Hudec. – Bratislava: FHI EU, 2014, 72 pages.

The aim of this thesis is to describe the information system security procedures and the risks involved during its development. These findings are then elaborated into an overview of security features and are compared to an implementation strategy in a specific environment. The work is divided into six chapters, contains 8 images and 2 tables. In the first chapter we describe the general procedures of information systems and security threats. In the following sections we define the objectives and methodology review. The fourth section describes implementation of security measures and compares it with general recommendations. In the last two sections we review the discovered knowledge in terms of adequacy and summarize success of our work. The result of the thesis is a set of recommendations and suggestions to improve information security.

Keywords:
Information security, IS, information system, BYOD

OBSAH str.

Zoznam ilustrácií a zoznam tabuliek

Zoznam skratiek

ARPA – Advanced Research Projects Agency

BYOD – Bring your own device

CSI – Computer Science Institute

DHS – Department of Homeland Security

IDS – Intrusion Detection System

IPsec – Internet Protocol security

ISP – Internet Service Provider

IS – informačný systém

ISO – International Organization for Standardization

IT – informačné technológie

ITIL – Information Technology Infrastructure Library

LDAP – Lightweight Directory Access Protocol

NAT – Network Address Translation

NIST – National Institute of Standards and Technology

PKI – Public Key Infrastructure

SSH – Secure SHell

SSO – Single Sign-On

SwA CBK – Secure Software Assurance Common Body of Knowledge

VPN – Virtual Private Network

ÚVOD

Informačná bezpečnosť je v dnešnej dobe na jednej z najvyšších priečok pozornosti pri implementácii systémov spracovávajúcich informácie. Preto sa aj v práci budeme venovať jej rôznym charakteristikám. Vývoj informačných systémov tvorí základ tejto problematiky, tejto oblasti sa však venuje už množstvo kvalitných odborných publikácií a existuje tiež nespočet metodológií a praxou overených postupov. Často opomínaný aspekt bezpečnosti býva samotné prostredie, v ktorom daný systém vzniká a tiež okolie tohto prostredia. Najslabší článok celého reťazca v tomto prostredí a teda najväčšie bezpečnostné riziko, ktoré sa následne prenáša aj na vyvíjaný systém, tvoria ľudia – zamestnanci a ich postoj k bezpečnosti.

V prvej kapitole poskytujeme prehľad vo všeobecnej informačnej bezpečnosti. Popisujeme vnútorné zloženie informačných systémov, prostredie a vzájomné interakcie jeho komponentov v ramci systému a tiež s jeho okolím. Zameriavame sa na bezpečnostné charakteristiky systémových komponentov a spôsobom ako pristupovať k implementácii bezpečnosti. Porovnáme vývoj štandardného a vývoj bezpečného systému. Taktiež priblížime princípy tvorby bezpečného softvéru a softvérového dizajnu. V závere kapitoly popisujeme typické kategórie bezpečnostných hrozieb a softvérových chýb.

V druhej a tretej kapitole si kladieme hlavný cieľ pre zvyšok práce, tj. uskutočniť analýzu firmy a na jej základe poukázať na dobré a slabé stránky v implementácii zabezpečenia konkrétneho prostredia a dopady stávajúcej definície a implementácie použitia osobných zamestnaneckých zariadení v tomto prostredí.

V štvrtej kapitole sa venujeme popisu všetkých významných aspektov bezpečnosti v konkrétnom ekonomickom prostredí z pohľadu súkromných zamestnaneckých zariadení a tiež zhŕňame aplikovateľné časti bezpečnostných odporúčaní do jednotného postupu pri zavádzaní novej implementácie.

V piatej kapitole sa venujeme zhodnoteniu pozorovaní a porovnávame ich so všeobecnými odporúčaniami z druhej kapitoly. Navrhujeme tiež dodatočné riešenia a odporúčania, ktoré by mali viesť k vyššej bezpečnosti.

Prácu uzatvára kapitola Záver, kde hodnotíme dosiahnuté výsledky.

1 Súčasný stav riešenej problematiky doma a v zahraničí

1.1 História informačnej bezpečnosti

História informačnej bezpečnosti začína pri počítačovej bezpečnosti. Potreba zabezpečenia počítačov, teda potreba zabezpečiť fyzické umiestnenie, hardvér a softvér pred hrozbami, vznikla za druhej svetovej vojny, kedy sa začali používať prvé zariadenia, vytvorené na pomoc pri výpočtoch pri prelamovaní komunikačných kódov. Na ochranu týchto zariadení a udržanie integrity dát bolo zavedených niekoľko úrovní zabezpečenia. Prístup k citlivým armádnym častiam, bol riadený hodnosťami a fyzicky reprezentovaný kľúčmi prideľovaných členom bezpečnostnej služby. Rastúca potreba udržať bezpečnosť nakoniec viedla k zložitejšiemu a technologicky vyspelejšiemu zabezpečeniu.

Počas týchto prvých rokov, bola informačná bezpečnosť jednoduchý proces založený prevažne na fyzickej bezpečnosti a jednoduchých systémoch klasifikácie dokumentov. Hlavné bezpečnostné hrozby tvorili: fyzické odcudzenie výpočtového zariadenia, špionáž a sabotáž.

Počas studenej vojny, boli sálové počítače čoraz dlhšie v prevádzke aby tak mohli vykonávať zložitejšie a sofistikovanejšie úlohy. Bolo nutné umožniť týmto sálovým počítačom komunikovať menej ťažkopádnym spôsobom než pomocou vtedy zvyčajného zasielania magnetických pások poštou. Vyriešením tejto požiadavky bolo v USA poverené oddelenie na Ministerstve obrany s názvom Advanced Research Project Agency (ARPA). Tak vznikol sieťový komunikačný systém na podporu výmeny vojenských informácií - projekt s názvom ARPANET.

Počas nasledovného desaťročia, sa stal ARPANET populárny a široko používaný a potenciál pre jeho zneužitie rástol. V roku 1973 boli identifikované podstatné bezpečnostné problémy ARPANETu [23]:

- vzdialené pracoviská nemali dostatočné kontroly a bezpečnostné opatrenia na ochranu svojich dát pred neoprávnenými vzdialenými používateľmi,
- jednoduchosť hesiel,
- nedostatočné bezpečnostné postupy pri dial-up pripojení,
- žiadna autentifikácia a autorizácia používateľov systému.

Posun smerom k bezpečnosti nad rámec ochrany fyzického umiestnenia začal až dokumentom ministerstva obrany s označením Rand R-609, ktorý sa pokúsil definovať viacero kontrolných mechanizmov potrebných pre ochranu viacúrovňového počítačového systému. Dokument bol utajený takmer desať rokov a v dnešnej dobe je považovaný za dokument, ktorý započal výskum počítačovej bezpečnosti. Zameranie bezpečnosti sa následne rozšírilo z fyzického zabezpečenia na zabezpečenie dát, obmedzenie náhodného alebo nevyžiadaného prístupu k dátam, zahrnutie zamestnancov rôznych úrovni riadenia.

Počítačové siete sa stali na konci dvadsiateho storočia bežne dostupné, rovnako ako nutnosť prepájania týchto sietí medzi sebou. Prepojením viacero samostatných sieti vznikol internet. Možnosti jeho využitia sa komercionalizáciou ďalej rozšírili a internet sa stal všadeprítomný.

Spočiatku boli spojenia vytvárane bez formálne definovaných štandardov komunikačných protokolov, zabezpečenie dát bolo minimálne. Formálne štandardy vznikli až dodatočne a prenos prebiehal použitím protokolov, ktorých hlavným cieľom bola spoľahlivost a nie bezpečnosť. V raných érach internetu sa spoliehalo na bezpečnosť postavenú na fyzickom prostredí dátového centra. Prepojením počítačov sa však táto bezpečnosť stratila a aj dáta boli zrazu vystavené hrozbám.

V súčasnej dobe, internet prepája milióny nezabezpečených počítačových sietí. Bezpečnosť každého počítača a informácií uložených v ňom je priamo závislá od úrovne zabezpečenia každého jedného počítača, ku ktorému je pripojený. Samotnú softvérovú bezpečnosť na aktualizovaných počítačoch zabezpečuje špecializovaný softvér (antivírus, antimalware) v kombinácii s firewallom a ďalšími aktívnymi ochrannými prvkami. Softvéry týchto kategórií vznikli ako reakcia na množiace sa programy, ktoré často úmyselne spôsobovali škody na dátach. Spôsob prenosu (infikovania počítača) takýmto programom sa taktiež zmenil a v dnešnej dobe je zdrojom takmer výhradne internet – aktívnym útokom na bezpečnostné slabiny počítača, alebo infikovaním sťahovaných dôveryhodných programov.

1.2 Definícia bezpečnosti

Bezpečnosť je ochrana proti nepriateľom, ktorí chcú spôsobiť škodu (či už úmyselne alebo inak). Napríklad národná bezpečnosť je mnohovrstvový systém, ktorý chráni zvrchovanosť štátu, jeho majetok, jeho zdroje a jeho občanov. Dosiahnutie primeranej úrovne bezpečnosti v organizácii vyžaduje mnohostranný systém.

Každá úspešná organizácia by mala mať nasledujúcich niekoľko vrstiev zabezpečenia na ochranu svojich činností:

- fyzické zabezpečenie - na ochranu fyzických predmety, objektov, alebo oblasti, pred neoprávneným prístupom a zneužitím,
- personálne zabezpečenie - ochrana jednotlivca alebo skupiny jednotlivcov, ktorí sú oprávnení využívať organizáciu a jej činnosti,
- ochrana činností - ochrana podrobností určitej operácie alebo série činností,
- ochrana komunikácie - ochrana komunikačných médií, technológie a obsahu,
- zabezpečenie siete - ochrana sieťových súčastí, pripojenia a obsahu,
- informačné zabezpečenie - ochrana dôvernosti, integrity a dostupnosti informačných aktív, či už pri skladovaní, spracovaní, alebo odovzdaní. To je dosiahnuté použitím politík, vzdelávania, školení a zvyšovania povedomia.

Model informačnej bezpečnosti by sa mal zakladať na troch princípoch: integrita, dôvernosť, dostupnosť.

1.3 Časti informačného systému (IS)

Informačný systém sa skladá viac než len z počítačového hardvéru. Tvorí ho množina softvéru, hardvéru, dát, ľudí, postupov a sieťových prvkov, ktoré umožňujú používať informačné zdroje v rámci organizácie. Týchto šesť častí umožňuje informácie vkladať, spracovávať, uchovávať a následne z IS vyberať. Každý z týchto komponentov má svoje špecifické silné a slabé stránky a bezpečnostné požiadavky.

Softvér

Softvérová časť IS sa skladá z aplikácií, operačných systémov a rôznych podporných programov. Softvér je z pohľadu zabezpečenia zrejme najzložitejšia časť IS.

Zneužitie chýb v softvéri tvorí podstatnú časť informačných útokov. Softvér je jadrom spracovania informácií. Vo väčšine prípadov je však softvér vyvíjaný v rámci obmedzení kladených projektovým manažmentom, ktorý sa snaží minimalizovať náklady, čas vývoja a potrebné ľudské zdroje. Informačná bezpečnosť je tak v nemálo prípadoch implementovaná dodatočne, namiesto toho aby bola vyvíjaná v rámci softvéru - priebežne a od jeho začiatku.

Hardvér

Hardvér je reprezentovaný zhmotnenými technologickými prvkami, ktoré vykonávajú softvér, ukladajú a prenášajú údaje, sprostredkúvajú interakciu - pridávanie a vyberanie informácií zo systému. Zabezpečenie hardvéru sa týka ochrany pred poškodením alebo krádežou, využitím obvyklých nástrojov bezpečnosti ako sú zámky, kľúče, kamery a senzory umožňuje prístup len oprávneným osobám. Samotný hardvér, napr. dátový nosič nemusí predstavovať významnú hodnotu, avšak ak sú na ňom uložené dáta, môže sa jeho cena niekoľkonásobne zvýšiť. Fyzické zabezpečenie sa tak stáva podstatnou časťou informačnej bezpečnosti.

Dáta

Dáta, údaje sú zvyčajne najcennejším majetkom spoločnosti a stávajú sa hlavným cieľom úmyselných útokov. Systémy v dnešnej dobe zvyčajne používajú na ukladanie dát databázové systémy. Ich použitie zvyšuje bezpečnosť dát a aplikácií, ak je daný databázový systém správne nakonfigurovaný. Zle nakonfigurovaný databázový systém predstavuje vyššie bezpečnostné riziko ako ukladanie údajov do štandardných súborov.

Ľudia

Často prehliadaným faktorom v informačnej bezpečnosti sú samotní ľudia. Ľudia sú často najslabším článkom vo firemnej informačnej bezpečnosti. Vyžadujú neustále školenia, zvyšovanie informovanosti a technických znalostí. Tieto musia byť adekvátnym spôsobom kontrolované a vynucované, inak dochádza k častým informačným škodám, a to z nedbanlivosti, alebo úmyselnej, či zlomyselnej činnosti. Bez technického školenia, si zamestnanci informačnú bezpečnosť predstavia v zjednodušenom modeli, ktorý poznajú z bežného života – napríklad ak pri posielaní dôvernej informácie stačí na zabezpečenie použiť doporučený list, obdobnú informáciu pošlú e-mailom ako štandardnú prílohu. Chyba v tomto modeli spočíva vo viere, že prenosová infraštruktúra je dostatočne zabezpečená, tak ako pri fyzickej bezpečnosti pošty. Toto je však vzhľadom na množstvo rôznych prvkov

patriacich rôznym subjektom a s rôznou úrovňou informačnej bezpečnosti neoddôvodnený predpoklad a správny postup by mal byť danú prílohu zašifrovať. Ďalší častý omyl pri manipulácii s dátami je ich likvidácia, ktorá je zvyčajne len jednoduché zmazanie súborov z nosiča (namiesto bezpečného prepísania obsahu), čo je v podstate rovnaká bezpečnosť akú by poskytovalo označovanie papierových dokumentov textom "Skartované", namiesto skutočného skartovania. Ľudia sú navyše často cieľom sociálneho inžinierstva a vďaka chybám v úsudku a pohodlnosti tak vedú k oslabeniu bezpečnosti, znefunkčneniu systému alebo neoprávnenému sprístupneniu informácií útočníkovi.

Postupy

Ďalšou často prehliadanou zložkou informačného systému riadenia sú postupy. Postupy sú písomné pokyny pre plnenie konkrétnej úlohy. Keď neoprávnený používateľ získa organizačné postupy, predstavuje to hrozbu pre informačnú integritu. Napríklad, zamestnanec banky sa naučí, ako meniť platné tranzakcie administratívnym zásahom, ktorý má podľa postupu použiť v konkrétnych prípadoch. Zamestnanec náhodou zistí bezpečnostnú slabinu (nedostatočná autentifikácia), ktorej zneužitím sa môže pokúsiť prevádzať financie na svoj účet. Firmy zaškolia zamestnancov postupy, ktoré potrebujú vykonávať, avšak častokrát opomenú doplniť ako majú danú informáciu ďalej chrániť. Toto je rovnako dôležitá časť ako fyzické zabezpečenie informačného systému. Zvláštnosť požiadavky na ochranu procesov pominie, keď si uvedomíme, že zapísaný alebo slovne odovzdaný postup je vo svojej podstate tiež informácia a teda ho treba chrániť.

Sieť

Sieť je jedným z hlavných zdrojov tlaku na zvýšenie informačnej a počítačovej bezpečnosti. Prepojené počítačové systémy v rámci intranetu, ktorý je ale následne pripojeny na extranet, vytvára prostredie v ktorom sú hrozby rádovo väčšie ako v prípade odpojeného intranetu. Použitie prístupov analogických fyzickej bezpečnosti (zámky, kľúče – mená a heslá) tu prestáva fungovať a je nutné pridávať ďalšie bezpečnostné prvky ako sú systémy na detekciu narušenia, ktoré automaticky rozpoznaju a upozornia na neštandardné správanie.

1.4 Bezpečnosť vs. použiteľnosť

1.4.1 Vyváženie informačnej bezpečnosti a prístupu

Úplná informačná bezpečnosť nie je dosiahnuteľná ani pri bezchybnom plánovaní a implementácii - takýto systém by nesmel informácie sprístupniť nikomu a teda by stratil zmysel. Aby bola dosiahnutá použiteľnosť aj informačná bezpečnosť, musí systém poskytovať dostatočný prístup, ktorý však vie zabezpečiť proti hrozbám.

Obavy a implementácie bezpečnostných opatrení informačného systému môžu byť v niektorých prípadoch zakorenené tak hlboko, že už nevyvažujú svoj prínos pre používateľov informácií a môžu nadmerne zaťažovať oddelenie bezpečnosti. Obe skupiny ľudí (oddelenie bezpečnosti a používatelia) pritom majú spoločný ciel - zabezpečiť dáta a ich dostupnosť bez zbytočných prekážok.

