Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnostní audit a politika IT organizace

Vypracoval: Bc. Leoš Turnovský
Vedoucí diplomové práce: Ing. Eva Červenková

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Bezpečnostní audit a politika IT organizace" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Evě Červenkové, vedoucí mé diplomové práce, za rady poskytnuté k vyhotovení závěrečné práce.

Bezpečnostní audit a politika IT organizace

Security Audit and IT organization

Souhrn

Tato práce se zabývá tématem bezpečnostního auditu a politiky IT organizace. Cílem této diplomové práce bylo provést interní audit bezpečnosti IT ve zvolené části informačního systému podniku.

Teoretická část je věnována problematice a obecnému postupu provádění auditu bezpečnosti IT. Vysvětleny jsou zde principy bezpečnosti informací. V této části je rovněž vysvětlena metodika řízení rizik a souhrn norem, které s auditem bezpečnosti IT souvisí, jako COBIT, ITIL a ISO 17799.

V praktické části je popsán postup provedení auditu. V první třetině praktické části jsou zdokumentovány podmínky a prostředí auditu. V druhé třetině je popsán stav bezpečnosti IT v době konání auditu. V poslední třetině praktické části jsou uvedena doporučení pro zvýšení bezpečnosti informací. V závěru jsou výsledky auditu shrnuty.

Summary

This thesis deals with security audit and IT policy of organization. The objective of this thesis was to conduct an internal audit of IT security in selected partition of the company information system.

The theoretical part is devoted to the matter and general procedure of auditing IT security. There are explained the principles of information security. This section also explains the risk management methodology and a set of standards that the audit of IT security is related to such as COBIT, ITIL and ISO 17799.

The practical part describes how to perform an audit. In the first third of this part are documented practical conditions and environment of the audit. In the second third is described state of IT security at the time of the audit. In the last third are provided practical recommendations to improve information security. In conclusion, the results of the audit are summarized.

Klíčová slova: audit, bezpečnost, IT, IS, politika, organizace, kontrola, hrozba, riziko

Keywords: audit, security, IT, IS, policy, organization, control, threat, risk

Obsah

1. Úvod

S rozšiřováním znalostí lidské společnosti přicházejí nové způsoby obživy a nové priority, na které společnost klade důraz. Zemědělskou společnost vystřídala společnost průmyslová. V současné společnosti mají více, než kdy předtím klíčovou roli informace. Proto lze říci, že v soudobém historickém období je průmyslová společnost střídána informační společností. Včasné, správné, přesné a především užitečné informace mají strategickou hodnotu, mnohdy obtížně vyjádřitelnou v penězích. Informační společnost využívá nejrůznější způsoby sběru, uchování, vyhodnocování a předávání informací. Na spolehlivém přístupu ke kriticky důležitým informacím je někdy založena hlavní činnost podniku. Spolehlivý přístup k informacím je rovněž nezbytný např. pro fungování státu. K informacím je přistupováno prostřednictvím informačního systému.

Rolí subjektu v informační společnosti není jen získávat informace a pak k nim přistupovat, ale zároveň zabránit, nebo alespoň oddálit, aby k pracně nabytým informacím přistupovaly konkurenční subjekty. Právě v této oblasti hraje klíčovou roli bezpečnostní audit informačního systému. Ne však ve smyslu vynalézání nových způsobů manipulace s informacemi, ale v organizaci a uceleném přístupu k zavádění účinných bezpečnostních opatření v praxi. Hlavním smyslem auditu bezpečnosti IS je poskytnout přehled o současném zabezpečení informačního systému a navrhnout takové řešení, aby náklady na zavedení takového řešení úměrně odpovídaly hodnotě informací, které je potřeba chránit. Neméně důležitým aspektem informačního systému je jeho spolehlivost v souvislosti s přístupem k informacím. Audit bezpečnosti informačního systému se rovněž zaměřuje na kontrolu opatření proti výpadkům v poskytování služeb.

2. Cíl práce a metodika

Cílem této diplomové práce bylo provést interní audit bezpečnosti IT ve zvolené části informačního systému podniku. Dílčí cíle práce byly následující:

- zhodnotit vnitřní směrnice o IT bezpečnosti a ověřit jejich dodržování
- vyhodnotit hrozby a rizika zadané části informačního systému
- formulovat doporučení na základě předchozích šetření
- odhadnout účinek navrhovaných opatření na bezpečnost informací
- odhadnout účinek navrhovaných opatření na rozpočet a odhadnout náklady na zavedení navrhovaných opatření do praxe

Předmětem auditu bezpečnosti bylo pro diplomovou práci zvoleno detašované prodejní call centrum modelového podniku, který byl pro účely práce vytvořen podle předlohy reálného podniku poskytující telemarketingové služby. K tomuto kroku bylo přistoupeno kvůli důvěrnosti auditorské činnosti. Audit byl metodicky proveden ve čtyřech krocích:

1) porozumění IT architektuře podniku
2) zjištění stavu bezpečnosti IT
3) zhodnocení stavu bezpečnosti
4) vytvoření doporučení pro snížení bezpečnostních rizik.

Jako rámec metodiky byly využity principy bezpečnosti IS/IT norem COBIT, ITIL a ISO 17799.

3. Přehled řešené problematiky

3.1. Vývoj auditu

Počátky auditorství sahají do dávné historie. Vládci starověkých civilizací pověřovaly důvěryhodné osoby, které měly za úkol zaznamenávat stav majetku hospodářských jednotek. Slovo audit pochází z lat. naslouchat. Z důvodu rozšířené negramotnosti byly auditorovi potřebné údaje předávány ústně. Později k této činnosti přibyla kontrola finančního hospodaření a veřejných účtů. S rozvojem účetnictví ve středověku došlo i k rozvoji auditorství. Auditoři v tomto období historie kontrolovali kopie účtů a zastávali dozorčí funkce. Do první poloviny 20. stol. bylo auditorství spojeno výhradně s účetnictvím. S nástupem informačních systémů do podnikového využití byl do finančního auditu zařazen jako doplněk audit informačních systémů. Na konci druhé poloviny 20. stol. byla založena asociace auditorů EDP (Electronic Data Processing) a o deset let později se transformovala do organizace ISACA (Information Systems Audit and Control Association). Díky činnosti ISACA se audit IS vyvinul v samostatnou disciplínu. V současnosti je úlohou ISACA sdružovat auditory IS a udělovat certifikace. [1; 2]

3.2. Definice auditu

Pojem audit lze interpretovat jako nejvyšší stupeň kontroly. Jeho úlohou je vytvořit komplexní systém kontrol nebo prověřit ten stávající s ohledem na cíle podniku a na stanovené standardy. *„Audit obecně je objektivní ověření stavu, jevu, záměru, skutečnosti se stavem nebo jevem žádoucím, tj. modelem, normou, standardem apod.“* (1) Audit provádí odborník, zvaný auditor. Výsledkem auditu je komplexní názor auditora informačního charakteru, zvaný výrok. *„Audit informačního systému je proces, jehož úlohou je posoudit objekty a vztahy mezi nimi v kontextu IS a tím přispět ke správné organizaci IS“* (1). Audit musí být komplexní, objektivní, nezávislý a formalizovaný. Efektivní audit zvyšuje ekonomickou hodnotu úspěšně auditovaného objektu, poskytuje o něm kvalitní informace, motivuje lidi pro kvalitní práci. Kvalita a význam auditu může být určen právními předpisy. Postup efektivního auditu se řídí metodikou a existující standardy. [1; 2]

3.3. Bezpečnost informací

Bezpečnost informací se v kontextu auditu interpretuje jako rovnovážný stav mezi rizikem a kontrolami, které riziko snižují. Tam kde je zvýšené riziko by měly být úměrně tomu propracovanější kontroly. Absolutní bezpečnosti nelze dosáhnout. Vždy existuje riziko, které zůstává, i když byla provedena všechna myslitelná opatření. Cílem je ale riziko minimalizovat na takovou úroveň, aby náklady na kontroly odpovídaly pravděpodobnosti a ceně ztráty. Bezpečnost informací se skládá z diskrétnosti, nedotknutelnosti a dostupnosti. Diskrétnost znamená, informace že jsou přístupné pouze pověřeným osobám předem určeným způsobem a v předem určeném čase. Nedotknutelnost znamená, že informace mohou být měněny a odstraňovány pouze pověřenými osobami. Dostupnost znamená, že s informacemi mohou pověřené osoby pracovat způsobem a v čase, který vyžadují. Tyto aspekty bezpečnosti informací jsou si obecně rovnocenné. Pro potřeby auditu je ale z důvodu odlišných kontrol pro každý aspekt nutné stanovit mezi nimi prioritu. [3]

3.4. Pojetí IT auditu

IT audit je postup sbírání a vyhodnocování dokumentace za účelem zjištění, zda informační systém zabezpečuje aktiva, udržuje datovou integritu, efektivně plní organizační cíle a efektivně spotřebovává zdroje. Zabezpečení aktiv zahrnuje ochranu počítačových aktiv (hardwaru i softwaru) před poškozením, neoprávněným použitím nebo krádeží. Stav datové integrity znamená, že data jsou přesná, úplná, a konzistentní. Na tyto dvě hlediska se IT auditoři zaměřují především. [3; 4]