1.4.2 Prístupy k implementácii informačnej bezpečnosti

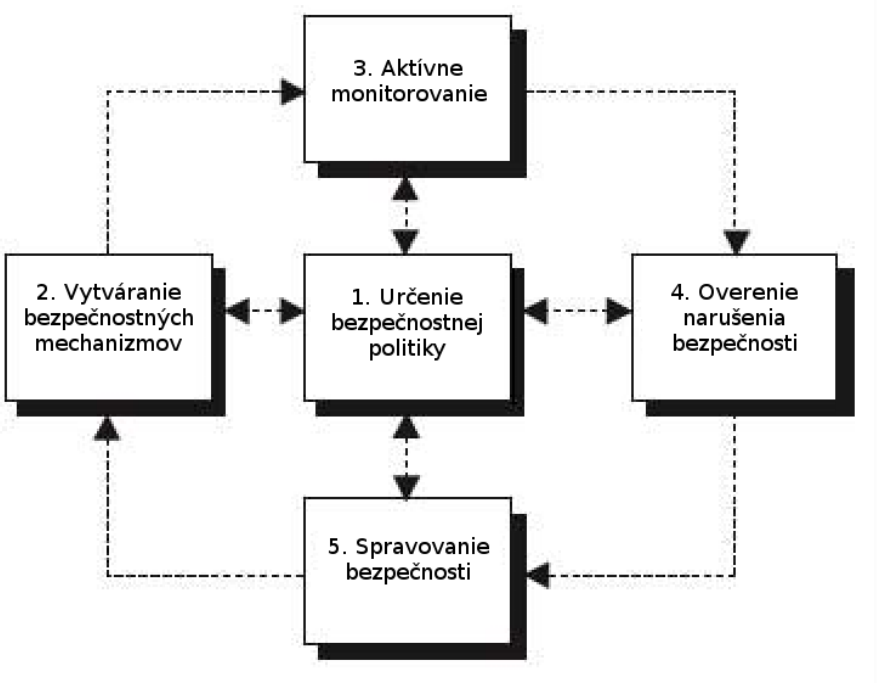
Implementáciu bezpečnosti nie je možné začať implementovať všade a naraz. Zabezpečenie informácii je postupný proces vyžadujúci riadenie, čas a trpezlivosť. Rozoznávame dva systematické spôsoby ako postupovať pri implementácii: zdola - nahor a zhora - nadol. Pri prvom spôsobe vylepšujú bezpečnosť svojich systémov správcovia. Takýto prístup má výhodu v tom, že správcovia poznajú svoje systémy najlepšie a majú teda aj vedomosti, ktoré môžu pri ich zabezpečovaní využiť. Poznajú a chápu hrozby ich systému a vedia ho proti nim chrániť. Takýto prístup nemá zvyčajne dlhotrvajúci úspech, keďže nezahŕňa konzultáciu s ovplyvnenými používateľmi a nemá jasnú podporu vedenia spoločnosti. V prístupe zhora nadol vedenie zavádza bezpečnostnú politiku, procesy, ciele, výsledky a určuje zodpovednosť. Takýto prístup má vyššie šance na úspech, keďže má zvyčajne aj samostatný rozpočet, plán, implementačné procesy a spôsoby na presadzovanie sa v spoločnosti. Pre zvýšenie úspešnosti sa používajú metodiky ako pri vývoji nového systému. Projekt zastupuje pred vedením osoba na pozícii vedúceho informačnej bezpečnosti (v angličtine Chief Information Officer - CIO). Bez jeho kontroly a podpory správcovia systémov zľahčujú význam bezpečnosti a pristupujú k nej ako k nedôležitej, zaťažujúcej časti. Dôležitá je aj účasť podpory a koncových používateľov - ich práca je priamo ovplyvňovaná bezpečnostnou politikou a jej úspechmi, resp. neúspechmi. Kľúčoví pracovníci z týchto oblastí by mali byť účastní aj pri návrhu bezpečnostných pravidiel.

Riadenie informačnej bezpečnosti má za cieľ vytvoriť systém, prostredníctvom ktorého je organizácia riadená a kontrolovaná a integrovať plánovanie bezpečnosti v širšom kontexte IT a obchodných plánov. Riadenia bezpečnosti zahŕňa vývoj a integráciu štruktúry a organizácie riadenia s procesmi, ktoré zahŕňajú všetky aspekty úspešného bezpečnostného programu. Dávajú podnikom istotu, že riziká sú definované a zodpovedajúco riadené. Riadenie informačnej bezpečnosti je v zodpovednosťou vrcholového manažmentu.

Efektívne riadenie informačnej bezpečnosti zahŕňa širokú škálu aktivít. Niektoré z hlavných kategórií týchto činností sú:

- vydávanie a pravidelná aktualizácia politík, postupov, noriem a smerníc,
- aktívne monitorovanie dodržiavania predpisov, rizík,
- vykonávanie testovanie narušenia v zodpovedajúcej detailnosti a pravidelnosti,
- navrhovanie vhodnej bezpečnostnej ochrany a pravidelné zlepšovanie už existujúcich opatrení,
- efektívne spravovanie zabezpečenia s cieľom zabezpečiť včasné kroky.

Na obrázku č. 1 je znázornený životný cyklus informačnej bezpečnosti podľa Sethuramana [5].



Obrázok č. 1 – Životný cyklus informačnej bezpečnosti systému [5].

V každej organizácii je informačná bezpečnosť súčasťou všetkých oddelení organizácie a vyžaduje zapojenie zamestnancov na všetkých úrovniach. Korporátne firmy majú svoje činnosti častokrát outsourcované do krajín, kde sa dajú vykonávať za nižšie náklady, ale porovnateľnú kvalitu – ak je v takejto forme činnosť outsourcovaná do zahraničia, majú bezpečnostné procesy presah naprieč organizáciami v rôznych krajinách a vyžadujú efektívne zosúladenie činností a bezpečnostných požiadaviek na ne v závislosti od krajiny, kde sa outsourcovaná činnosť vykonáva.

Organizácia vykonáva zvyčajne outsourcing v troch fázach:

- pred outsourcovaním (vykonané pred podpísaním zmluvy o outsourcovaní):
    - výber poskytovateľa služieb,
    - posudzovanie bezpečnostných rizík,
    - posúdenie bezpečnostnej spôsobilosti poskytovateľa služby,
    - zavedenie bezpečnostných systémov a procesov,
- počas outsourcovania:
    - ustanovenie zmluvných záväzkov,
    - zriadenie servisnej zmluvy (Service Level Agreement),
    - rozpracovanie úrovní požadovaných služieb,
    - bezpečnostné a prevádzkové požiadavky,
    - spôsoby overovania a auditu,
- po skončení outsourcovania.

Mnoho poskytovateľov outsourcovaných služieb zavádza komplexný systém riadenia bezpečnosti v súlade s normami ako je NIST 800, ISO 17799. Touto formou sa snažia dosiahnuť certifikáciu a zvýšenie poskytovanej informačnej bezpečnosti. Niektorí poskytovatelia sa zameriavajú aj na dodržanie odporúčaných postupov uvedených v štandarde ISO 20000, ktorý popisuje manažment IT služieb (Information Technology Infrastructure Library - ITIL) a zlepšujú tak kvalitu poskytovaných služieb. Takéto zmluvy majú zvyčajne viacročné trvanie a zmluvné strany majú podpísané aj iné dlhodobé zmluvy.

1.4.3 Vývoj systému

Informačná bezpečnosť musí byť spravovaná podobným spôsobom, ako každý iný systém danej spoločnosti.

Jedným z možných prístupov vývoja informačného systému v spoločnosti, kde nie sú ešte zavedené formálne bezpečnostné štandardy, je použiť vývojový cyklus bezpečného systému. Metodika vývoja sa skladá zo šiestich fáz - zber údajov, logický návrh, fyzický návrh, implementácia, údržba a zmeny. Každá z fáz vývojového cyklu by mala zahrňovať aj dopad rozhodnutí na bezpečnosť systému a dát ktoré používa. Odporúčané kroky v jednotlivých fázach podľa štandardu NIST 800-64 [8][9] sú nasledovné:

Zber údajov, analýza

Zaviesť kategorizáciu hrozieb a vážnosti dopadov na systém v prípade, že nastanú. Môžeme definovať tri úrovne dopadu na firmu, alebo osoby (nízku, strednú, vysokú)[24], v prípade uskutočnenia bezpečnostnej hrozby. Pri výbere vhodných bezpečnostných kontrol informačných systémov sa firma môže oprieť o zavedené kategorizácie bezpečnostných štandardov. Z predbežného posúdenia rizika vyplynie základný popis bezpečnostných požiadaviek na systém. Posúdenie by malo definovať prostredie, v ktorom sa daný systém nachádza.

Fáza logického a fyzického návrhu

Táto fáza pozostáva z niekoľkých previazaných častí:

- hodnotenie rizík – prístup k riziku pomocou analýzy identifikujúcej požiadavky ochrany pred nimi. Postup je identifikovaný prostredníctvom formálneho procesu hodnotenia rizík. Analýza vychádza z počiatočného posúdenia rizika vykonaného počas prvotnej fázy, ktoré rozpracováva do väčších detailov,
- analýza funkčných bezpečnostných požiadaviek - je to analýza požiadaviek, ktorá zahŕňa nasledujúce časti:
    - zabezpečenie prostredia systému (tj. politika informačnej bezpečnostni a bezpečnostnej architektúry),
    - funkčné bezpečnostné požiadavky,
- analýza požiadaviek nutných na zabezpečenie – analýza požiadaviek, ktoré sa zameriavajú na vývojové činnosti a nutné podklady, potrebných na

zabezpečenie požadovanej úrovne dôveryhodnosti systému, pri ktorom bude informačná bezpečnosť fungovať správne a účinne. Právne a funkčné bezpečnostné požiadavky, budú použité ako základ pre stanovenie, koľko a aké druhy podkladov sú nevyhnutné,

- zváženie nákladov – určuje, akú časť nákladov na vývoj možno pripísať informačnej bezpečnosti v priebehu životného cyklu systému. Tieto náklady zahŕňajú hardvér, softvér, personál a školenia,
- bezpečnostný plán – popisuje vykonávanie bezpečnostných kontrol, plánovaných alebo ad-hoc. Bezpečnostný plán tiež poskytuje kompletnú charakteristiku a opis informačného systému, ako aj prílohy a odkazy na kľúčové dokumenty podporujúce informačnú bezpečnosti firmy (napr. plán riadenia konfigurácie, havarijný plán, plán reakcie na incidenty, povedomie o bezpečnosti a tréningový plán, posúdenie rizík, bezpečnostné testovanie a vyhodnotenie výsledkov, bezpečnostné akreditácie, akčný plán),
- vývoj kontroly zabezpečenia – zaručuje, že bezpečnostné kontroly uvedené v príslušných bezpečnostných plánoch sú navrhnuté a implementované. Prevádzkované informačné systémy môžu vyžadovať úpravy a ďalšie rozpracovanie plánov bezpečnostných kontrol, doplnenie existujúcich riadiacich prvkov alebo modifikáciu vybraných prvkov, ktoré nie sú efektívne v požadovanej miere,
- testovanie a vyhodnocovanie vývojovej bezpečnosti – zabezpečuje, že bezpečnostné kontroly vyvinuté pre nový informačný systém pracujú správne a sú účinné. Niektoré typy bezpečnostných kontrol (predovšetkým kontroly netechnickej povahy) nemôžu byť skúšané a hodnotené, dokiaľ informačný systém nie je nasadený. Tieto prvky sú typicky prvky riadenia a prevádzkovej kontroly,
- ostanté časti plánu – zaručuje, že všetky potrebné časti procesu vývoja sú brané do úvahy pri začlenovaní bezpečnosti do životného cyklu. Tieto časti sú napr.:
    - výber vhodného typu zmluvy,
    - účasť všetkých potrebných funkčných skupín organizácie,
    - účasť certifikátora,
    - účasť poskytovateľa akreditácie,
    - vývoj a realizáciu nevyhnutných zmluvných plánov a procesov.

Fáza implementácie

Kontrola a potvrdenie zabezpečia, že spoločnosť naplní požiadavky špecifikácie a zahrnie ich do dodávky systému. Integrácia systému zabezpečí, že systém bude zapojený a súčinný na mieste určenia inštalácie a prevádzky. Nastavenie prvkov zabezpečenia musí prebehnúť v súlade s dodávateľskými inštrukciami a dostupnými bezpečnostnými postupmi.

Bezpečnostná certifikácia zabezpečí, že riadenie je implementované požadovaným spôsobom, postupom a zaručuje, že bezpečnostné opatrenia budú ochraňovať informačný systém a jeho dáta. Certifikácia taktiež odhaľuje a popisuje známe zraniteľnosti systému.

Bezpečnostná akreditácia poskytuje nevyhnutnú bezpečnostnú autorizáciu informačného systému na požadované spracovanie a prenos informácii. Táto autorizácia pochádza od predstaviteľov spoločnosti, na základe dosiahnutej požadovanej úrovni zabezpečeného riadenia a známych rizík.

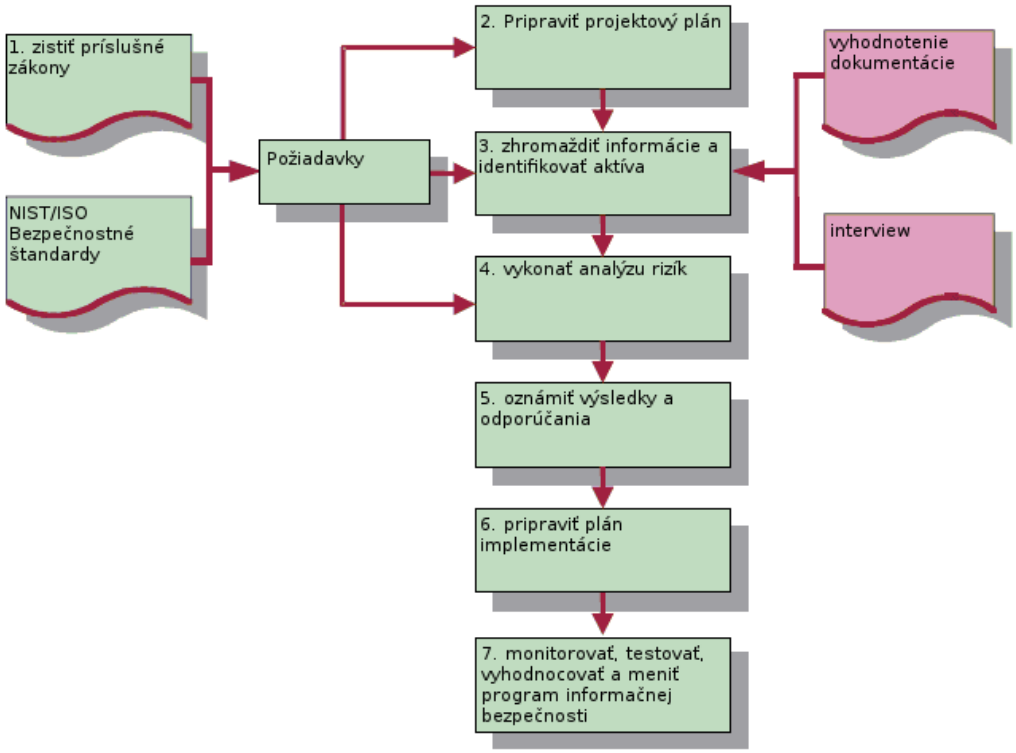
Údržba a zmeny

Riadenie verzií a konfigurácie - zabezpečí dostatočné zváženie potenciálnych bezpečnostných dopadov pre jednotlivé druhy zmien informačného systému a jeho okolia. Postupy pre riadenie verzií a konfigurácie zásadne ovplyvňujú zavedenie bezpečnosti na najnižšej úrovni v hardvéri, softvéri a firmvérových komponentoch informačného systému a následne aj správu a udržiavanie presného popisu jednotlivých zmien sytému. Priebežné monitorovanie efektivity kontroly zmien umožňuje udržanie kontroly formou pravidelného testovania a vyhodnocovanie výsledkov testov. Monitorovanie zabezpečenia a hlásenie jeho stavu zodpovedným osobám je najzákladnejšou činnosťou komplexného bezpečnostného programu. Ukladanie informácií zabezpečí ich dostupnosť v prípade, že by boli potrebné z právnych, resp. vykazovacích dôvodov. Metódy ukladania sa môžu v čase vyvíjať a zastarať. Bezpečné likvidovanie médií umožní dáta zmazať, médiá vyčistiť a v prípade potreby aj prepísať. Obdobne treba pristupovať aj k likvidácii hardvéru a softvéru.

Je nutné aby sa informačná bezpečnosť začleňovala do systému od počiatku, ako aby bola doplnená vo fázy implementácie, prípadne až po nej. Informačné systémy, ktoré neboli navrhované s ohľadom na informačnú bezpečnosť, prípadne bola takáto vlastnosť pridaná dodatočne, vyžadujú zvyčajne neustále dolaďovanie a aktualizovanie, aby dokázali zabraňovať meniacim sa hrozbám systému a informáciám. Firmy túto úlohu čoraz častejšie

chápu a zameriavajú sa intenzívnejšie na zahrnutie bezpečnosti do vývoja, čím sa snažia zvýšiť nielen užitočnosť systémov, ale aj dôveru zákazníkov v tieto produkty.

Metodiku podľa štandardov NIST 800 prakticky zhŕňa vo svojej práci Peter Adler [15]. V práci porovnáva existujúce právne obmedzenia týkajúce sa univerzitného prostredia v USA: rôzne nariadenia a zákony o ochrane osobných údajov. Poukazuje na duplicity v štandardoch (NIST 800, ISO 17799 a ďalších) a ich významný prienik – všeobecné odporúčania v podobe jednotného prístupu k plánovaniu bezpečnosti (obrázok č. 2).



Obrázok č. 2 – Ukážka jednotného prístupu k plánovaniu bezpečnosti podľa Adlera [15].

1.4.4 Vývoj bezpečného systému

Vývoj prebieha v rovnakých fázach ako pri normálnom systéme. Metodológia je taktiež rovnaká, okrem dvoch procesov, v ktorých sa mierne odlišujú. Podstatou implementácie je identifikovanie konkrétnych hrozieb a vytvorenie kontrol na ich elimináciu. Vývoj bezpečných systémov zjednocuje tento prístup a snaží sa nepoužívať jeho aplikovanie len na nahodilé časti systému.

Zbieranie údajov

Je to fáza, ktorou vývoj zabezpečených systémov začína, spisujú sa ciele, procesy, očakávané výsledky projektu a tiež rozpočet, časové a iné obmedzenia.

Analýza

Vo fáze analýzy sa spracovávajú dáta zozbierané v predchádzajúcej fáze. Vývojový tím spracováva predbežnú analýzu existujúcich bezpečnostných politík a procesov a tiež hrozieb a s nimi súvisiacich opatrení. V tejto fáze sa tiež analyzujú právne stránky bezpečnosti. Do vývojového procesu je zapojené oddelenie riadenia rizika.

Logický návrh

Vo fáze logického návrhu vznikajú podklady a náčrty informačnej bezpečnosti, identifikujú a skúmajú sa kľúčové bezpečnostné politiky, ktoré by mohli mať dopad na zvyšok systému. V tejto fáze sa tiež vypracovávajú plány reakcií na bezpečnostné incidenty, katastrofické scenáre; plánuje sa kontinuita, reakcia a obnova po incidente. Krátka analýza realizácie na konci fázy rozhodne o tom, či sa bude daný systém vyvíjať v spoločnosti alebo sa vývoj outsourcuje.