S růstem informačních technologií v podnikovém využití vzrostla hrozba ztráty informací. Konvenční systémy a procesy spoléhaly na ruční kontroly k zajištění přesnosti a úplnosti datových záznamů. V takovém prostředí byly chyby odstraněny, hned jak se na ně v průběhu procesu narazilo. Procesy, které se dříve vykonávaly ručně, jsou nyní zcela automatizovány a úlohu kontroly převzaly počítačové aplikace s návazností na IS organizace. Pokud však tyto aplikace nepředvídají všechny druhy chyb, které mohou při manipulaci s daty nastat, mohou být bez povšimnutí zpracovány neúplné nebo chybné transakce. Jestliže z takového datového zdroje čerpá více aplikací, chyba se přenáší dál a je zjištěna až na konci procesu. Náprava takové chyby může vyžadovat rozsáhlou ruční analýzu v závislosti na množství a charakteru postižených záznamů. [3; 4]

Rovněž vzrůstá závislost podniků na možnosti přistupovat k uchovávaným informacím, bez kterých, pokud by byl přístup např. vlivem náhodné události znemožněn, nemohou vykonávat svojí činnost. Data je nutné chránit nejen před procesními chybami a náhodnými událostmi, ale také před cíleným zásahem zvenčí. Okolní subjekty mohou mít vlivem tvrdého konkurenčního boje zájem o přístup ke strategickým datům nebo se dokonce mohou pokusit sabotovat IS podniku. [3]

K omezení uvedených hrozeb slouží bezpečnostní prvky jako omezený přístup k počítačovému vybavení, kontrola uživatelů a přístupů k datům, nástroje pro odhalení vniknutí a firewall, šifrování dat a informací, záloha dat, záložní datové úložiště s jiným geografickým umístěním, mechanismus obnovy dat v případě katastrofy, řízení sítě. Právě tyto prvky jsou předmětem bezpečnostního auditu. [3]

Audit IS se skládá ze tří částí [1]:

1. hodnocení výsledků zpracování na počítačích – zahrnuje vstupy, zpracování a výstupy IS, prověřují se minulé a existující transakce
2. hodnocení rizika a kontrol počítačového zpracování – rozšíření o předběžné hodnocení spolehlivosti a průkaznosti počítačově zpracovávaných transakcí
3. hodnocení a optimalizace procesů IT i navazujících procesů - rozšíření do širší oblasti útvaru IS/IT v rámci organizace

3.5. Druhy auditu

Audity lze třídit z různých hledisek podle toho, jak se na ně nahlíží. Např. z hlediska vykonavatele auditu může být audit interní nebo externí. Interní audit je prováděn zaměstnanci auditované organizace. Externí audit provádí pracovníci externí organizace. Specializované auditorské firmy na základě objednávky poskytnou tým pracovníků, který audit vykoná ve smluveném časovém období a cenu. Mohou být využívány oba druhy auditu najednou, každý se svým specifickým zaměřením. Činnost obou auditů je třeba koordinovat. Z časového hlediska může být audit jednorázový nebo průběžný. Z hlediska věcného zaměření auditu může být audit legálnosti programového vybavení, audit bezpečnosti, technický audit, audit informační strategie a legislativní audit. [1; 5]

Bezpečnostní audit se provádí za účelem zjištění stavu bezpečnosti informací v podniku a zahrnuje audit IS, penetrační testy a analýzu rizik. Technický audit odhaduje účinek investic do infrastrukturních komunikačních systémů a jejich ochrany. Technický audit zahrnuje audit software a hardware, audit infrastruktury. Audit informační strategie je prováděn za účelem stanovení strategie pro IT podniku a zahrnuje koncepce, hodnocení spokojenosti uživatelů, rozbor funkčnosti. Z hlediska na právní systém se jedná o legislativní audit, jehož úlohou je zjistit, zda IS vyhovuje požadavkům daných zákonem. Dále je úlohou forenzního auditu, sběr informace pro soudní procesy při vyšetřování kriminality. Druhým pohledem na audit z hlediska právního systému je tzv. předinvestiční prověrka, která slouží investorovi při rozhodování o koupi podniku. [1; 5]

3.6. IT Governance

IT Governance, neboli správa a řízení informačních technologií, je rámec, který zastřešuje všechny standardy auditu IS. Tento projekt definuje postavení a rozdělení odpovědnosti mezi útvarem IT a exekutivou podniku a vlastníky. Úkolem ITG je sjednocení podnikové, využití příležitostí v odvětví IT, zodpovědné využívání IT zdrojů a řízení rizik spojených s vývojem, pořízením a provozováním IT. ITG se zavádí tzv. akčním plánem. Akční plán zahrnuje seznam aktivit, výstupní měřítka, seznam příkladů, kritické faktory úspěchu a tzv. Performance drivers. [1; 6]

Kvůli častým změnám v podnikatelské sféře a rychlému vývoji IT, není možné dosáhnout naprosté shody podnikové a IT strategie. Proces harmonizace je nekonečný cyklus, který spočívá ve snaze přiblížení a vyrovnávání podnikové strategie a podnikových procesů k IT strategii a IT procesům. IT musí podniku přispívat generováním přidaných hodnot včas, v rámci rozpočtu a s přínosy, které byly slíbeny. Jedná se především o podnikatelské výhody plynoucí z využívání nějakého IS, urychlení procesů podniku, čímž se např. čas potřebný k vyřízení objednávky se zkrátí, produktivita zaměstnanců se zvýší apod. Pro formování strategie je třeba měřit výkonnost IT. V této oblasti se využívá metoda Balanced Scorecards, která umožňuje hodnotit nehmotná aktiva jako je orientace na uživatele, efektivnost procesů, schopnost učit se. V IT je třeba identifikovat a omezovat rizika. Prostřednictvím řízení rizika se zavádí rámec, který stanovuje kritéria pro měření, akceptaci, řízení a ohlašování rizik. Tímto se dosáhne rychlé a včasné reakce na rizika. [1; 6; 7]

3.7. Bezpečnost IT

Protože bezpečnost nelze zajistit stoprocentně a zavedená opatření v čase ztrácejí účinnost, bezpečnost informačního systému je především cestou, nikoli cílem. Model bezpečnosti v podniku se skládá ze čtyř kroků, které na sebe postupně navazují a tvoří cyklus. Čtyřmi prvky tohoto tzv. kola bezpečnosti je plánování, prevence, detekce a reakce. [8]

3.7.1. Plánování

Bezpečnost je vyzývavý koncept, obzvláště když přijde na technologii. Když je zvažováno jak poskytnout bezpečnost, je třeba začít klást si následující otázky: Jaký druh majetku je třeba zabezpečit? Jaké jsou nároky na bezpečnostní opatření chráněného majetku? Jaká jsou rizika specifická pro takové bezpečnostní nároky? Jak lze nastavit priority a efektivně přistupovat k těmto rizikům? Tyto otázky popisují přístup založený na riziku bezpečnosti. Známé metody bezpečnosti rizika zahrnují operační kritické riziko, aktivum a metodu vyhodnocení zranitelnosti. [8]

Nejdříve se určí aktivum, čímž může být server z hardwarového hlediska, informace v databázi, nebo třeba chráněné výrobní postupy. V praxi někdy klient nedokáže zodpovědět otázku, co je pro něj nejcennější aktivum. Proto je vhodné nejprve tuto otázku zúžit na aktiva v podobě digitálních informací, která jsou pro podnik cenná. Fyzické prostředky, na kterých se digitální aktiva vyskytují, jsou z hlediska bezpečnosti rovněž důležitá, ale snadnější je zvážit tyto vztahy později v procesu hodnocení rizika. Rovněž je doporučeno odložit zvažování méně hmatatelných aktiv jako je např. reputace. [8]

Kategorie zvažovaných citlivých aktiv v podobě digitálních informací zahrnují pověření (jako hesla a osobní šifrovací klíče), osobně rozpoznatelnou informaci, finanční nástroje nebo informace (jako např. data kreditních karet), chráněné informace (zahrnující nehlášené finanční výsledky nebo podnikové metodiky) a dostupnost k produkčním zdrojům (zahrnuje přístup k funkčnímu systému, k elektřině atp.) [8]

Jakmile bylo určeno, jaká aktiva bude snaha zabezpečit, dalším krokem je určit požadavky na jejich zabezpečení. Požadavky je doporučeno roztřídit do co nejobecnějších kategorií. Většina definic bezpečnosti informačního systému se soustřeďuje na důvěrnost, integritu a dostupnost důležitých aktiv. K těmto aspektům by mohl být přidán ještě jeden, odpovědnost, k doplnění, že systém musí také věrně zaznamenávat aktivity, aby mohly být později zkoumány a auditovány. [8]

Jakmile jsou stanoveny aktiva a jejich bezpečnostní požadavky, následuje zvážení rizik, kterému každé aktivum čelí. Tento proces je obvykle nazýván hodnocení rizika. Existuje několik přístupů k hodnocení rizika. Nejméně formálním je sestavení logického systémového diagramu, dále jeho dekompozice na dílčí části, přičemž je věnována pozornost hranicím a vzájemným vztahům mezi jednotlivými částmi stejně jako u klíčových aktiv. Nakonec je vhodné v týmu prodiskutovat možné hrozby. [8]