Fyzický návrh

Na základe požiadaviek logického návrhu sa vo fáze fyzického návrhu vyhodnocujú jednotlivé informačné bezpečnostné technológie, vyhodnocujú sa alternatívne riešenia a volí sa konečný návrh. Logický návrh sa môže spätne upravovať. Zároveň sa stanovujú konkrétne štatistiky úspešnosti, bezpečnosti a spôsob ich vyhodnocovania. Na konci fázy sa vykoná štúdia uskutočniteľnosti, ktorá vyhodnotí pripravenosť spoločnosti na projekt. Záver z tejto štúdie predkladá vedúci informačnej bezpečnosti vedeniu, ktoré rozhoduje o schválení projektu a postúpení do ďalšej fázy.

Implementácia

Prebieha obdobne ako fáza implementácie normálneho systému - riešenie sa zaobstará kúpou, alebo vyrobí vo vývojovom oddelení. Systém sa cyklicky vyvíja a testuje. Súčasťou implementácie je aj príprava školenia používateľov, príručiek a smerníc. Výsledný systém sa odovzdá riadeniu na konečne schválenie a uvedenie do prevádzky.

Údržba a zmeny

Údržba je najdlhšou a najdôležitejšou fázou. Bezpečnostné informačné systémy potrebujú neustále monitorovanie, testovanie, úpravy, vylepšovanie a upravovanie.

Normálne aplikácie nemajú v rámci vývoja prihliadané na obnovu dát po zlyhaní, útoku, na rozdiel od bezpečnostných informačných systémov, kde sú činnosti ako oprava, obnova a stabilizácia očakávané vlastnosti. Informačný systém pružne reaguje na nové aj staré hrozby a obdobne sa prispôsobuje aj celá spoločnosť.

V tabuľke č. 1 uvádzame najvýznamnejšie rozdiely vo vývoji bezpečného IS v porovnaní s vývojom štandardného IS, rozdelené podľa jednotlivých fáz vývoja.

Tabuľka č. 1 – Rozdiely vo vývoji zabezpečeného IS a vývoju štandardnému IS.

Fáza	**Ďalšie vlastnosti fázy z pohľadu bezpečného vývoja**
zbieranie údajov	Manažment definuje procesy a ciele, ktoré zadokumentuje vo forme bezpečnostnej politiky.
analýza	Analyzujú sa existujúce bezpečnostné politiky, hrozby a metódy riadenia. Zvažujú sa aj právne dopady a analýza rizík.
logický návrh	Vytvoriť podklady pre bezpečnostný projekt, naplánovať reakcie na bezpečnostné incidenty, plán pre biznis procesy pre prípad zlyhania. Rozhodnúť o implementácii vo vlastnej réžii alebo outsourcovaní projektu.
fyzický návrh	Zvoliť technológie potrebné pre naplnenie bezpečnostného projektu, definovať metriku úspešnosti projektu, nadizajnovať bezpečnostné opatrenia riešiace logický návrh. Preveriť a schváliť projekt.
implementácia	Vyvinúť alebo kúpiť bezpečnostné riešenie, na konci fázy prezentovať vedeniu výstup projektu.
údržba a zmeny	Monitorovanie prevádzky, testovanie, oprava a inovovanie produktu s ohľadom na meniace sa hrozby.

1.4.5 Vývoj bezpečného softvéru

Systémy sa skladajú z hardvéru, softvéru, sietí, údajov, postupov a ľudí ktorí ich používajú. Mnoho problémov s bezpečnosťou týchto systémov má pôvod v softvéri. Bezpečné systémy vyžadujú bezpečný, alebo aspoň dodatočne zabezpečiteľný softvér. Vývoj systémov a softvéru, ktorý používajú sa často realizuje pomocou štandardizovaných metodológií. Mnoho organizácií túto potrebu uznalo a zahŕňa ju do cieľov pri plánovaní vývoja. Takto vyvinutý softvér má potom väčšiu šancu na úspešné zahrnutie do bezpečného systému.

Softvérové záruky (Software assurance)

Organizácie sa snažia zahŕňať bezpečnostné aspekty do vývojových cyklov a tým čeliť bezpečnostným problémom skôr než nastanú. O štandardizáciu tohto procesu a vytvorenie odporúčaní sa od roku 2003 pokúša aj pracovná skupina pod vedením Ministerstva obrany USA, ku ktorému sa pridala nejskôr aj oddelenie pre vnútroštátnu bezpečnosť - Department of Homeland Security - DHS.

Pracovná skupina vytvorená odborníkmi z dotknutých oblastí formulovala dve základné otázky:

- Aké inžinierske činnosti a ich vlastnosti sa týkajú dosiahnutia bezpečného softvéru?
- Aké znalosti sú nutné k vykonaniu týchto činností?

Na základe týchto podkladov a množstva ďalších dokumentov vznikla následne množina odporúčaní s názvom Secure Software Assurance Common Body of Knowledge (SwA CBK) [16] obsahujúca sekcie:

- Povaha nebezpečenstva
- Základné pojmy a princípy
- Etika, právo a riadenie
- Požiadavky na bezpečný softvér
- Dizajn bezpečného softvéru
- Tvorba bezpečného softvéru
- Verifikácia, validácia a vyhodnotenie bezpečného softvéru
- Nástroje a metódy bezpečného softvéru

- Procesy v bezpečného softvéru
- Riadenie projektu bezpečného softvéru
- Zaobstaranie bezpečného softvéru

1.4.6 Princípy softvérového dizajnu

Dobrý softvérový vývoj by mal vyústiť do hotového produktu, spĺňajúceho všetky špecifikácie stanovené dizajnom. Zvláštnu pozornosť si pri tom zasluhujú bezpečnostné charakteristiky týchto špecifikácií. Všeobecné bezpečnostné charakteristiky sa dajú zhrnúť do nasledovných princípov:

- udržať dizajn jednoduchý a pokiaľ možno čo najmenší,
- prístupy špecifikovať povoleniami a nie zákazmi,
- každý prístup ku každému objektu je nutné skontrolovať na oprávnenosť,
- dizajn by nemal byť tajný ale otvorený a bezpečnosť by nemala závisieť od jeho znalosti ale od pridelených oprávnení,
- viacúrovňové uzamykanie/privilégiá,
- princíp najmenších oprávnení - každý program a používateľ by mal pracovať s minimálnou nevyhnutnou množinou oprávnení k vykonávaniu svojej činnosti,
- používateľské rozhranie by malo byť prehľadný a jednoducho ovládateľný, čím umožní používateľom nadobudnúť rutinu a používať softvér bezpečným spôsobom.

1.5 Obchodné dôvody - potreba informačnej bezpečnosti

Na rozdiel od iných programov informačných technológií, hlavnou úlohou bezpečnostného informačného programu je zabezpečiť, že systémy a ich obsah zostane bez zmien. Organizácie sú nútené vynakladať veľké objemy zdrojov na zabezpečenie ich informačných systémov, ktoré by mohli inak vložiť na vylepšenie týchto systémov. Útoky na informačné systémy sa vyskytujú na dennej báze a tým rastie aj potreba informačnej bezpečnosti súbežne s vyspelosťou útokov. Organizácie si musia uvedomovať okolie v akom sa ich systémy nachádzajú aby mohli rozpoznávať medzi skutočnými a potenciálnymi problémami.

1.5.1 Prínosy pre podnik

Informačná bezpečnosť organizácie sa zakladá na štyroch funkciách:

1. chrániť beh organizácie,
2. umožniť bezpečný beh aplikácií na informačných systémoch,
3. ochraňovať dáta, ktoré organizácia zbiera a používa,
4. ochraňovať technologické aktíva organizácie.

Ochrana behu organizácie

Manažment a tiež IT manažment sú zodpovedné za implementáciu informačnej bezpečnosti, ktorá má ochraňovať beh organizácie. Informačná bezpečnosť je často vnímaná ako príliš zložitá technická úloha, pričom v skutočnosti je to viac úloha pre klasický manažment než pre technický. Riadenie informačnej bezpečnosti sa totiž dotýka viac nariadení a ich vynútenia, než spôsobom ich zavedenia. Každá oddelenie v organizácii musí zvažovať informačnú bezpečnosť z pohľadu dopadu na beh a nákladov na jeho narušenie a obnovu, ako len z čisto technického.

Umožnenie bezpečného behu aplikácií

Organizácie sú nútené efektívne používať silne previazané, zložité aplikácie v prostredí, ktoré chráni ich beh (hlavne prvky infraštruktúry ako e-maily, operačné systémy, instant messaging aplikácie). Organizácie získavajú tieto prvky od externých dodávateľov, prípadne si ich vybudujú samé. Po zapojení do infraštruktúry musí manažment dohliadať na ich spravovanie a neposunúť ich celé IT oddeleniu.

Ochraňovanie zbieraných a používaných dát

Je to kritický aspekt informačnej bezpečnosti. Vysoká hodnota dáva motiváciu útočníkom - kradnúť, sabotovať, prípadne poškodiť ich. Účinný program informačnej bezpečnosti zabezpečí ich hodnotu a integritu.

Ochrana technologických aktív

Pre efektívny chod musí organizácia prevádzkovať jej veľkosti adekvátne bezpečnostné prvky infraštruktúry. Malým podnikom postačia štandardné e-mailové služby od dodávateľa internetovej konektivity v spojení so softvérovým šifrovaním na individuálnej úrovni. Ako podnik narastá, stáva sa tento spôsob neudržateľný a podnik musí vytvoriť ďalšie bezpečnostné služby. Typicky PKI infraštruktúru, previazanie systémov,

šifrovacie postupy a zmluvné zabezpečenie. PKI infraštruktúra zahŕňa správu elektronických certifikátov na zabezpečenie autenticity komunikujúcich strán. V každom z týchto certifikátov sa nachádza aj overiteľný verejný kľuč a celý tento certifikát je zabezpečený proti poškodeniu samostatným elektronickým podpisom. Vo všeobecnosti, čím je organizácia rozsiahlejšia a má častejšie požiadavky na zmeny, tým robustnejšie technológie začne používať.

1.6 Bezpečnostné hrozby

Hrozby sú relatívne dobre známe a zdokumentované. Všeobecne prijímaný je aj fakt, že pripojením sa k internetu zvyšuje riziko vonkajších hrozieb. Firma Kaspersky Lab, ktorá dodáva vlastné antivírusové riešenia pre osobné zariadenia a firemné prostredia, vo svojej správe píše o vyše 5 miliardách útokov na počítače a mobilné zariadenia [2]. Hrozby, ktoré vplývajú na bezpečnosť firmy:

- aplikácie mobilného bankovníctva s prístupom na firemné účty,
- zadné vrátka v operačnom systéme mobilného zariadenia,
- útoky na počítače vo firemnej sieti cez napadnuté mobilné zariadenie.

Zdrojom hrozieb je teda v nezanedbateľnej miere aj správanie zamestnancov v informačnej infraštruktúre, presnejšie disciplína pri pripájaní vlastných zariadení.

Hrozby môžeme rozdeliť podľa kategórie, pričom najširšiu kategóriu tvoria softvérové hrozby vznikajúce z chýb pri vývoji softvéru.

1.6.1 Kategórie hrozieb

V nasledovnej tabuľke uvádzame štrnásť všeobecných kategórií, ktoré pokrývajú aktuálne prítomné hrozby zamestnancov, informácií a systémov spoločnosti. Každá spoločnosť si musí ohodnotiť jednotlivé hrozby, ktorým čelí, vzhľadom na prostredie, všeobecnú politiku a postoj k rizikám a pravdepodobnosť výskytu [2], [3].

1. napadnutie, poškodenie intelektuálneho vlastníctva, pirátstvo,
2. softvérové útoky - vírusy, trójske kone, malware,
3. zhoršenie kvality poskytovaných služieb ISP,
4. špionáž, neoprávnený prístup,
5. prírodné pohromy - zásah blesku, povodne, oheň,

6. zlyhanie ľudského faktora,
7. hrozba vyzradenia informácií,
8. strata čiastočného/plného prístupu k dátam a systémom - hardvérové zlyhanie bez záložného riešenia a obnovy, resp. postupov obnovy,
9. nedostatočná, resp. chýbajúca kontrola nad (sieťovými) prvkami IS,
10. úmyselné poškodenie,
11. krádež,
12. zlyhanie hardvéru,
13. zlyhanie softvéru,
14. morálne zastaranie použitých technológií.

1.6.2 Bezpečnostné chyby pri vývoji softvéru

Najvážnejšie problémové oblasti pri vývoji softvéru, ktorý je následne ťažké, alebo nemožné nasadiť bezpečným spôsobom [1]:

- Pretečenie zásobníka
- Vkladanie príkazov
- Cross-site scripting
- Zlyhanie pri ošetrovaní chýb
- Zlyhanie zabezpečenia sieťového prenosu
- Zlyhanie pri ukladaní a ochrane dát
- Nepoužívanie kryptograficky bezpečných náhodných čísiel
- Chyby pri formátovaní reťazcov
- Nesprávne nastavenia prístupov k súborom
- Nesprávne použitie SSL
- Informačný únik
- Chyby z pretečenia čísiel
- Chyby zo súbehu
- SQL Injection
- Spoliehanie sa na správnosť prekladu názvov sieťových komponentov na IP
- Výmena neoverených kľúčov
- Používanie zadných vrátok
- Používanie systémov so slabými kľúčmi
- Slabá použiteľnosť

2 Cieľ práce

Celosvetový trendu používania vlastných zariadení v pracovnom prostredí je na vzostupe a firmy prejavujú neistotu pri zavádzaní pravidiel práce s nimi a z nedostatočnej skúsenosti robia chyby pri implementácii. Tento trend je známy ako Bring Your Own Device – BYOD a snaží sa zosúladiť korporátne bezpečnostné očakávania a politiky s každodennou realitou, kedy zamestnanci volia na prvom mieste pohodlie práce a bezpečnosť až na druhom.

Cieľom tejto práce bolo uskutočniť analýzu informačného prostredia firmy a na jej základe poukázať na dobré a slabé stránky v jej implementácii, ktoré môžu byť návodom pri zavádzaní BYOD v ďalších firmách.

Pre dosiahnutie cieľa sme si vytýčili rad podcieľov:

- poukázať na hlavné problémy týkajúce sa informačnej bezpečnosti v informačných systémoch firiem
- charakterizovať všeobecný vývoj a trendy
- popísať základné charakteristiky BYOD
- na základe analýzy aplikácie BYOD v konkrétnom podniku poukázať a charakterizovať základné procesy týkajúce sa zavádzania BYOD
- zistiť nedostatky v analyzovanom systéme
- navrhnúť spôsoby ich zlepšenia

3 Metodika práce a metódy skúmania

Prácu sme vypracovali na základe systematicky zozbieraných a zotriedených informácií o konkrétnych bezpečnostných opatreniach. Tieto sme zhromaždili hlavne z osobných rozhovorov s administrátormi siete, zamestnancami a vedúcimi pracovníkmi. Všeobecné informácie a odporúčania potom z literárnych zdrojov a v nemalej miere tiež z online dostupných materiálov uvedených v zozname použitých materiálov. Za hlavný zdroj pri čerpaní informácií o bezpečnosti považujeme materiály z akademického výskumu, bezpečnostných štandardov a odporúčaní, ktoré sú dostupné v textovej forme.

V prvom rade sme si na základe preštudovanej literatúry a vykonaných rozhovorov stanovili cieľ a jeho podciele. Následne sme pristupovali k ich plneniu a vyvodzovaniu záverov.

V práci sa v prvej kapitole dotkneme teoretických podkladov zahŕňajúcich bezpečnostné prvky v jednotlivých fázach vývoja informačného systému. Pri písaní tejto kapitoly sme použili metódy porovnávania, zovšeobecňovania, abstrakcie analýzy, syntézy a pozorovania.

V kapitole 2 a 3 stanovujeme cieľ práce a uvádzame metodiku práce a metódy skúmania. Popísanie nastupujúceho trendu z pohľadu pozície a vplyvu zamestnancov a nimi používaných zariadení na bezpečnosť celého procesu tvorby tvorí potom samostatnú, štvrtú kapitolu. Pri písaní tejto kapitoly využívame hlavne prvky porovnávania, abstrakcie, analýzy a syntézy. Pri písaní tejto kapitoly sme použili aj metódu pološtruktúrovaného interview, ktoré pozostávalo zo širokých otvorených otázok, ktoré sú adresované jednotlivcom, a to konverzačným, relaxačným a neformálnym spôsobom. Túto metódu sme použili pri získavaní poznatkov od zamestnancov, administrátorov informačných systémov a tiež pri komunikácii s vedením firmy. V interview sme viedli otvorenú diskusiu o implementácii bezpečnostných mechanizmov, podmienkach a prostriedkoch potrebných na ich prevádzku a údržbu.

Konkrétne ekonomické prostredie tvorí prostredie stredne veľkej IT firmy pôsobiacej na Slovensku, ktorá sa špecializuje na dodávanie softvérových in-house riešení určených pre stredný a vrchný menežment stredne veľkých firiem. Riešenia sú postavené nad aplikačným portfóliom a databázami firmy Oracle a sú tvorené internými analýzami,

konzultáciami so zákazníkmi, implementovaním, testovaním, nasadením a údržbou, pričom všetky tieto činnosti vykonávajú priamo zamestnanci firmy.