3.7.2. Ohodnocování rizika

Po sestavení seznamu hrozeb je každé hrozbě přiřazena priorita tak, aby k nim bylo efektivně přistupováno. Přidělení příliš velkého množství zdrojů na snížení hrozeb s nízkým rizikem může být pro organizaci stejně škodlivé jako podhodnocení přidělovaných zdrojů na snížení hrozeb s vysokým rizikem. [8]

Řízení rizik

Nejprve je nutné upřesnit výklad některých termínů, zejména rizika a nebezpečí. Aktivem se v kontextu řízení rizik rozumí vše, co má pro organizaci hodnotu. Nebezpečím se rozumí bezprostřední či akutní stav. Pojem riziko se používá při vyjádření pravděpodobnosti výskytu hrozby. Hrozba je jakákoliv náhodná či úmyslná nežádoucí událost s negativním vlivem. Během analýzy se provádí výpočet nebo alespoň odhad frekvence výskytu hrozby. K tomu mohou být využity katalogy typických nebo frekventovaných hrozeb daných objektů analýzy. Základní dělení hrozeb je na lidské a přírodní. Hrozby se hodnotí na stanovené škále z hlediska síly jejich dopadu. Dopadem se rozumí důsledek negativního vlivu. Za účelem ochrany před hrozbou byla vyvinuta různá ochranná opatření. Ochranná opatření mohou být fyzická nebo logická. [1; 9]

Proces řízení rizik se skládá ze stanovení a ošetření rizika. Stanovení rizika zahrnuje analýzu a hodnocení rizik. Cílem analýzy rizik je identifikovat rizika, aktiva, hrozby, slabiny a pravděpodobnosti dopadu. Odhadování rizik se provádí určením efektivnosti kontrol a analýzou rizik, které se k nim vážou. Náplní hodnocení rizik je porovnání odhadnutého rizika s předem stanovenými kriterii, za účelem seřadit rizika podle priorit. Ošetření rizika spočívá ve vytvoření plánu a stanovení, která rizika budou odstraněna, která budou snížena a která přijata. Přijatá rizika se nazývají zbytková. [1]

Na rizika je možno nahlížet z různých úhlů pohledu. Z hlediska podnikání je rizikem možnost, že hrozba negativně ovlivní schopnost organizace plnit podnikatelské cíle. Jsou to strategická rizika prostředí, provozní rizika prostředí, informační rizika. Z hlediska ekonomického se rizika dělí na přijatelná a nepřijatelná. Z hlediska počítačového zpracování se rozlišují rizika aplikační (přístup do aplikací, vstup dat, odmítnutí a zpracování transakcí) a rizika všeobecná (organizace a provoz IT, vývoj a řízení změn aplikací, přístup k IS). [1; 10]

Z hlediska auditu se rozlišuje přirozené riziko, též zvané inherentní. Jedná se o tendenci analyzovaného objektu k chybě za podmínky neexistence vhodné kontroly. Bezpečnostní riziko podnikové databáze je velmi vysoké, protože je možné z ní získat nebo smazat důležité informace. Naopak trvale odpojený počítač od počítačové sítě má malé inherentní riziko, protože se nepoužívá pro kritické procesy podniku. Při určování inherentního rizika se používají jak průřezové, tak podrobné kontroly. Tzv. zbytkové riziko, nebo též reziduální, představuje akceptovatelné riziko v podmínkách existence vhodných kontrol. [1; 10]

Dalším rizikem z hlediska auditu je riziko kontrol. Jedná se o pravděpodobnost, že dojde k chybě, která nebude kontrolním systémem včas odhalena a napravena. Riziko kontroly vstupních dat člověkem je vysoké, protože člověk snadno něco může přehlédnout. Naopak automatizovaná kontrola má nízké riziko kontrol. Auditor může konstatovat, vysoké riziko kontrol v případě, že kontroly neexistují, pokud nejsou vyhodnoceny jako efektivní nebo není prověřeno jejich dodržování v praxi. [1; 10]

Posledním rizikem z hlediska auditu je riziko detekce, nebo též auditu. Jedná se o riziko, že auditor neodhalí chybu, která je přítomna. Pravděpodobnost odhalení chyb bezpečnosti aplikačního systému je malá z důvodu nedostupnosti logů z období provádění auditu. Naopak pravděpodobnost odhalení chyby u plánu na obnovu dat po nedávném výpadku pevného disku je vysoká, protože lze snadno ověřit jeho existenci. [1; 10]

Při práci by měl auditor dokumentovat, jakou metodologii pro rizikovou analýzu použil. Dokumentace by měla zahrnovat metodologii, identifikaci významných nebezpečí ve vazbě na rizika, rizika a nebezpečí, která auditor bude řešit, podpůrné údaje zdůvodňující tvrzení auditora, použité nástroje. [1]

Druhy analýzy rizik

K analýze rizik lze přistupovat několika způsoby. Základní přístup spočívá v rychlém zavedení bezpečnostních opatření. V tomto přístupu se provádí povrchní analýza, opatření jsou přejata z nějakého standardu. V praxi dojde k porovnání aktuálních bezpečnostních opatření se zvoleným standardem a zavedou se ta, která dosud nebyla využívána. Slabinou základního přístupu je možnost nasazení neadekvátního opatření. Neformální přístup vychází ze zkušeností osob, které jsou se zkoumaným prostředím odborně seznámeny. Tento přístup je značně subjektivní a doporučuje se ho využít pouze jako krok předcházející podrobné analýze rizik Podrobná analýza rizik je dalším přístupem. Jedná se o nejpřesnější a zároveň nejnáročnější metodu. Nejdříve se identifikují a ohodnotí aktiva, u kterých se pak posoudí jejich hrozby a zranitelnost. Z toho se vyvodí rizika a z nich bezpečnostní opatření. Je doporučeno volit kombinovaný přístup v závislosti na důležitosti předmětů kontroly. [1; 9]

K ohodnocení rizika může být použito několik postupů. Prvním a exaktnějším způsobem je kvantitativní metoda. Klasický a jednoduchý postup k ohodnocování rizika vyjadřuje následující vzorec: riziko = dopad x pravděpodobnost. V tomto postupu je dopad obvykle vyjadřován v peněžní hodnotě a pravděpodobnost v procentuální hodnotě. Rovnice může být dále specifikována rozdělením dopadu na aktiva x hrozby a pravděpodobnosti na zranitelnost x zmírnění. Cílem je vyjádření korelace mezi hodnotou chráněných aktiv, hodnotou hrozby a hodnotou ochrany, neboli hledá se výše míry návratnosti investice vložené v úmyslu redukovat rizika. [1; 8]

$$ALE = SLE \times ARO$$

ALE – Annualized Loss Expectancy – očekávané ztráty
SLE – Single Loss Exposure – ztráta při jednom výskytu hrozby
ARO – Annualized Rate of Occurance – vyjádření pravděpodobnosti výskytu hrozby za rok [1]

Tento postup je poměrně jednoduchý a umožňuje lepší začlenění podnikových a bezpečnostních zájmů. Ohodnocení dopadu na podnik může být například přiděleno vedoucímu ve finančním oddělení podniku a odhad pravděpodobnosti vedoucímu bezpečnosti podniku. Takové rozdělení práce a odpovědnosti přináší dobré výsledky, pokud se jedná o řízení rizik podniku obecně. [8]

Další možností odhadování rizika je přístup DREAD. Tato kvalitativní metoda vyjadřuje riziko v nespojité škále hodnot, které se přiřazuje prostřednictvím subjektivního vyjádření analytiků. Výsledné riziko je průměrem součtu jednotlivých ukazatelů rizika. Každý ukazatel je ohodnocen číselně v intervalu <0; 10>, přičemž čím vyšší je význam, tím vyšší číslo je přiřazeno. Jednotlivé ukazatele jsou: velikost způsobené škody, opakovatelnost zneužití slabiny, složitost zneužití slabiny, množství zasažených uživatelů, složitost objevení slabiny. [1; 8]

Risk =(DAMAGE+REPRODUCIBILITY+EXPLOITABILITY+AFFECTED_USERS+DISCOVERABILITY)/5

[11]

Odhad rizika je poměrně subjektivní záležitost, proto je možné kombinovat zavedené metodiky nebo i vyvíjet svoje vlastní. Hlavní je, aby pro odhad všech rizik byla použita stejná metodika, protože rizika budou v dalším kroku mezi sebou srovnávána. Důležité je ovšem také, aby byla zvolená metodika pro podnik vyhovující. Také je užitečné před ohodnocením rizika stanovit hranice, pod kterou musí být riziko sníženo. Tím se omezí zpětné ovlivňování hranice rizika podle výsledků, které byly získány. Na výši této hranice by měla panovat shoda. [8; 9]