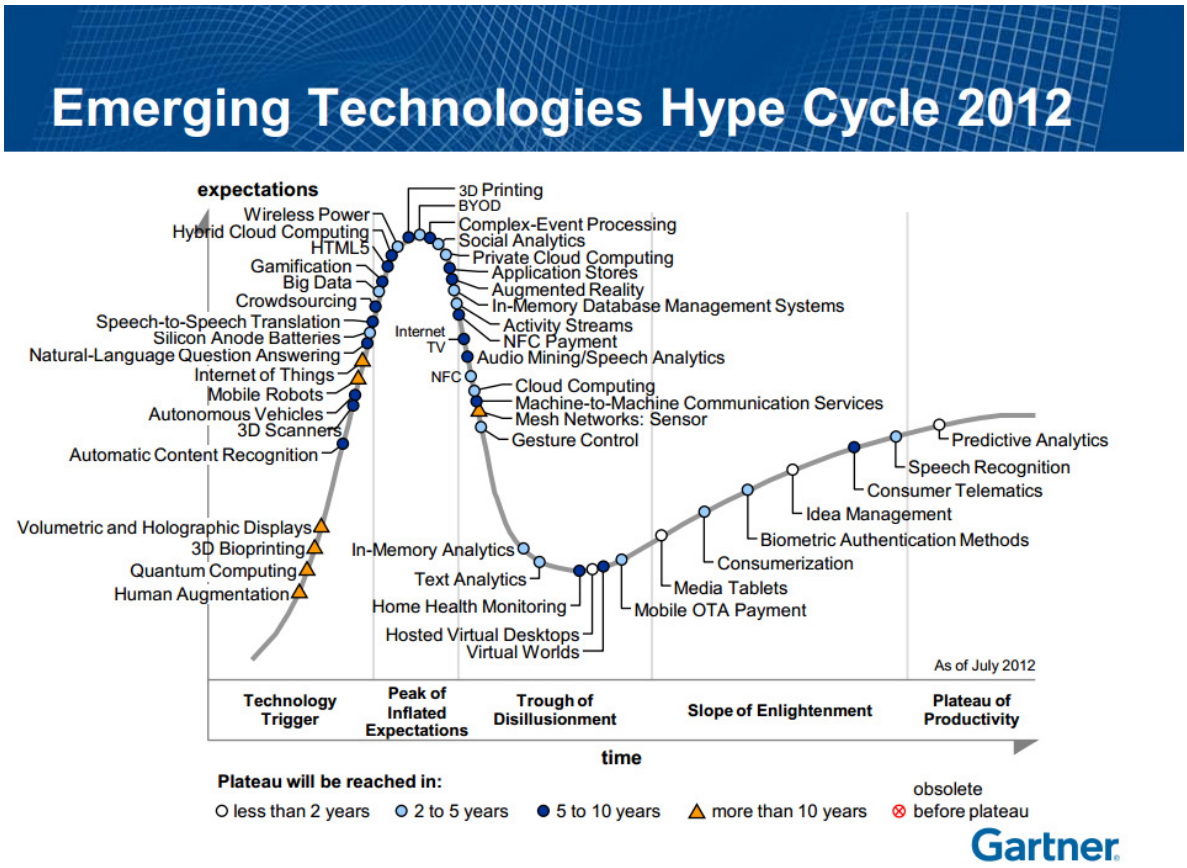
Zmluvné dojednanie s firmou, nám poskytlo cenný vhľad do jej fungovania a bezpečnostných opatrení, zároveň nás, ale obmedzilo v detailoch, ktoré môžeme v tejto práci uverejniť a to vrátane jej názvu (firmu teda nebudeme konkrétne pomenovávať a ak z textu nevyplýva iné, máme na mysli vždy vyššie spomínanú). Z rovnakých dôvodov sme nemohli otestovať funkčnosť firmou implementovaného riešenia nad rámec štandardného používania (ako napr. vykonať záťažové testy, pokus o prelomenie bezpečnosti, hádanie hesiel, pokúsiť sa o narušenie činnosti služieb a aplikácií), nakoľko sa nám nepodarilo zabezpečiť dostatočné záruky, že naša činnosť nepoškodí bežnú prevádzku firmy.

Pri skúmaní informačnej bezpečnosti firmy popisujeme jej aktuálne používané zariadenia a infraštruktúru. Firemné priestory tvoria tri sektory umiestnené v dvoch lokalitách. Sektor A tvorí štandardné kancelárske priestory a vybavenie, neobsahuje žiadne cenné dáta a v zásade len poskytuje infraštruktúru na pripojenie sa k ostatným častiam. Sektor B sa tiež nachádza v kanceláriách, ale je v časti s kontrolovaným fyzickým prístupom, tvoria ju hlavne počítače na ktorých sú spustené citlivé interné aplikácie. Sektor C sú servery v dátovom centre, ktoré prevádzkujú vývojové, testovacie a produkčné aplikácie pre zákazníkov firmy. Táto časť má kontrolovaný fyzický prístup a ďalšie bezpečnostné prvky. Obe lokality sú napojené na internet a v prípade potreby je možné ich prepojiť bezpečným spojením, ktoré je zároveň využívané na automatické zálohovanie interných systémov.

4 Výsledky práce

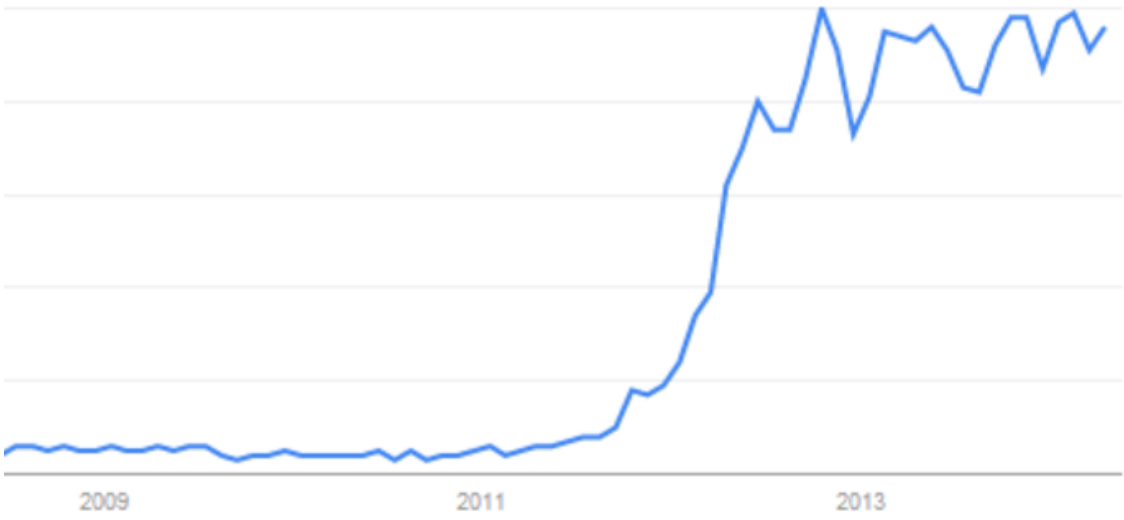
4.1 Trend BYOD

BYOD sa stal alebo stane jedným z najvplyvnejších trendov a dotkne sa každej jednej IT organizácie. Do povedomia sa dostal v roku 2005, ale skutočný záujem nastal až v roku 2012 a pretrváva dodnes. Skutočnosť, že sa jednalo o prudký nárast záujmu dokumentuje aj spoločnosť Gartner [17], ktorá vo svojej hype krivke (na obrázku č. 3) predpovedá udržanie a stabilizáciu tohto trendu v nasledovných 2 až 5 rokoch.



Obrázok č. 3 – Hype krivka pre rok 2012 a nasledovné roky podla Gartner [17].

Udržanie záujmu o trend potvrdzuje obrázok č. 4., ktorý zobrazuje relatívne porovnanie počtu vyhľadávaní slova „BYOD“ na Google.com na časovej osi. Trend vyhľadávania odzrkadľuje zrejmý záujem verejnosti – zamestnancov, vedúcich pracovníkov a IT odborníkov, čo potvrdzuje opodstatnenosť tejto témy.



Obrázok č. 4 - Trend vyhľadávania výrazu „BYOD“ na Google.

Oddelenie informačnej bezpečnosti v organizácii má za úlohu zladiť pripájenie vzdialených používateľov a zároveň udržať informačnú bezpečnosť organizácie. Aby to dosiahlo, musí riešiť nasledovné úlohy.

Definovať zrozumiteľnú bezpečnostnú politiku, ktorú budú zamestnanci chápať a dodržovať. Aj keď zamestnanci môžu chcieť používať svoje vlastné zariadenie, organizácia musí poskytovať jasné usmernenia ohľadom prijateľného a bezpečného používania. Názory a možnosti na to, čo je a čo nie je prijateľné, sa môžu dramaticky líšiť. Je takmer isté, že zamestnanci budú považovať bezpečnostnú politiku BYOD ako obmedzujúcu prácu na nimi vlastnenom zariadení. Zladenie jednoduchosti a komfortu práce za súčasného udržania bezpečnosti je zrejme najzložitejšia úloha bezpečnostného oddelenia.

Aj po zhode na bezpečnostnej politike BYOD medzi používateľmi a bezpečnostným oddelením je jej vynucovanie často ešte viac náročné. Vo vysoko decentralizovaných podnikoch presadzujúcich politiky BYOD zabezpečenia je toto ešte náročnejšie. Napriek tomu neschopnosť presadiť (aj nepopulárne) politiky zabezpečenia môže dostať organizáciu do stavu dátového ohrozenia. Mnoho zariadení môže byť riadne zabezpečených, ale zabezpečenie, že tieto možnosti sú správne a aj nastavené a zadokumentovať tento fakt, môže vyžadovať dodatočný softvér a zavedenie nových postupov.

V prípade straty zariadenia, alebo odchodu zamestnanca z organizácie, musí bezpečnostný tím zabezpečiť, že firemné dáta na zariadení sa odstránia a zároveň minimalizovať dopad na používateľove vlastné dáta.

BYOD reprezentuje globálne nastupujúci trend, ktorý si vynucuje zmenu spôsobov akým sú používané súkromné zariadenia v pracovnom prostredí [11]. BYOD je o používaní zariadení zamestnancami, ktoré zvyšujú ich produktivitu. Sú to zariadenia, ktoré si kupujú zamestnanci alebo im ich kupujú zamestnávatelia – je to akékoľvek zariadenie bez jasného vlastníka, používané na firemnej infraštruktúre. V tejto práci sa zameriame na to, ako tento nový trend ovplyvní biznis prostredie, aké nove požiadavky kladie na IT oddelenie a vedúcich informačnej bezpečnosti. Pre lepšie pochopenie dôsledkov, ktoré BYOD so sebou prináša, je účelné zamerať sa na biznis dôvody, ktoré vedú k jeho akceptovaniu [7].

4.2 Prijatie stratégie

Bezpečnosť BYOD a správa zariadení sú základné prvky podnikovej BYOD stratégie, ktorá musí brať do úvahy všetky typy a funkcie pracovníka pred nasadením BYOD riešenia. Organizácia musí zvážiť riešenia naprieč prvkami zabezpečenia, ktoré zaisťujú vstupné body, poskytujú ochranu pre podnikové siete a ochraňujú dáta. Pre dosiahnutie úspešnej implementácie si musia byť koncoví používatelia vedomí firemnej politiky a chápať riziká BYOD. Správa mobilných aplikácií nadobúda vyšší význam v podnikovej politike, keďže podniky presúvajú svoju pozornosť od riadenia mobilných zariadení na vývoj, dodávanie a bezpečnosť mobilných aplikácií.

Nárast je aj v zavádzaní úložísk podnikových aplikácií (application store). Veľké podniky venujú pozornosť poskytovaniu aplikácií svojim zamestnancom ako všeobecných, tak aj pre podnik špecifických, interných. Vytvorením takýchto úložísk získava organizácia:

- kontrolu nad inštalovanými aplikáciami (ich presnými verziami)
- poskytovať k nim používateľskú podporu,
- zabezpečiť kompatibilitu medzi jednotlivými aplikáciami,
- inštalovať dodatočné bezpečnostné opatrenia pre aplikácie so známymi chybami (patche)
- možnosť školiť svojich zamestnancov na konkrétne aplikácie.

4.3 Používateľské zariadenia

Do nedávnej doby poskytovali zamestnávatelia svojim zamestnancom počítače (pracovné stanice a notebooky), aké si samotní zamestnanci nemohli, alebo z rôznych dôvodov nechceli zaobstarať. S narastajúcou dostupnosťou notebookov, netbookov, tabletov, chytrých telefónov, čítačiek a iných zariadení, už ale zamestnanci zvyčajne vlastnia zariadenie pomáhajúce im v každodennom živote. Preto bol neodvratný moment, kedy sa títo zamestnanci začali dožadovať ich používania aj v pracovnom prostredí. Väčšina IT organizácii túto myšlienku zavrhla z dôvodu bezpečnosti a tiež nemožnosti poskytovať podporu tak širokej škále dostupných zariadení, okrem krátkeho zoznamu otestovaných zariadení.

V posledných rokoch používateľský tlak na využívanie chytrých zariadení narastal a to aj za situácie, keď si dané zariadenie museli zakúpiť osobne [13]. Toto viedlo k zvoľneniu informačných reštrikcií a bol umožnený čiastočný, obmedzený prístup k firemným prostriedkom z týchto zariadení.

Tento trend je nezvratný a každá organizácia sa naň bude musieť časom adaptovať. Mnoho ľudí používalo osobný počítač na prácu v aplikáciách a telefón na telefonovanie. Klasické telefóny sú však už vytláčané chytrými, na ktorých môžu byť tiež spúšťané aplikácie, je možé z nich zároveň pristupovať na internet. Chytré telefóny začínajú mať porovnateľné možnosti ako osobné počítače, čím sa voči nim stavajú samostatnou triedou so širšími vlastnosťami. Dochádza ku konvergencii zariadení – jedno zariadenie je určené súčasne na komunikáciu, aplikácie a prácu. Trend názorne zobrazuje prieskum GartnerPress v tabuľke č. 2, v ktorej vidíme, že počet dodaných počítačov sa od roku 2012 znižuje, ale objem mobilných zariadení stúpa. Odhadovaný dodaný počet na rok 2017 tento rozdiel ešte viac zvýrazňuje.

Tabuľka č. 2 – Počet celosvetovo dodaných zariadení podľa kategórie (v tis. ks) [6].

Device Type	2012	2013	2014	2017
PC (Desk-Based and Notebook)	341,263	315,229	302,315	271,612
Ultramobile	9,822	23,592	38,687	96,350
Tablet	116,113	197,202	265,731	467,951
Mobile Phone	1,746,176	1,875,774	1,949,722	2,128,871
Total	2,213,373	2,411,796	2,556,455	2,964,783

V dnešnej dobe si mnoho ľudí myslí, že špecializované zariadenia si zachovajú svoj význam, ako napríklad chytré telefóny určené hlavne na telefonovanie, keďže z notebooku sa síce telefonovať dá, ale mobilný telefón je ľahšie prenositeľný. Obdobne majú svoje špecifické výhody a nevýhody aj tablety. Diverzita teda zrejme zostane zachovaná a žiadny univerzálny prístroj na všetky činnosti nevznikne.

Hlavný dopad nových trendov je však ten, že čoraz viac zariadení bude pripájaných zamestnancami.

Podľa výskumu firmy Gartner, má v súčasnosti iba 33 percent organizácií politiky BYOD pre chytré telefóny a 47 percent má politiky BYOD týkajúce tabletov. Najväčšie riziká predstavujú [19]:

- strata chytrého telefónnu,
- zníženie bezpečnosti aplikácií nedbanlivosťou,
- využívanie nezabezpečenej komunikácie,
- používanie nevynútiteľnej bezpečnostnej politiky,
- nadmerná záťaž IT oddelenia.

Strata alebo krádež chytrého telefónu obsahujúceho dáta organizácie. Toto riziko je umocnené hrozbou právnych postihov hroziacich organizácii. Ochranou je prípade použitie kvalitného hesla, prípadne inštalácia ochranného časovaného softvéru, ktorý po špecifikovanej dobe bez pripojenia k organizačnej infraštruktúre automaticky zničí dáta na zariadení.

Ak organizácia používa vzdialenú kontrolu dát na mobilnom zariadení, nezodpovedný prístup zamestnanca k aplikáciám môže napriek tomu sprístupniť organizačné dáta použitím slabých hesiel, inštalovaním nebezpečných aplikácií a používaním služieb, ktoré významne zasahujú do súkromia. Vzdialená kontrola je v tomto prípade aplikovaná neskoro.

Zmena spôsobu komunikácie z e-mailovej na zasielanie správ (instant messaging, internetové SMS), využitím služieb tretích strán. E-mailová komunikácia je zvyčajne zabezpečená internými informačnými systémami, ktoré ale neposkytujú žiadne formy rýchlej komunikácie.

Čiastočného povolenie používania firemných dát na nezabezpečených mobilných zariadeniach - bezpečnostné oddelenie vymenuje typy dokumentov, ich obsah a formu práce s nimi. Vynútenie tejto bezpečnostnej politiky je však slabo aplikovateľné.

Medzi používateľské zariadenia a predmety predstavujúce riziko patria tie, ktoré môžu byť použité na uchovanie citlivých dát [28]:

- notebooky,
- chytré telefóny,
- USB disky,
- pamäťové karty,
- tablety,
- elektronické diáre (PDA),
- digitálne prehrávače,
- zapisovateľné dátové nosiče (CD, DVD, BD),
- elektronické čítačky,
- iné zariadenia obsahujúce úložný priestor (napr. chytré hodinky, okuliare).

Pripájanie zariadení, ktoré nie sú schopné aplikovania bezpečnostných politík predstavuje samostatnú kategóriu BYOD. Bezpečnosť na nich, je dosahovaná nepriamo – zabránením pripojenia k zariadeniam, ktoré takúto politiku podporujú. Politika zvyčajne deaktivuje rizikové porty periférií (napr. USB konektory), alebo nepovolí komunikáciu s pripájanými zariadeniami, podľa zoznamov povolených zariadení.

Zvýšenie nepriamej záťaže IT oddelenia pri zabezpečovaní zariadení, v prípade, že neexistuje zoznam povolených zariadení. V tomto smere je riešením zavedenie kategórií podpory, ktoré bude IT oddelenie poskytovať pre zariadenia rôznych kategórií, nenachádzajúcich sa na zozname plne podporovaných zariadení.

4.4 Prekrývanie osobnej a pracovnej zóny

Čoraz častejšie sa dá práca chápať ako aktivita, ktorá nieje viazaná na konkrétne miesto a je možné ju vykonávať vzdialene s použitím internetu. Možnosť pripájať sa z rôznych miest cez mobilné siete priamo do firemných intranetov dáva zamestnancom flexibilitu a teda priamo zvyšuje ich produktivitu [10]. Nepriamo tak prispieva k rozmazávaniu hranice medzi pracovným a osobným časom, keď zamestnanci vymenia

pevné termíny za flexibilitu a možnosť určiť si kedy a kde chcú danú aktivitu vykonať. Častokrát sú dokonca osobné a pracovné činnosti úplné poprepletané.

Vedľajším efektom takejto flexibility je, že užívatelia sú kôli jednotlivým pracovným úlohám čoraz menej ochotní vymeniť práve používané osobné zariadenie, za pracovné a očakávajú, že budú môcť používať pravé jeden mobilný telefón a jeden osobný počítač, pripadne notebook na prácu aj osobný čas a nemať kôli tomu ďalšie firemné zariadenia.

Vlastníctvo zariadenia je taktiež sporné. Mnoho zamestnancov je ochotných používať svoje osobné mobilne zariadenia a notebooky na prácu s aplikáciami organizácie. Firmy tiež finančné dotujú zamestnancov a podporujú ich vo výbere preferovaného zariadenia. Dôsledok oboch týchto rozhodnutí je, že organizačné a osobné dáta sú čím ďalej tým viac popreplietané a ťažšie rozlíšiteľné a pokryteľné bezpečnostnými pravidlami a pravidlami na ochranu súkromia.

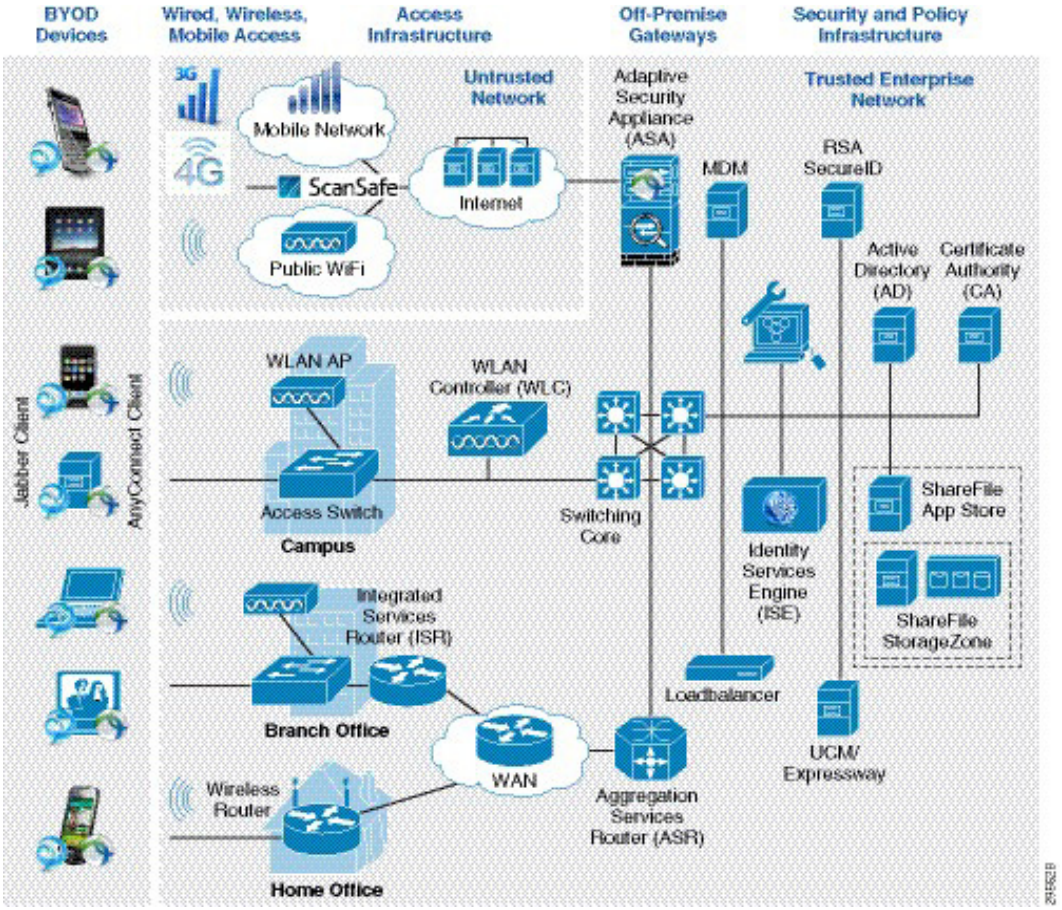
Odhaduje sa, že počet mobilných zariadení a objemu dát, ktoré vytvárajú sa zvýši 26-násobne počas rokov 2010 až 2015 Tvoriť ich budú chytré telefóny a notebooky užívateľov potrebujúcich neustále internetové pripojenie. Umožnia im to zamestnávatelia (pomocou WiFi sieti), 3G a 4G mobilní operátori a tiež zákaznícke služby (kaviarne, verejné hot-spoty) [7].

Čím viac zamestnancov bude mať jednoduchý prístup k práci vďaka takýmto sieťam, tým viac sa tieto siete budú rozširovať, čím umožnia ešte jednoduchší prístup k nim. Poslednou fázou je vzdialené pripojenie sa k práci z hocijakého miesta, čo znamená, že do firemných sieti sa bude pripájať stále viac zariadení a tiež aj častejšie a teda sa zvýši dopyt po aplikáciách schopných bežať neustále.

Pracovné aj osobné komunikačné prostriedky čoraz častejšie využívajú multimédia, čím vytvárajú väčší dátový tok prechádzajúci sieťou. Aplikácie určené na spoluprácu taktiež kladú dôraz na multimédia.

Mobilita zamestnancov a kolaborácia bude čoraz viac zdôrazňovať dôležitosť kvalitnej bezdrôtovej infraštruktúry a dostupnosti. Ďalšou hnacou silou je bežná dostupnosť používateľských zariadení s vyššími nárokmi a poskytovanými službami, ako sú napríklad HD video kamera v mobilných zariadeniach. Tento trend sledujú aj 4G mobilne siete a prístup na WiFi služby, ktoré už poskytujú dostatočnú prenosovú kapacitu.

Mobilní zamestnanci budú musieť pristupovať k niektorým aplikáciám spusteným vo firemnej infraštruktúre pomocou vzdialeného prístupu. Jeden zo spôsobov ako to dosiahnuť je bezpečným prepojením sietí pomocou VPN softvéru. Tento vytvorí v mobilnom zariadení virtuálny sieťový adaptér, ktorý simuluje pripojenie priamo v cieľovej sieti. Jedným z takýchto VPN softvérov je Cisco AnyConnect Client, zobrazený vľavo na obrázku č. 5., pomocou ktorého je možné sa pripojiť k firemnej sieti jednotným spôsobom.



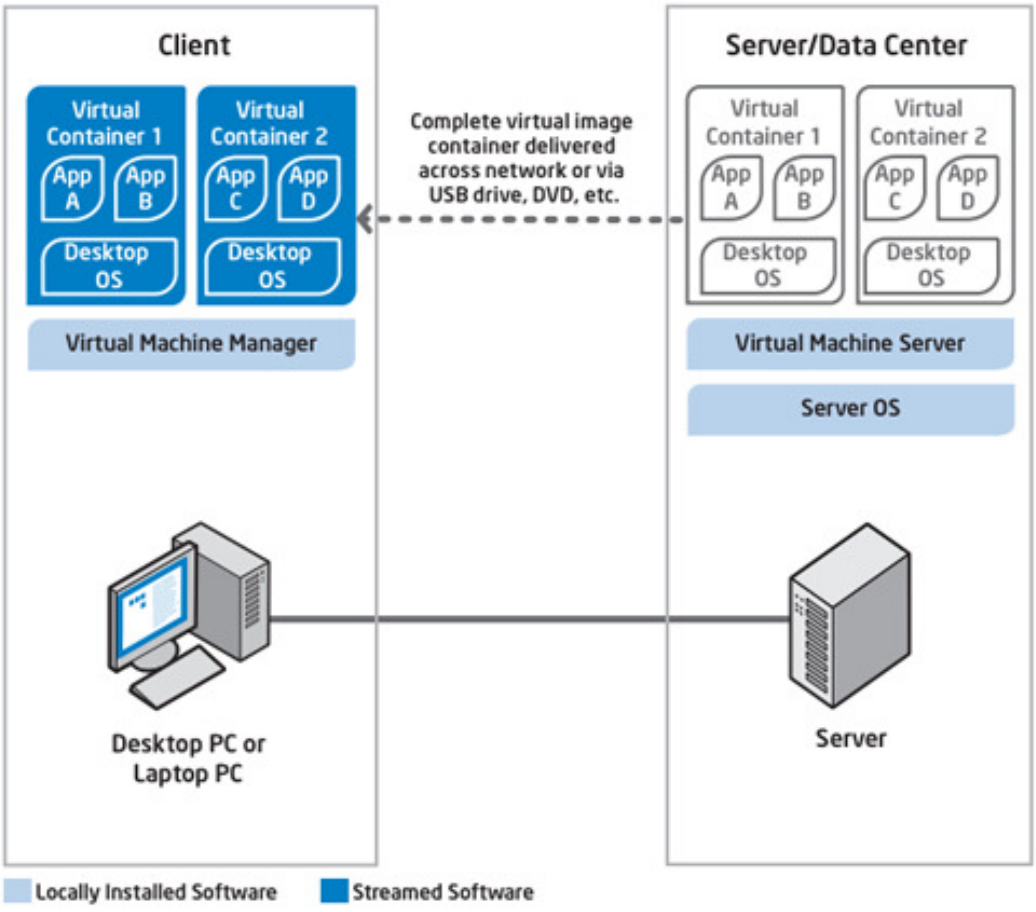
Obrázok č. 5 – Všeobecná topológia pripojenia mobilných zariadení pomocou technológií Cisco [7].

Používanie aplikácií bežne dostupných na tabletoch a mobilných telefónoch na prácu má ešte priestor na dosiahnutie požadovaného komfortu práce. Táto zmena je ale očakávateľná v blízkej budúcnosti a už dnes sú zakúpiteľné komerčné aplikácie poskytujúce vysoký komfort a výkon aj na týchto obmedzených zariadeniach v oblasti multimédií a spolupráce.

Z pohľadu bezpečnosti je možné aplikácie izolovať virtualizovaním – aplikácie sa neinštalujú priamo do zariadenia, ale do aplikácie, ktorá imituje prostredie virtuálneho

počítača (napr. použitím riešení od firmy VMWare, alebo Oracle VirtualBox). Nevýhodou takéhoto prístupu je náročnosť samotnej virtualizačnej aplikácie a to ako na procesorový výkon, tak na dostupnú operačnú a diskovú pamať. Toto riešenie teda nie je použiteľné na priemerných mobilných zariadeniach.

Iným spôsobom ako vyriešiť otázku bezpečnosti a zároveň zvýšiť komfort práce a možnosti mobilného zariadenia, je použitie vzdialenej virtualizácie. Vzdialená virtualizácia prenáša nároky na spustenie virtualizačnej aplikácie z mobilného zariadenia na špecializovaný server, ku ktorému sa mobilné zariadenie pripojí cez vzdialený prístup. Obrázok č. 6 znázorňuje takéto spojenie.

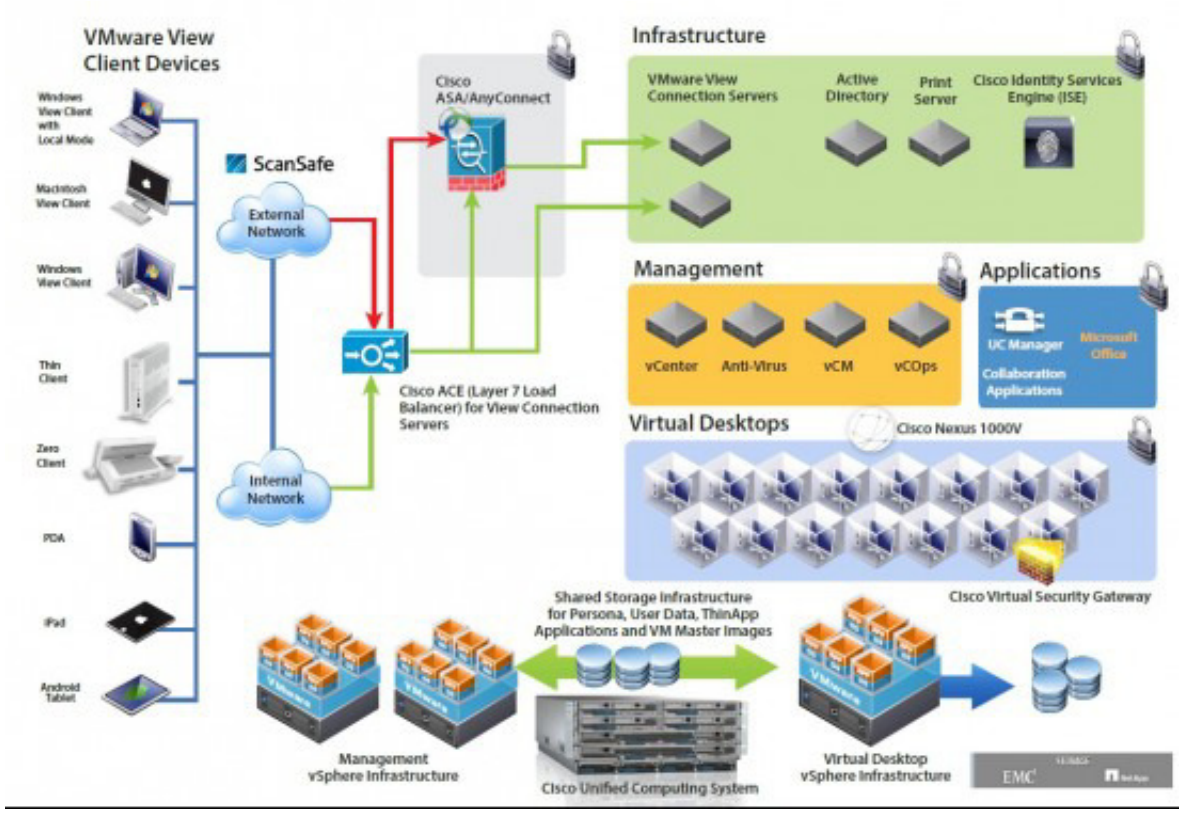


Obrázok č. 6 – Všeobecná schéma vzdialenej virtualizácie [25].

Vzdialená virtualizácia znižuje nároky na výkon mobilného zariadenia a obmedzuje bezpečnostné riziká tým, že mobilné zariadenie poskytuje zobrazovanie a vstupy používateľa, avšak samotné dáta a aplikácie sú stále v zabezpečenom prostredí firemnej infraštruktúry. K virtualizovanému prostrediu sa používateľ prihlasuje hneď v prvom kroku

a teda bezpečnostná autentifikácia a autorizácia nemôže byť obídená. Používateľ teda pracuje len s interaktívnym obrazom aplikácie, ktorá spracováva dáta. Virtualizácie už štandardne poskytujú možnosť kopírovania dát do klientskej zobrazovacej aplikácie, čo predstavuje bezpečnostné riziko. Správca má pre takýto prípad zvyčajne možnosť ovplyvniť toto nastavenie a umožniť ho len vybraným používateľovi na základe bezpečnostnej politiky.

Na obrázku č. 7 vidíme komplexné riešenie dodávané firmou VMWare v kombinácii s VPN riešením od firmy Cisco. Mobilné zariadenie spúšta len zobrazovaciu aplikáciu VMWare View Client, ktorá sa pomocou zapúzdreného VPN klienta pripojí k firemnej infraštruktúre. Jednotlivé prvky infraštruktúry sú modularizované a poskytujú tak zjednodušenú administráciu a bezpečnostnú kontrolu. Bezpečné VPN pripojenie je dosiahnuté použitím riešenia od firmy Cisco (detail v obrázku č. 5).



Obrázok č. 7 – Schéma vzdialenej virtualizácie od firmy VMWare [27].

Ďalšou výhodou vzdialenej virtualizácie je možnosť administrácie virtualizovaných aplikácií:

- zálohovanie,
- upgrade,
- dodatočné sprístupnenie privilegovaných aplikácií (druhostupňová autorizácia),
- poskytovanie vzdialenej technickej podpory,
- správa softvérových licencií,
- prepojenie na ostatné interné systémy,
- jednotná správa používateľov.

4.5 Nove úlohy a postupy IT oddelenia

Zahrnutie BYOD do existujúcich procesov a bezpečnostných opatrení bude výzvou hlavne pre IT oddelenia - zabezpečiť dostupnosť a dosiahnuteľnosť, je v protiklade zaužívaných postupov riadenia IT implementácii bezpečnosti a podpory.

Typicky prístup IT oddelenia je poskytnúť zoznam schválených zariadení na prácu vo firemnom prostredí - štandardizovaný osobný počítač, notebook a úzka množina mobilných zariadení, či chytrých telefónov. Zamestnancom je tento zoznam pevne daný a typicky nemajú možnosť použiť zariadenia iné než uvedené v zozname.

S príchodom BYOD zariadení sa musí zmeniť aj postoj IT oddelenia - zariadenia sa menia príliš často, na to, aby bolo možné vytvárať zoznam povolených zariadení. Taktiež úplná technická podpora daného zariadenia by vytvárala neúmerné nároky.

IT oddelenia si z týchto dôvodov vytvárajú - z makro pohľadu, zoznam typov zariadení, ktorým umožnia pristupovať k sieti (s prípadným pod zoznamom zakázaných zariadení, či výrobcov, z dôvodu známych bezpečnostných chýb). Technická podpora sa tak mení z plnej na čiastočnú (IT podpora po telefóne), resp. podporu cez knowledge base, wikipedie.

4.6 Udržanie bezpečného prístupu k firemnej sieti

Umožnenie výberu zariadenia neznamená stratu bezpečnosti. IT oddelenie musia zaviesť politiku minimálneho zabezpečenia, ktoré musí dané zariadenie spĺňať, aby mohlo byť na firemnej sieti použité - vrátané zabezpečenia WiFi, VPN prístupov a tiež ochrany pred vírusmi/adware. Okrem možnosti výberu zariadení je nutné mať možnosť identifikovať každé jedno takéto pripájajúce sa zariadenie a umožniť autentifikáciu jeho používateľovi.

4.6.1 Sprístupňovanie nových zariadení

Väčšina BYOD implementácií má množstvo rozličných pripájaných zariadení od notebookov, až po čítačky kníh. Pridávanie nových zariadení - v momente prvého pripojenia sa na sieť - by malo byť jednoduché a ideálne bez nutnosti zásahu IT oddelenia -

toto je dôležité hlavne pre zariadenia, ktorých vlastníkmi sú zamestnanci. IT oddelenie však potrebuje mať v prípade potreby možnosť updatovať všetky pripojené zariadenia.