3.7.3. Cyklus vytváření bezpečnosti

Politika

Rizika, která se v procesu ohodnocování dokumentují, se následně snižují, odstraňují nebo se přenášejí např. prostřednictvím pojištění. Smyslem vývoje politiky ve fázi plánování je stanovit plán na snížení rizika. Bez politiky, která definuje co je a co není narušení bezpečnosti, není možné bezpečnost zavádět. Postup definuje, jak jsou rizika snižována v souvislém přístupu. Dobré bezpečnostní postupy vycházejí z dobré, obecně uznávané předlohy, jako je rámec ISO 17799. [8]

Základním krokem při vytváření politiky je porozumění podniku. Bezpečnostní odborník nejprve musí porozumět podniku, který přišel pomoci zabezpečit. Porozumění podnikového provozu vytváří slovník, který umožňuje plodnou konverzaci a vede k tomu, aby byl odborník vnímán jako přínos, nikoli jako překážka. Vždy je vhodnější získat zdroje pro měření rizika a implementaci měřících kontrol od vedoucích v podniku. [8]

Navazujícím krokem je kulturní přijetí, jehož cílem je přesvědčit vedení, aby si důkladně pročetlo podporu a politiku. Vedení nakonec politiku prosazuje, a pokud manažeři nevěří, že je správná, je velmi obtížné přimět kohokoli v podniku, aby se jí řídil. Vytvořením soustavy governance, která zahrnuje klíčové partnery podniku s definovanými odpovědnostmi, se politika snadněji prosazuje a vyvíjí v dlouhodobém období. Současně je třeba si uvědomit, že takové přijetí vedením je účinné pouze, pokud zaměstnanci poslouchají své nadřízené, což nemusí být vždy samozřejmostí. V každém případě je ale potřeba nějaká úroveň prolnutí kultury bez ohledu na to, jak tvrdě politiku prosazuje, jinak by politika nebyla přijata v rozsahu potřebném pro uplatnění zásadních změn v bezpečnosti. Vhodné je také zasvěcovat do bezpečnostního programu všechny úrovně podniku, aby bylo jisté, že je šířeji přijat a že bude vnímán jako rozumný a praktický prostředek ke zlepšení pozice podnikové bezpečnosti. To významně zvětší potenciál ke kulturnímu přijetí více, než bolt-on procesy, které každý zesměšňuje. [8]

Politika se nejprve navrhuje jako soupis průvodních zásad a záměrů na vysoké úrovni abstrakce. Poté se vytvoří podrobnější standardy implementace a operační procedury, které podpoří nařízení politiky. Tento vícevrstvý přístup vytváří modularitu, která usnadňuje údržbu politiky v dlouhém období, tím že poskytuje přizpůsobivost ke změnám implementačních detailů bez vyžadování přehodnocení celé politiky a změny cyklu. [8]

Říká se, že jedinou konstantou je změna a pro bezpečnostní politiku to platí také. Je třeba očekávat, že podnik bude vyžadovat výjimky v politice a bude ji chtít v pravidelných intervalech měnit. Je potřeba vytvořit proces, který by toho docílil. Doporučené jsou nejméně výroční zprávy a také zvláštní proces pro výjimky a nouzové změny. Tyto procesy by měly být tak těžkopádné, nakolik je cílem odradit od častých žádostí o výjimky a změny politiky. [8]

Prevence

Nezbytnost některých preventivních kontrol vyvstane během procesu ohodnocování a vývoje politiky. Na protiopatření se většinou pohlíží z technického pohledu, ale ke snížení rizika můžou být zavedena o něco širší opatření více lidského charakteru. Školení a nácvik jsou nejzřejmějším způsobem, jak zvýšit účinek bezpečnostní snahy napříč podnikem. Zprávy můžou pomoci této snaze naplánováním pravidelného sdělování aktualit řadovým zaměstnancům i vedoucím a stejně tak udržet informační tok mezi bezpečnostním týmem a zbytkem podniku. [8]

Bezpečnostní provoz zahrnuje obecnou bezpečnostní údržbu jako správa bezpečnostních záplat, ochrana proti malware, fyzický i logický přístup, kontrola příchozí i odchozí síťové komunikace, bezpečnostní sledování a odezva, správa bezpečnostních účtů a skupin. Některé části bezpečnosti podniku si potřebují přisvojit proaktivní a výhledový přístup. Práce bezpečnostního architekta je obzvláště důležitá pro vývoj aplikací, kde se vývojáři musejí řídit pevnými normami a pravidly, aby se vyhnuli zanesení mnoha chyb, které se v procesu vývoje softwaru nevyhnutelně objevují. Tato funkce může navíc vykonávat pravidelná vyhodnocení fyzické sítě a platformy bezpečnostní architektury tím, že zavedená pravidla srovnává s vyvíjejícími se standardy a technologiemi. Tím je zajištěno, že podnik udržuje krok s nejnovějším pokrokem v bezpečnosti. [8]