V ideálnom prípade bude pridanie zariadenia bez nutnosti dodatočnej inštalácie klientského softvéru. V takomto prostredí je potom možné jednoducho pripájať aj zariadenia návštevníkov (tj. nie priamych zamestnancov firmy, ktorí nemajú uzatvorené zmluvy o zodpovednosti).

4.6.2 Vynucovanie firemných politik používania siete

Firmy majú zvyčajne mnoho politík, ktoré potrebujú udržať v praxi (v závislosti od oblasti podnikania a jej štátnej regulácie; a vlastnej, internej politiky). Zapojenie BYOD musí poskytnúť spôsob ako tieto politiky vynucovať. Toto môže byť mimoriadne náročné na okrajových typoch zariadení (ako sú napr. tablety). Ďalšou komplikáciou je premiešavanie osobných a pracovných úloh na zariadeniach. Napríklad chytré telefóny, ktoré sa používajú aj na pracovné aj na súkromné hovory majú s veľkou pravdepodobnosťou nainštalované rovnako súkromné tak aj pracovné aplikácie. Prístup na internet, zdieľanie súborov a vo všeobecnosti používanie aplikácii môže podliehať rôznym politikám v závislosti od toho, či sú používané v pracovnom alebo osobnom čase, sieti a či používajú niektorý z firemných prostriedkov (napr. tlačiareň).

4.6.3 Viditeľnosť zariadení na sieti

Typicky v klasických prípadoch mal zamestnanec pridelený jeden počítač a na sieti bol identifikovateľný unikátnou IP. Ak potreboval podporu IT oddelenia - títo ho vedeli jednoducho identifikovať a nájsť zariadenie, ktoré mu prestalo fungovať. S príchodom BYOD však môže mať každý zamestnanec viacero súčasne aktívnych zariadení na sieti, niektoré zariadenia môžu byť na viacerých sieťach naraz, resp. prepínať medzi nimi podľa dostupnosti a priepustnosti. IT oddelenia musia mať nástroje na sledovanie a vizualizáciu prítomnosti zariadení (“sieťová viditeľnosť”) [7].

4.7 Ochrana dát a prevencia pred stratou

Jednou z najväčších výziev implementácie BYOD je ochrana korporátnych dát. Ak je majetok firmy (napr. laptop) používaný na prístup k firemným aplikáciám a dátam, je typicky úzko kontrolovaný IT oddelením a aplikujú sa naň reštriktívnejšie používateľské politiky.

Niektoré (výrobné) oblasti navyše podliehajú regulátorovi (napr. ochrana osobných údajov) a bezpečnostná politika na zariadeniach teda musí spĺňať aj tento aspekt. V prípade BYOD zariadení je toto významne zložitejšie než na firemných zariadeniach s plnou kontrolou. Typický zástupca je tablet alebo chytrý telefón vlastnený zamestnancom a bežne používaný v osobnom živote a tiež na prácu s firemnými aplikáciami. Zdieľanie dát cez Cloud môže byť síce akceptovateľné pre osobné použitie, ale v prípade firemného predstavuje dodatočné riziko (napr. v prípade vyššie spomínaných osobných údajoch).

Kombinovanie zamestnancami vlastnených zariadení využívajúcich firemné dáta, ktoré sú pripojené k cloudových služieb, predstavuje riziko ak si tieto služby zamestnanci pripájajú sami a táto služba nieje nijak zmluvne previazaná s organizáciou zamestnanca. Organizácia môže úspešne používať vlastný Cloud, prípadne má prenajaté Cloud riešenie od dodávateľa. V takomto prípade je aplikovanie bezpečnostných politík významne jednoduchšie a v prípade potreby vynútiteľné.

Trend pripájania neschválených Cloudových služieb nazývajú informační experti ako Bring Your Own Cloud [18]. Tento trend pridáva ešte väčší tlak na existujúce bezpečnostné procesy a komplikuje úlohu sledovania, bezpečnosti a dokumentovania miest, kde všade sú dáta uložené. Najbežnejším problémom, s ktorým sa bezpečnostné oddelenie stretáva, je likvidácia firemných dát, ktoré zamestnanec uložil do Cloudu tretej strany a následne stratil oprávnenie k nim pristupovať alebo organizáciu opustil. Situácii nepomáha ani fakt, že o tejto skutočnosti informoval bezpečnostné oddelenie a v prípade nespolupráce je jedinou cestou súdny spor.

IT oddelenie musí mať teda pripravenú stratégiu na ochranu firemných dát na všetkých zariadeniach, či už vlastnených firmou alebo zamestnancami. Táto môže zahŕňať napríklad šifrovanú dátovú partíciu s firemnými dátam, ktorú je možné jednoducho spravovať, alebo prístup na Virtuálny Desktop, kde dáta nie sú prenášané a ukladané na prístupovom zariadení, ale len zobrazované.

4.7.1 Odoberanie prístupu

V životnom cykle zariadenia a zamestnanca môže prísť k bodu, kedy už nechceme danému zariadeniu umožniť prístup k prostriedkom siete. Takáto situácia je typicky po jeho krádeži, ukončení zmluvného vzťahu so zamestnancom, pripadne pri zmene pozície zamestnanca. IT oddelenie potrebuje mať rýchly spôsob odobratia, resp. zmeny prístupu povolenému zariadeniu, prípadne mať možnosť vzdialene vymazať údaje z neho. Vzdialené zmazanie poskytuje najväčšie pohodlie ako pre používateľov, tak aj pre IT oddelenie – nijak ich pred jeho aktivováciou nezaťažuje. Ak je ale zariadenie odcudzené sofistikovaným útočníkom, ktorý ho nepripojí k sieti a zariadenie nemá nainštalovaný softvérový časový zámok, vyžadujúci raz za obdobie aktívne pripojenie k firemnej infraštruktúre, útočník má neobmedzený čas na získanie dát z neho, prípadne na prelomenie ochranných mechanizmov. Na zabránenie takémuto riziku je vhodné použiť spomínaný softvérový časový zámok. V prípade ešte vyššej bezpečnosti, je možné od používateľa vyžadovať neostále aktívne pripojenie, priebežne overovať jeho autorizáciu a v prípade potreby vykonať automatické zmazanie. Toto je už ale typicky príliš obmedzujúce pre bežných používateľov a v ostatných prípadoch sa použitie BYOD zariadení na takúto prácu apriori zakazuje.

4.8 Dopad na prácu používateľov

Pretože zariadenia pripájajúce sa k sieti majú úplne nove schopnosti a IT oddelenie nemusí byť schopné správne zhodnotiť a kategorizovať každé jedno, vzniká priestor pre vytvorenie nových útočných vektorov. Napríklad, mnoho tabletov má možnosť vytvárať Ad Hoc WiFi spojenie. Ak sa autentifikované zariadenie pripojené k sieti spojí s iným zariadením cez Ad Hoc WiFi spojenie, môže takto sprístupniť neautentifikovanému zariadeniu prístup k firemnej sieti. Obdobný problém predstavujú bluetooth spojenia, ktoré sú vo väčšine chytrých telefónov a tabletov. IT oddelenie má v tomto smere pred sebou výzvu udržať vynucovanie politik aj pri takýchto situáciách - napríklad vypnutím možnosti Ad Hoc pripájania na všetkých autentifikovaných zariadeniach.

S prichádzajúcou všadeprítomnosťou bezdrôtových sietí, je očakávaná ich vysoká rýchlosť a spoľahlivosť, tak ako v prípade drôtových spojení. Používatelia vyžadujú rovnakú rýchlosť, spoľahlivosť, odozvu aplikácii, videokonferencií a iných kolaboračných nástrojov. Táto požiadavka posúva pohľad IT oddelenia na tieto siete z “dodatočných,

podporných firemných prostriedkov" na "kritické pre beh organizácie" s cieľom poskytovať služby v kvalite drôtového sieťového pripojenia - dostupnosť, monitorovanie výkonu, prelínanie sietí a migrácia živého spojenia [7],[12].

Počet zariadení na zamestnanca pripojených naraz v sieti stúpa a teda aj celkový počet zariadení môže dosiahnuť bod, kedy sa vyčerpajú interne prideľované IP adresy - väčšina systémov pochádza z obdobia protokolu IPv4, kedy bol očakávaný počet súčasne pripojených zariadení rádovo nižší. Tento tlak zrejme vyústi do aktualizácie používaného softvéru a hardvéru na protokol IPv6, ako v intranete, tak aj v prezentácii voči internetu. Tento protokol poskytuje oproti IPv4 4-krát dlhšie adresy pre jednotlivé pripojené zariadenia.

Hlavnou silou za používaním BYOD zariadení sú však samotní používatelia. Z používateľského pohľadu prináša BYOD výzvy samostatnej kategórie. BYOD riešenia a technológie sa rýchlo vyvíjajú. Najväčšou výzvou pre všetkých účastníkov tohto procesu je udržať veci pre koncového používateľa jednoduché. Rôznorodosť zariadení a spôsobov ako sa môžu pripojiť, z ktorej siete príde spojenie a na čo bude toto spojenie použité môže pre koncových používateľov vytvoriť neprekonateľnú prekážku. Každé zariadenie a výrobca môže mať svoje špecifické kroky potrebne na pripojenie a udržanie takéhoto spojenia. Bezpečnostné opatrenia a kroky môžu byť obdobne rôzne v závislosti od miesta a spôsobu pripojenia. Napríklad pripojenie cez firemnú WiFi môže vyžadovať meno a heslo, ale pripojenie cez verejnú WiFi môže vyžadovať navyše aj pripojenie VPN spojením a ďalšie bezpečnostné kroky.

V neposlednom rade BYOD musí byť dostatočné jednoduchý a poskytovať čo najpodobnejšiu používateľskú skúsenosť (user-experience) bez ohľadu na okolnosti pri vytváraní spojenia a to na všetkých zariadeniach.

BYOD prináša so sebou zmiešavanie osobných a pracovných úloh na jednom zariadení - adresár, emaily, súbory, aplikácie a prístup na internet - vytvárajú výzvy. V ideálnom prípade samotní používatelia vyžadujú oddelenie súkromných a pracovných dát. Súkromné fotografie, SMS správy, chát, telefonáty a browsovanie internetu by mali podliehať ochrane súkromia - dokumenty súbory a aplikácie používajúce firemné údaje a browsovanie počas pracovnej doby musia na druhú stranu podliehať firemnej politike.

Niektoré firmy vyžadujú pred pripojením zamestnancom vlastneného zariadenia do siete podpísanie dohody, ktorá umožní firme sledovať dodržiavanie pravidiel zaobchádzania s dátami z dôvodu ochrany. V prípade potreby sa používajú rôzne nástroje vrátané vzdialeného vymazania všetkých dát na zariadení, potenciálne vrátané používateľských osobných dát, čo môže viest k zvýšenému napätiu medzi IT oddelením a používateľmi.

V prípade, že sú takéto zásahy príliš invazívne, majú potenciál ohroziť pridanú hodnotu o ktorú sa snaží zavedenie BYOD. Zvyčajnou sťažnosťou používateľov, ktorí sú nútení používať VirtualDesktop aplikácie je, že práca v takomto prostredí má pomalú odozvu a citeľne znižuje efektivitu práce. Aplikácie pre VirtualDesktop a aj protokoly, ktoré používajú budú v budúcnosti smerovať k eliminácii tohto rozdielu.

4.9 Zvažovanie nasadenia a určenie stratégie zavedenia

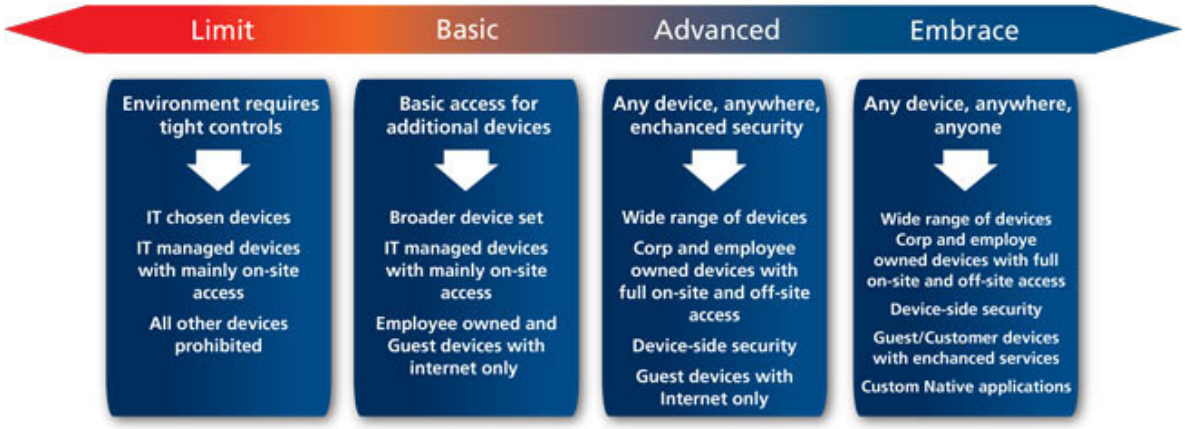
Každému nasadeniu BYOD by malo predchádzať vyhodnotenie rôznych aspektov. Dôležitú súčasť rozhodnutia tvorí pochopenie rôznych segmentov užívateľov v rámci implementácie BYOD. Jedno z odporúčaní je vykonať internú analýzu zamestnancov, ktorá určí typy, vlastnosti (typické použitie zariadení, aplikácie, prístupové body, požadovaná úroveň podpory z IT) týchto segmentov používateľov. Táto analýza bude následné podkladom pre nákladovú analýzu implementácie. Všeobecné pravidlá nie je možné určiť nakoľko každá firma ma inú štruktúru zamestnancov a ich možností a potrieb. Najjednoduchšie implementácie BYOD sú tie, kde sú nároky na IT oddelenie a podporu nízke - väčšinu potrebných nastavení zvládnu používatelia sami.

Rôzne oblasti majú rôzne prístupy k spôsobu zavádzania BYOD - každá firma ničmenej potrebuje mať svoju stratégiu kodifikovanú a formálne spísanú a to aj v prípade, ak sú BYOD zariadenia vylúčené z pripájania k firemným prostriedkom.

Oblasti s prítomnosťou regulácie (napr. finančný alebo bezpečnostný sektor) budú využívať striktnejšie politiky v BYOD prístupoch než bežné firmy a zariadenia budú zrejme mať striktnú kontrolu z IT oddelenia, ktorá môže byť v tomto prípade adekvátna a akceptovateľná.

Rôzne úrovne prijatých stratégií BYOD znázorňuje obrázok č. 8. V základnej úrovni je striktná bezpečnosť vynucovaná IT oddelením na podporovaných zariadeniach,

pričom ostatné zariadenia majú prístup zakázaný. Väčšina firiem bude zrejme povoľovať prístup rôznym zariadeniam, ale tento bude obmedzený pri používaní aplikácii s možnosťou aplikovania bezpečnostných zmien, ktoré následné umožnia použitie väčšiny aplikácií. V najvyššej úrovni sú podporované všetky zariadenia, vrátane zákazníckych a prístup do systémov je umožnený aj z extranetu a implementácia mobilného strategického prístupu k vývoju aplikácii a dátam, tj. aplikácie budú optimalizované pre tablety a chytré telefóny.



Obrázok č. 8 – Rôzne úrovne komplexnosti nasadenia BYOD [26].

4.10 Právna zodpovednosť a ochrana

Najdôležitejšou časťou nasadzovania BYOD je zavedenie dohody o používaní zariadení. Táto musí predchádzať implementácii, keďže dodatočné nemusí byť vynútiteľná. Premiešanie osobných a firemných údajov na zamestnancom vlastnených zariadeniach pokrývajú politiky, ktoré môžu do takto dotknutých dát zasahovať - táto informácia musí byť komunikovaná a akceptovaná vopred. Dohoda by mala spĺňať zákonné povinnosti a informovať hlavne o otázkach [10]:

- aká všeobecná politika sa vzťahuje na firemné dáta?
- bude komunikácia a práca monitorovaná?
- bodú sa politiky vzťahovať aj na súkromné údaje?
- aké sú oblasti, ktoré politika pokrýva? Napríklad:
    - textové správy,
    - chat,
    - telefonické a video hovory,

- browsovanie internetu,
- e-maily,
- GPS a iné lokalizačné služby,
- dostupné/inštalované/spustené aplikácie a služby,
- multimediálny obsah (fotografie a videa),
- vzdialená kontrola zariadenia (a jeho súčasti),
- vzdialene vymazávanie,
- čo sa stane v prípade krádeže zariadenia (a povinnosti z toho vyplývajúce).

Cieľom takejto dohody je vyhnúť sa a predchádzať komplikáciám informovaním o právnej zodpovednosti. Zamestnanci musia prijať plnú zodpovednosť za svoje aktivity a chrániť firemné dáta svojim proaktívnym a vedomým konaním.

Druhá strana mince je ochrana používateľských dát pred neoprávneným zásahom do nich: čítanie, zmena alebo zmazanie. Pri nejasných hraniciach medzi osobnými a pracovnými dátami môže IT oddelenie pri prístupe na diaľku zasiahnuť do súkromných dát, ku ktorým nemá oprávnenie.

Bežne využívaný spôsob systému riadenia mobilných zariadení organizáciou v prípade jeho straty je [21]:

- diaľkové zmazanie dát,

- sledovanie GPS pozície.

Z pohľadu práva takáto činnosť spadá nie je nezákonná. V súčasnosti neexistuje žiadna právna úprava ani judikatúra (v USA), ktorá ustanovila precedens. Čoraz bežnejšia je prax žiadať od zamestnanca podpísanie dodatku k pracovnej zmluve, že súhlasí v prípade narušenia bezpečnosti so sledovaním pozície a prípadným zmazaním dát.

Ak ale zamestnanec opustí organizáciu dobrovoľne, rozviazaním pracovnej zmluvy, stane sa získavanie údajov jeho z osobného zariadenie problémom. Nie je právne jasné, či organizácia má právo vzdialene sledovať alebo vymazať obsah osobné zariadenie ex-zamestnanca, aj keď potenciálne obsahuje dáta organizácie. Nevzťahuje sa už totiž naňho žiadna platná pracovná zmluva a teda potenciálne nie je zaviazaný BYOD politikami organizácie. Zákonnosť takejto činnosti je sporná.

Takéto dodatky sú právne sporné. Ak zamestnanec súhlasí s jeho s podpísaním, nezostáva mu než vystaviť osobné dáta vzdialenej kontrole a samotné zariadenie sledovanie v prípade, že si to bezpečnostná situácia bude vyžadovať. Ak zamestnanec odmietne dodatok podpísať, zamestnávateľ nemá inú možnosť, než mu použitie takýchto zariadení obmedziť, prípadne ak je to nevyhnutnou súčasťou jeho pracovných povinností, ukončiť pracovný pomer. Existujú odôvodnené obavy, či sú vôbec tieto dodatky právne záväzné.

Aj keď dal zamestnanec písomný súhlas k aplikovaniu bezpečnostnej politiky BYOD, nezbavuje to v určitých prípadoch organizáciu právnych záväzkov.

Ak v prípade narušenia bezpečnosti použije organizácia vzdialené monitorovanie zariadenie zamestnanca a prístup k dátam, mohol zamestnávateľ omylom zobraziť osobné informácie, ktoré má právny zákaz zisťovať. Napríklad podľa zákazu diskriminácie podľa rasy alebo vierovyznania.

Jednou z výnimiek pri používaní vlastných zariadení je prípad ak je zamestnanec potenciálne predvolateľný v prípade právneho sporu. Túto skupinu tvoria zvyčajne zamestnanci na riadiacich pozíciách. V právnych sporoch s organizáciou bude takmer určite zariadenie používané na pracovné aj súkromné účely súčasťou dôkazových materiálov a jeho obsah sa tak stane verejne prístupným pri súdnom pojednávaní. Tomuto sa dá predchádzať striktným nepoužívaním BYOD zariadení na pracovné účely (a to ani na prijímanie pracovných telefonátov), ale výhradne pre osobné použitie [20].

Nedávne štúdie ukazujú, že zamestnanci majú obavy z BYOD bezpečnostnej politiky, ktoré ovplyvňujú ich súkromie [22]:

- 45% obavy z prístup k osobným údajom IT oddelenia zamestnávateľa,
- 66% má obavy o stratu osobných dát, pri vzdialenom vymazaní,
- 36% chce všetky mať svoje osobné údaje úplne oddelené od organizačných.

Iný spôsob prístupu k právnemu riziku je taktika vyčkávania. Niektoré organizácie sú si vedomé právnych nejasností v politikách BYOD, ktoré by mohli vyústiť do súdnych sporov. Nemajú ale istotu ako správne danú situáciu riešiť. Takéto organizácie nepoužívajú vzdialené vymazanie dát alebo zistenie pozície zariadenia, vystavujú však neprimeranému rizikú firemné dáta, alebo zavádzajú nejasné klauzuly o zodpovednosti do zmluvných dodatkov, ktoré môžu neskor použiť na svoju obhajobu. Oba spôsoby skrývajú potenciálne vysoké náklady pri súdnych sporoch.

Efektívny a zároveň právne jasný spôsob ako zaobchádzať s dátami organizácie na zamestnaneckých zariadeniach musí zabraňovať:

- skopírovaniu dát mimo bezpečnej aplikácie z BYOD zariadenia
- skopírovaniu dát z firemnej siete ak je k nej zariadenie pripojené
- pripojeniu iného zariadenia cez BYOD zariadenie

4.11 Analýza stavu BYOD v konkrétnom prostredí

Prostredie – Sektor A – kancelárie, zamestnanci

Fyzický prístup zabezpečujú čipové karty a kód. Priestor poskytuje základnú infraštruktúru na pripájenie zariadení do siete (notebooky, tlačiarne, tablety) – cez ethernet alebo WiFi. Z bezpečnostného hľadiska je považovaný tento priestor za internet/extranet a preto tu ani žiadne dáta nie sú priamo dostupné.

Prostredie – Sektor B – kancelária, vedenie

Fyzický prístup je riadený rovnako ako v sektore A, čipové karty však musia mať špeciálnu autorizáciu. Pripojenie je možné len cez ethernet, v sektore sa nachádzajú počítače ktoré obsahujú interné firemné dáta. Bezpečnosť dát proti poškodeniu je dosiahnutá šifrovaným zálohovaním do dátového centra. Ochranu dát pred odcudzením zabezpečuje antivírus, vzdialené monitorovanie, IDS a firewall ale v neposlednom rade zaškolením používateľov.

Prostredie – Sektor C – dátové centrum

Tento sektor je fyzicky najneprístupnejší a väčšine zamestnancov ani nie je známa jeho presná lokalita. Vzdialené pripojenie je možné v základnom režime SSH, následne boli pridané služby VPN, VPN-IPSEC, RemoteDesktop. Obsahuje serverové vybavenie, na ktorom sú prevádzkované databázy (testovacie, vývojové a produkčné), zálohovací systém a diskové pole. Softvérové zabezpečenie je obdobné ako v sektore B, antivírus má ale vyššie zaťaženie kôli zdieľanému diskovému poľu.

Zamestnanci si čoraz častejšie kupovali vyspelejšie zariadenia (notebooky a časom aj chytré telefóny), než tie, čo dostávali od firmy. Tieto zariadenia používali na pracovné úlohy namiesto firemných. Firma si toto správanie zamestnancov všimla a na začiatkoch ho tolerovala. Časom sa z tohto okrajového trendu stal mainstream, ktorý mal potenciál znížiť

náklady na obstaranie a údržbu zamestnaneckých - používateľských zariadení [14]. Firma preto aktívne pristúpila k prijatiu tohto trendu za súčasť internej stratégie.

Firma eviduje množstvo zamestnaneckých zariadení a aktívne podporuje používanie súkromných notebookov, dátovýc nosičov ako sú napr. USB disky, chytré telefóny a tablety. Notebooky umožňujú efektívnejšie pracovať, keďže parametre si zvolí sám podľa jeho úloh a potrieb (dual-display vs. veľký display vs. ultrabook). Tablety a chytré telefóny prinášajú nové možnosti na testovanie softvérových produktov na rôznych zariadeniach.

Firma rieši oddelenie firemných a súkromných dát len na úrovni aplikácií. Telefonické a e-mailove kontakty zamestnancov firma nepovažuje za kritické a ani ich ako také nechráni inak než internými nariadeniami. Oddelenie súkromných dát a aplikácií je možné vďaka tomu, že dáta nie sú samostatne spracovávané mimo nich a tiež výhradným používaním tenkých klientov, resp. interných webových aplikácií. Oddelenie je zavŕšené použitím virtualizácie (VirtualBox, VMWare), ktoré navyše rieši právne šedú oblasť použitia licencovaného softvéru na súkromnom zariadení. Virtualizácia prináša ďalšiu výhodu a to možnosť pracovať z domu, prípadne poskytovať podporu produkčným aplikáciám mobilne [12].

Virtualizácia samotná je zabezpečená dodatočne, použitím šifrovania virtuálnych diskov.

Vo firme sa IT oddeleniu podarilo zvládnuť podporu rôznych zariadení zavedením štandardných virtualizačných nástrojov (ktoré majú vlastnú podporu a sú pravidelne aktualizované) a tiež požívaním webových aplikácií a kompatibilných webových prehliadačov.

Firma nepoužila v implementácii BYOD žiadne intruzívne a reštriktívne politiky.

Bezpečný prístup k internej sieti, resp. aplikáciám v dátovom centre zabezpečuje firma používanim VPN a generovaním unikátnych certifikátov pre každého zamestnanca. VPN prístup je teda viazaný na konkrétnu zodpovednú osobu.

Pripojenie cez WiFi v sektore A nie je nijak špeciálne regulované – chápe sa ako nezabezpečený internet a prístup je riadený heslom a WPA2 šifrovaním. Prístup do tejto siete dostávajú zvyčajne aj návštevy firmy a teda potenciálne nezabezpečené a zavírené počítače.

Vo firme je pridanie nového zariadenia, resp. zamestnanca poloautomatizované. Zamestnancovi je vygenerovaný unikátny platný elektronický certifikát a je mu vysvetlený spôsob jeho použitia pri vzdialenom prístupe. Bez vlastníctva tohto certifikátu, resp. počas obdobia jeho neplatnosti, nemôže zamestnanec vykonávať žiadne činnosti ani pristupovať k aplikáciám, resp. dátam, okrem používania kancelárskeho vybavenia (tlačiarne) a aj to len v prípade ak sa nachádza v sektore A.

Firemné interné predpisy sa v tomto smere nesnažia vytvárať dojem vynútenej bezpečnosti – uplatňovanie bezpečnostných politík je teda tvorené organizačným nariadením a jeho dodržiavanie je kontrolované pri servisnej údržbe, resp. inštalovaní virtualizácie.

Agregovanú sieťovú viditeľnosť zabezpečuje vo firme implementované IDS, ktoré spracováva okrem iného aj bezpečnostný žurnál o použitiach certifikátov. Poskytuje tak prehľad o aktívnych aj minulých pripojeniach a štatistické údaje o nich (objem prenesených dát, zdrojový systém). Systém umožňuje unifikovať aj zariadenia nepoužívajúce certifikáty ale pripojené k sieti a tieto následne zgrupovať a analyzovať z pohľadu rôznych rezov, resp. dimenzií. Systém poskytuje rôzne pravidelné a aj výnimkové (narušenie bezpečnosti, pokus o použitie neplatného certifikátu) výstupy (sms notifikácia, zasielanie zoznamu podozrivých operácií e-mailom).

Firma poskytuje zamestnancom oba prístupy v kombinovanej forme – virtualizované prostredie nad šifrovanými diskami. Samotné prostredie navyše neobsahuje priamo žiadne citlivé dáta.

Použitie interných webových aplikácií, ktoré ukladajú svoje dáta do zálohovaných databáz je ďalší spôsob, ktorý zabraňuje poškodeniu dát.

Prístupy zamestnanca sú deaktivované v dvoch fázach, najprv je deaktivovaný (zneplatnený) jeho certifikát, čím sa mu znemožní prístup do aplikácií a je mu deaktivovaný prístupový čip, čím sa mu odoberie fyzický prístup. Následne, v druhej fáze, sú mu deaktivované jednotlivé účty v konkrétnych interných aplikáciách.

Firma je použitím virtualizácie a fyzickým oddelením lokalít v situácii, kedy jej bežná činnosť je nerozoznateľná od vzdialenej práce. Zamestnanci sa rovnakým spôsobom prihlasujú do systémov bez ohľadu na to, či sa nachádzaju v sektore A, doma, alebo u zákazníka. Podmienkou takéhoto použitia je však dostupnosť pripojenia na internet a jeho

priemerná stabilita. V prípade nedostupnosti štandardnej internetovej konektivity je možné použiť mobilný internet cez chytré telefóny. Použitie tenkých aplikačných klientov však zabezpečuje, že objem prenášaných dát nebude veľký a aj na takomto úzkom prenosovom pásme sú aplikácie reálne použiteľné.

Virtualizácia priniesla firme ešte jednu veľkú výhodu – ak sieť zákazníka vyžaduje použitie nekompatibilnej VPN, môžu táto aj s firemnou bežať paralelne v samostatných virtuálnych počítačoch na jednom zamestnaneckom notebooku, čím sa zvýši jeho produktivita oproti klasickému spôsobu – manuálne prepínanie sa do jednotlivých VPN sietí. Zamestnanci majú túto výhodu navyše dostupnú nielen v priestoroch firmy, ale aj doma, pri vzdialenej podpore zákazníckych systémov.

Použitie interných aplikácií je podmiennené pripojením sa cez inštalovaný VPN softvér vo virtualizovanom počítači. Túto stratégiu považuje za najmenej invazívnu. Stratégia navyše jasne ošetruje nejasnosti pri používaní softvérových licencií na súkromnom zariadení.

Právne stránky používania zamestnaneckých zariadení sú riešené dodatkom k zamestnaneckej zmluve. Táto zmluva pokrýva:

- zodpovednosť za činnosti nesúvisiace s pracovnými úlohami,
- oboznamuje s rozsahom monitorovania aktivít (IDS, prístupy k aplikáciám, analýza metadát),
- kategorizuje dáta a prístupy k nim (dáta interných aplikácií, dáta v špeciálnom režime),
- špecifikuje prístupy a bezpečné použitie jednotlivých aplikácií (a povinnosti z toho vyplývajúce),
- vlastníctvo dát a spôsoby ich použitia zamestnancom (zahŕňa zákaznícke údaje)
- korektné použitie telefonických a e-mailových kontaktov,
- fair-use, eticky korektné využívanie internej infraštruktúry (priestory, internet, tlačiarne),
- použitie softvéru a softvérových licencií,
- postup pri krádeži a kontaktné osoby.

Firma si nenárokuje mať možnosť vzdialeného prístupu, kontroly a manipulácie s virtualizovaným počítačom, keďže na ňom obsiahnuté dáta sú zo zásady nespadajúce do kategórie chránených.

4.12 Odporúčania pri novej implementácii BYOD

Na základe zozbieraných teoretických poznatkov a analýzy implementácie v konkrétnom ekonomickom prostredí firmy odporúčame pri budúcich implementáciách použiť nasledovné kroky:

4.12.1 Definovanie požiadaviek

Určenie množiny cieľových zariadení

Prvým krokom je vybrať typy prístrojov a operačných systémov, ktoré je organizácia schopná podporovať. Nie je možné normalizovať riadenia pre mobilné zariadenia, pretože každý operačný systém, a dokonca aj hardvérmôže ovplyvniť rozsah možností IT oddelenia. Východiskové hodnotiace kritériá politiky mobilných zariadení, pri posudzovaní operačných systémov a typov zariadení sú nasledovné:

Z pohľadu bezpečnosti:

- podpora šifrovania,
- schopnosť identifikovať,
- vzdialená uzamykateľnosť a mazanie,
- vzdialená lokalizácia.

Z pohľadu manažovateľnosti:

- softvérové alebo hardvérové riadenie zariadenia,
- možnosť použit a preberať vzdialené politiky.

Z aplikačného pohľadu:

- dostupnosť kľúčových aplikácií pre produktivitu,
- dostupnosť ostatných aplikácií, ktoré umožnia dodatočné zvýšenie produktivity,
- možnosť inštalovať vlastné, interné aplikácie.

Na základe týchto kritérií určiť typy zariadení a operačné systémy, ktoré bude organizácia podporovať.

Sieťová dostupnosť

Následne je nutné vytvoriť prostredie, ktoré umožnia BYOD novým zariadeniam registráciu. Najjednoduchší spôsob je vytvoriť WiFi sieť, oddelenú od interných komponentov. Táto bude slúžiť výhradne na registráciu nových zariadení a ich previazanie na konkrétne osoby. Po zaregistrovaní zariadenia by mali interné systémy riadenia mobilných zariadení prideliť prislúchajúce práva a obmedzenia podľa stanovených bezpečnostných politík pridelených jednotlivých používateľom.

Základné práva by mali zahŕňať prístup k e-mailu, firemnej WiFi (iná ako registračná) a nastaveniu prístupov pre použitie VPN spojenia. Tieto práva a prístupy by mali byť popísané v bezpečnostnej politike organizácie. Zariadenia, ktoré neumožňujú dodržanie bezpečnostnej politiky by mali mať prístup do interných systémov zablokovaný. Za takéto zariadenia považujeme napríklad tie, ktoré majú nainštalované zakázane aplikácie.

Poskytovanie prístupu cez centralizované riadenie má výhody pre organizáciu aj pre zamestnancov:

- zamestnanci získavajú prístup rýchlo a bez nutnosti kontaktovať IT oddelenie,
- WiFi heslá môžu byť často menené bez nutnosti ich zverejňovať,
- ochrana pred dodatočne zistenými nebezpečnými aplikáciami prebehne automaticky.

Správa politík

Poslednou zložkou pripravenosti IT oddelenia je správa politík a obmedzení zamestnaneckých zariadení. Tieto rozdeľujeme do nasledovných kategórií:

- Politikami riadená správa - informácie o zamestnancoch sú uložené v centrálnom internom systéme (napr. LDAP, Active Directory). Pripojením bezpečnostných profilov a aplikovaním politík na ich mobilné zariadenia sa správa používateľov a zariadení zjednoduší.
- Bezpečnosť - vytvorenie základnej bezpečnostnej politiky, ktorá sa aplikuje, ak zariadenie prestane byť v súlade s požiadavkami. Ďalšie kroky by mali byť:
    - vytvorenie pravidiel pre používane heslá
    - zoznam zakázaných aplikácií
    - zoznam nepovolených nastavení systému

- Správa dokumentov - ak organizácia plánuje poskytovať zamestnancom bezpečný prístup k firemným dokumentom, odporúčame implementovať centrálne spravované úložisko dokumentov, ktoré je previazané s bezpečnostnými politikami. Tým umožňuje IT oddeleniu zmazať súbory podľa potreby. Je to najjednoduchší model pre zabezpečenie firemných dát pri rešpektovaní vlastníctva zariadenia a používateľsého komfortu práce.

4.12.2 Právne otázky

Najvýznamnejšou výzvou IT oddelenia pri implementácii BYOD je udržať rovnováhu medzi vynucovaním bezpečnosti interných systémov a rešpektovaním súkromných dát zamestnanca na zariadení. Keďže sa jedná o tak citlivú otázku, považujeme za nutné formálne popísať tento vzťah.

Politika mobilných zariadení - je to komplexný dokument, ktorý by mal zahŕňať konkrétne požiadavky organizácie, založený na odporúčaniach poskytnutých rôznymi internými zainteresovanými stranami, vrátane všeobecného právneho poradcu, IT oddelenia, ľudských zdrojov, zamestnancov a ďalších.

Každá bezpečnostná politika je jedinečná, ale mala by sa zaoberať niektorými alebo všetkými z týchto aspektov:

- Zoznam kritérií:
    - definuje zodpovednosť,
    - definuje porušenie bezpečnostnej politiky, vrátane dôsledkov,
    - vymedzuje súbor štandardov, bez uvádzania detailov.
- Používatelia a financovanie:
    - definuje použitie zariadení zamestnancami,
    - definuje, ako budú požiadavky na bezpečnosť oznamované zamestnancom,
    - stanovuje prípadné náhrady za opakujúce sa náklady zamestnancov,
    - definuje podporu kontraktorov pri používaní vlastných zariadení v podnikovej sieti.
- Právne aspekty:
    - popis právnej vymožiteľnosť,
    - popisuje zákony krajiny na ochranu súkromia dát a ich obmedzenie v súvislosti s bezpečnostnými opatreniami a vyžadované súhlasy,

    - právo na audit a kontrolu činnosti na osobných zariadeniach a prípadných obmedzeniach vyplývajúcich z miestnych zákonov a predpisov,
    - rozlíšenie právnych záväzkov používateľov a organizácie pri používaní licencií a aplikácií,
    - udelenie súhlasu spoločnosti prístupovať k zariadeniam za pracovnými účelmi,
    - postup ako odregistrovať zariadenie a ako zmazať citlivé dáta organizácie,
    - stanovuje povinnosť zamestnanca nahlásiť stratu zariadenia a právo zamestnávateľa na jeho diaľkové vymazanie.
- Ľudské zdroje:
    - detaily možných činností organizácie nad firemnými dátami na zariadení,
    - bezpečnostné politiky, ktoré sa vzťahujú na zariadenie aj mimo pracovných hodín,
    - bezpečnostné školenia zamestnancov.

Dodatky k pracovnej zmluve zamestnancov

Tento dokument len potvrdzuje súhlas zamestnanca s dokumentom Politika mobilných zariadení. Súhlasom s týmto dokumentom berie zamestnanec na vedomie, že IT oddelenie má právo a schopnosť zabezpečiť mobilné zariadenie a údaje, ktoré obsahuje, v prípade potreby.

Dodatky k pracovnej zmluve sú dôležité, pre prípadnú budúcu situáciu, že zamestnanec poprie znalosť bezpečnostných politík mobilných zariadení. Keďže zamestnancov súhlas umožňuje IT vykonávať bezpečnostné opatrenia, vrátane zmazania niektorých alebo všetkých dát na zariadení a prípadne zabavenie zariadenia, je dôležité, aby organizácia vedela preukázať svoje právo vykonávať tento typ činnosti. Dodatky zamestnancov by mali byť preto uschované a byť dostupné v prípade právnej potreby.

4.12.3 Implementácia systému riadenia prístupu mobilných zariadení

Po zozbieraní všetkých požiadaviek a ich spracovaní, treba vybrať príslušnú softvérovú aplikáciu, ktorá umožní správne riadiť a zabezpečiť firemné a zamestnanecké mobilné zariadenia.

Podobne ako u kritérií, použitých pri posudzovaní rôznych typov operačných systémov a typov zariadení, je potrebné zabezpečiť, že vybrané riešenie schopné zabezpečiť požadované funkcie. Toto určíme vyhodnotením nasledovných kritérií:

- Flexibilita platformy:
    - jednoduchosť inštalácie do existujúceho prostredia,
    - využitie existujúceho zabezpečenia a sieťovej infraštruktúry,
    - nároky na prispôsobenie do požadovanej podoby,
    - schopnosť riadiť všetky typy zariadení a operačných systémov prostredníctvom jednotného systému.
- Administrácia:
    - správa založená na bezpečnostných profiloch,
    - správa a distribúcia mobilných interných a komerčných aplikácií.
- Bezpečnosť:
    - použitie viacerých politík na jedno zariadenie, napríklad základné plošné bezpečnostné nastavenia pre všetky zariadenia, ale oddelené práva a obmedzenia podľa používateľských profilov,
    - automatické presmerovanie nevyhovujúcich zariadení ,
    - bezpečná distribúcia a správa dokumentov,
    - schopnosť diaľkového vymazania.

5 Diskusia

Z popísaného stavu implementácie BYOD vo firme je zrejmé, že sa firma touto oblasťou aktívne zaoberá a využíva ju na zníženie svojich priamych nákladov na vybavenie zamestnancov.

Z odporúčaní štandardov zavádzania BYOD pokrýva implementácia bezpečnosti BYOD vo firme nasledovné oblasti:

- pridávanie, správu a odoberanie prístupov,
- oddelenie citlivých zdrojov od nezabezpečených,
- autentifikáciu a autorizáciu používateľov,
- vymedzenie právnej zodpovednosti a odporúčaní,
- bezpečnostné školenia,
- kategorizáciu a stupne ochrany dát.

K úplnej implementácii bezpečnosti chýbajú časti:

- formálne zdokumentované postupy aktualizácie,
- možnosti vzdialenej kontroly,
- možnosť vynútenia bezpečnostnej politiky,
- presnejšia evidencia používania infraštruktúry,
- audit prístupov a kontrol,
- pravidelná zmena hesiel, zadokumentovanie a audit takýchto zmien.

Firme teda chýba hlavne formálne podchytenie implementácie a vynucovanie politiky.

Za negatívum považujeme tiež neexistenciu dokumentu, ktorý popisuje činnosť správcov systému, čo môže spôsobiť ich nenahraditeľnosť (či už v pozitívnom alebo negatívnom zmysle). Jeho neexistencia môže spôsobiť škody pri dočasnom zastupovaní kľúčových administrátorov menej skúsenými kolegami a má tak potenciál ohroziť nimi poskytovanú dlhodobo budovanú bezpečnosť a spoľahlivosť.

Neexistencia vzdialenej kontroly nad virtualizovanými prostrediami vystavuje firmu zbytočnému riziku zneužitia softvérových licencií. Vhodným riešením by bola inštalácia vzdialenej, časovo obmedzenej automatickej deaktivácie licencií.

Riešenie virtualizáciou prináša nepriame riziko vo forme nechceného prepojenia dvoch VPN systémov. V prípade, že používateľ nedodrží povinnosť použiť dva virtualizované počítače paralelne, ale pripojí hostiteľský počítač do jednej VPN a hostovaný virtualizovaný počítač do druhej VPN, umožní tým druhej VPN prístup do prvej VPN, čím ohrozí ich vzájomnú bezpečnosť. Takáto situácia v histórii firmy skutočne nastala. Zakázanie vnorenej VPN však nie je vynútené (takúto možnosť poskytuje napr. VPN riešenie firmy Checkpoint).

Pri odcudzení zariadení s virtualizovaným prostredím dochádza k strate jeho konfigurácie a vytvára tak dodatočnú potrebu inštalácie a konfigurácie. V tomto smere odporúčame použiť automatické zálohovanie snapshotov virtualizovaných diskov na lokálne diskové pole v sektore A. Následný automatizovaný presun na diskové pole v sektore C, kde bude bezpečne zálohované a dostupné v prípade potreby. Toto riešenie je vyžaduje vytvorenie diskového poľa v sektore A, ktoré bude používané ako dočasné úložisko. Potenciálne negatívum tohto riešenia je nutnosť byť dostatočnú dobu pripojený k dostatočne rýchlej sieti, aby bolo možné skopírovať aktuálny snapshot virtualizovaných diskov, čo je pri aktuálnych rýchlostiach siete v sektore A v pomere k priemernej veľkosti virtualizovaných diskov približne 10minút a teda nepovažujeme toto obmedzenie za významnú technickú prekážku.

Ďaľšie odporúčanie na zlepšenie implementácie je zavedenie jednotnej správy používateľov napríklad cez systém LDAP, čím sa zjednoduší ich správa a tiež sprehľadní budúci dokument popisujúci činností a procesov správcov. Ďalším krokom po zavedení LDAP by malo byť implementovanie systému Single-Sign-On (SSO), ktorý umožňuje jednotné, jednorazové prihlásenie aj odhlásenie zo všetkých aplikácií.

Za najprekvapivejší bod v implementácii považujeme existenciu a vysokú kvalitu zmluvného dodatku vymedzujúceho práva a povinnosti pri používaní osobných zariadení zamestnancami. Firma tak účinne predchádza právnym rizikám pri použití BYOD zariadení. Predpokladáme, že je to dôsledok predchádzajúcich negatívnych skúseností z doby, keď takýto dodatok neexistoval, resp. nebol takto do detailov prepracovaný.

Neexistenciu implementácie BYOD na chytrých telefónoch firmou vysvetľuje fakt, že firma sa týmto segmentom zákazníckych zariadení nezaoberá a nemá pre ne ani špeciálne vyvíjané aplikácie. Nepovažujeme teda nepokrytie žiadnou metodológiou za chybu.

V poslednom rade chceme ohodnotiť bezpečnosť sektoru B, ktorý má síce špeciálne kontrolovaný fyzický prístup, ale je prepojený počítačovou sieťou so sektorom A. Informačná bezpečnosť v ňom je zabezpečovaná inštaláciou antivírusov a firewallov na jednotlivých počítačoch. Naše odporúčanie je pristupovať k tomuto sektoru z pohľadu bezpečnosti rovnako ako k sektoru C a teda uzavrieť ho do samostatnej zóny, prístupnej z extranetu len cez VPN a zabezpečenú kombináciou NAT+firewall.

Súčasný stav zapezbečenia informačných systémov firmy a formu implementácie považujeme teda za krok správnym smerom. Výzvou pre firmu je udržať nastolený štandard, pravidelne revidovať bezpečnostnú politiku a zvážiť implementáciu nami spomenutých odporúčaní.

Záver

Bezpečnosť informačného systému tvorí nezanedbateľnú časť pri jeho vývoji, implementácii a údržbe. Svojou zložitosťou a dôležitosťou sa vyrovná ostatným častiam vývojového cyklu informačných systémov. Jej nepresnosť, neúplnosť či prípadné úplné ignorovanie však môže viesť k veľkým škodám na aktívach firmy – o to viac, že hrozba takýchto škôd (či už úmyselných alebo neúmyselných) je v dnešnej dobe reálna a nielen hypotetická.

V práci sme načrtli všeobecné prístupy k informačnej bezpečnosti a jej rôzne charakteristiky a úskalia. Práca plynulo nadviazala na popis aktuálneho trendu akceptovania a využívania osobných zariadení vo firemnom prostredí a na pracovné úlohy. Tento trend prináša nové výzvy a úlohy na riešenie pre IT oddelenie, v nemalej miere je však zaťažené aj právne oddelenie – prácou na formalizovaní dohôd so zamestnancami a ich pravidelnou aktualizáciou v spolupráci s IT oddelením. Spôsob akým bude firma akceptovať zamestnanecké zariadenia, vyplynie z prvotného rozhodnutia vedenia o stratégii zavádzania BYOD a následne v jeho implementácii IT oddelením. Toto môže byť v rozsahu od striktného zákazu, až po rýchle a bezproblémové automatické pripojanie s možnosťou okamžite využívať dané zariadenie na pracovné úlohy. Cieľom BYOD by však malo byť pripojenie zariadení pri udržaní informačnej bezpečnosti a komfortu bežnej práce.

Práca prináša ucelený prehľad výhod a rizík súvisiacich s implementáciou BYOD na konkrétnom príklade firmy a tiež zhŕňa všeobecné odporúčania pre budúce implementácie. Môže sa tak stať zdrojom cenných informácií pre zamestnancov IT oddelení.

Z dôvodov spomenutých v metodickej časti sme sa bohužiaľ nemohli venovať praktickému overeniu bezpečnosti a záťažovým testom interných aplikácií, ktoré boli pôvodne súčasťou našich cieľov. Napriek týmto obmedzeniam si myslíme, že práca poskytuje dostatočne veľký vhľad do teórie informačnej bezpečnosti v oblasti BYOD, v primeranej miere popisuje implementáciu na konkrétnom modeli a popisuje postupy na lepšie zvládnutie prípadnej budúcej implementácie.

Priestor na ďalší výskum vidíme v už spomenutých záťažových testoch, bezpečnostných auditoch interných aplikácií, overení funkčnosti IDS, prípadne v praktickej implementácii spomínaného prechodu na LDAP, či SSO riešenie. Ďalším, v tejto práci neriešeným, prvkom informačnej bezpečnosti vhodným na spracovanie, by mohlo byť popis architektúry databázových aplikácií, ktoré firma vyvíja, resp. používa počas vývoja.

Zoznam použitej literatúry

[1] HOWARD, M. – LEBLANC, D. – VIEGA, J., 2005. *19 Deadly Sins of Software Security–Programming Flaws and How to Fix them*. New York : McGraw-Hill/Osborne, 2005.

[2] Kaspersky Lab, 2013. *KASPERSKY SECURITY BULLETIN 2013*. Kaspersky Lab, 2013. Dostupné na internete: < http://media.kaspersky.com/pdf/KSB_2013_EN.pdf >

[3] WHITMAN, M., 2003. *Enemy at the Gates: Threats to Information Security*. Communications of the ACM, 46/8

[4] Gartner Press, 2013. *Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013*. Gartner. Dostupné na internete: <http://www.gartner.com/newsroom/id/2408515>

[5] SETHURAMAN, S., 2006. *Framework for Measuring and Reporting Performance of Information Security Programs in Offshore Outsourcing*. Dostupné na internete: <http://www.isaca.org/Journal/Past-Issues/2006/Volume-6/Pages/JOnline-Framework-for-Measuring-and-Reporting-Performance-of-Information-Security-Programs-in-Offshore-Outso1.aspx>

[6] Gartner Press, 2013. *Forecast: Devices by Operating System and User Type, Worldwide, 2010-2017, 1Q13 Update*. Gartner. Dostupné na internete: <http://www.gartner.com/resId=2396815>

[7] Cisco Systems, Inc., 2014. *Device Freedom Without Compromising the IT Network.* Dostupné na internete: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf

[8] GRANCE, T. – HASH, J. – STEVENS, M. 2003, *Security Considerations in the Information System Development Life Cycle 800-64*. NIST. Dostupné na internete: <http://www.albany.edu/acc/courses/ia/acc661/NIST-SP800-64.pdf>

[9] KISSEL, R. a kol. 2008. *Security Considerations in the Information System Development Life Cycle 800-64 Revision 2.* NIST. Dostupné na internete: <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

[10] Intel Corp., 2012. *Improving Security and Mobility for Personally Owned Devices*. Dostupné na internete: <http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/improving-security-and-mobility-for-personally-owned-devices-paper.pdf>

[11] PAUL, F. 2013. *What A Typical BYOD Program Really Looks Like*. Dostupné na internete: <http://readwrite.com/2013/01/18/readwrite-survey-results-what-a-typical-byod-program-really-looks-like>

[12] Deloitte LLP, 2013. *Understanding the BYOD landscape*. Dostupné na internete: <http://www.deloitte.com/assets/Dcom-Guam/Local%20Assets/Documents/Technology,%20Media%20and%20Telecommunications/Understanding%20the%20bring-your-own-device%20landscape.pdf>

[13] DERNBECHER, S. – BECK, R. – WEBER, S. 2013. *Switch to Your Own to Work with the Known: An Empirical Study on Consumerization of IT*. Dostupné na internete: <http://ginevra.btoresearch.com/images/freepaper/165_Switch%20to%20Your%20Own%20to%20Work%20with%20the%20Known_%20An%20Empirical%20Study%20on.pdf>

[14] LANG, B. 2012. *Best Practices for Embracing BYOD*. Dostupné na internete: <http://health-information.advanceweb.com/Features/Articles/Best-Practices-for-Embracing-BYOD.aspx>

[15] ADLER, P.M., 2006. *A Unified Approach to Information Security Compliance*. Dostupné na internete: <http://www.educause.edu/ero/article/unified-approach-information-security-compliance>

[16] REDWINE S. T., Sept. 2006. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.1*. US Department of Homeland Security, 2006. Dostupné na internete: < http://www.omg.org/news/meetings/workshops/SWA_2007_Presentations/00-T1_Redwine_Supplement.pdf >

[17] GartnerPress, 2012. *Emerging Technologies Hype Cycle: Whats Hot for 2012 to 2013*, GartnerPress, 2012. Dostupné na internete: <http://www.infoq.com/news/2012/08/Gartner-Hype-Cycle-2012>

[18] Enterprise CIO Forum, 2014. *BYOC: Bring Your Own Cloud or Bring Your Own Confusion?*, Enterprise CIO Forum, 2014. Dostupné na internete: <http://www.enterprisecioforum.com/en/blogs/katerinam/byoc-bring-your-own-cloud-or-bring-your>

[19] SPRING T., 2014. *Horror Stories: Top 5 BYOD Threats*. CRN, 2014. Dostupné na internete: <http://www.crn.com/news/mobility/300072711/horror-stories-top-5-byod-threats.htm>

[20] DOHERTY S., Mar. 2013. *BYOD is not for everybody, and especially not for executives*. TechRepublic, 2013. Dostupné na internete: < http://www.techrepublic.com/blog/tech-decision-maker/byod-is-not-for-everybody-and-especially-not-for-executives/8220/>

[21] Route1 Inc., Sept. 2013. *Avoiding BYOD Legal Issues*. Route1 Inc., 2013. Dostupné na internete: <https://www.route1.com/thought-leadership/item/download/88_633115bd25f49cf2e2b3099a3b7ddc4e.html>

[22] Aruba Networks, 2013. *Employees tell the truth about your company's data*. Aruba Networks, 2013. Dostupné na internete: <http://www.arubanetworks.com/pdf/solutions/EB_mdmreport.pdf>

[23] METCALFE B., Dec. 1973. *The Stockings Were Hung by the Chimney with Care*. Arpa Network Working Group, 1973. Dostupné na internete: <http://www.rfc-base.org/txt/rfc-602.txt>

[24] EDMEAD M., T., Máj 2007. Understanding the Risk Management Process. CISSP, CISA, 2007. Dostupné na internete: <http://www.theiia.org/intAuditor/itaudit/archives/2007/may/understanding-the-risk-management-process/>

[25] ReadWrite, 27. Február 2013. *BYOD Security: Yes, It IS Possible To Have A Secure Bring Your Own Device Program*. ReadWrite Inc., 2013. Dostupné na internete: <http://readwrite.com/2013/02/26/security-basics-of-byod>

[26] Global Knowledge, 2012. *Bring Your Own Device (BYOD) Cisco Training*. Global Knowledge Training LLC, 2012. Dostupné na internete: <http://www.globalknowledge.net/Certifications/Cisco-Certifications/Bring-Your-Own-Device-BYOD-Cisco-Training/>

[27] PAIKEDAY T., 12. August 2012. VMware Mobile Secure Desktops – built on Cisco VXI. Cisco Corp, 2012. Dostupné na internete: <http://blogs.cisco.com/datacenter/vmware-mobile-secure-desktops-built-on-cisco-vxi/>

[28] Office of the Information Commissioner, 6. Marec 2013. *Use of portable storage devices*. Office of the Information Commissioner, 2013. Dostupné na internete: <http://www.oic.qld.gov.au/__data/assets/pdf_file/0012/21306/portable-storage-device-policy.pdf>