Detekce

Dokumentace politiky je výborná věc, ale ani dobrá politika není příliš užitečná, pokud nelze zjistit, jestli se jí někdo řídí. Oblast detekce se soustředí na nalézání a odhalování bezpečnostních slabin a je důležitou součástí odhalování narušení bezpečnostní politiky. Ostatní procesy, které spadají do oblasti detekce jsou: automatizované skenování slabin, správa bezpečnostních událostí a informací, systémy pro detekci průniku, systémy pro detekci anomálií, interní audity zahrnující penetrační testy. [8]

Reakce

Posledním krokem bezpečnostního cyklu je reakce. Za předpokladu, že jsou ve fázi detekce odhaleny bezpečnostní slabiny i bezpečnostní průniky, následujícím krokem je poměrně rychle analyzovat další postup. Některé klíčové elementy části reakce zahrnují odpověď na událost, náprava, auditorské rozhodnutí, obnovení. Element odpověď na událost popisuje mnoho kritických postupů, které by pro minimalizaci škod měly následovat okamžitě po výskytu bezpečnostní události. Tyto procedury by tedy měly být připraveny předem. [8]

3.7.4. Základní bezpečnostní zásady

Každý by měl být zodpovědný za bezpečnost – ani mnoho pozorných bezpečnostních odborníků nemůže v nutném měřítku pokrýt všechny aktivity, které nastávají v každodenním provozu. Dobré je rozdělit odpovědnost za bezpečnost napříč podnikem tak, aby šla řídit. Jak se někdy říká: *„Lidé jsou ultimátním systémem detekce průniku.“* (8)

Blokovat nebo zakázat vše, co není výslovně povoleno – kromě pár nejasných výjimek nejsou známy žádné metody vzdáleného útoku na systém, na kterém neběží žádné služby. Z toho vyplývá, že pokud je zcela blokovaný přístup ke službám, nebo jsou služby úplně deaktivovány, nemůže dojít k jejich napadení. To je však malá útěcha pro ty služby, které jsou povoleny, jako např. internetové informační služby, které jsou nezbytné k provozu webové aplikace. Pokud je třeba povolit přístup ke službě, je třeba se ujistit, že byla zabezpečena podle přijatých postupů. Protože samotné aplikace bývají téměř vždy jedinečné, musejí být zabezpečené designovými a implementačními přijatými postupy. [8; 12]

Vždy nastavit heslo, vymyslet ho rozumně složité a často ho měnit – hesla jsou kletbou světa bezpečnosti. Jsou prvořadým způsobem autentifikace snad u každého produktu, který existuje. Slabá hesla jsou hlavní příčinou, kvůli které sítě nevyhoví v penetračních testech. Hlavní zásadou je tedy nikdy nenechat heslo prázdné a ujistit se, že není snadno uhodnutelné. Pokud je to vhodné, je dobré použít kombinovanou přihlašovací metodu zahrnující např. biometrické údaje nebo generátor klíče. [8; 12]

Doporučeníhodné je držet krok s vydáváním opravných balíků. Když je v tak rozšířeném produktu, jako jsou Windows, nalezena chyba, Microsoft ve snaze získat dobrou pověst a povědomí o svých produktech, chybu zveřejní v řádu hodin. To znamená, že k instalaci záplaty, než někdo zkusí bezpečnostní dírou proniknout, je od oznámení stále menší prostor. [8; 12]

Veškerý přístup autorizovat s co nejmenším možným oprávněním. Přestože tento koncept je obvykle tvrdě dodržován, ale také je nejvíce zneužitelný. Autorizace, tedy ověření přihlašovacích údajů na straně serveru nebo operačního systému, je posledním významným mechanismem, který chrání citlivé zdroje od přístupu nepovolaných uživatelů. Uhádnutí slabého hesla je dost špatné, ale situace se zhorší, když se zjistí, že podřadný uživatelský účet může nastavit sdílení citlivých podnikových finančních dat. Vyžaduje to hodně práce inventarizovat všechny zdroje IT prostředí a stanovit vhodné oprávnění přístupu. Pokud se to ale neudělá, systém bude jen tak silný, jako jeho nejslabší článek. [8; 12]

Žádný systém není ostrov, obzvláště ten využívající Windows. Omezená důvěra je v tomto hledisku klíčová. Jedním z nejefektivnějších útoků proti sítím ze stanic s těmito operačními systémy je zneužití nedůležitého člena domény se slabým administrátorským heslem. Poté se z tohoto počítače vyextrahují přihlašovací údaje pro oprávněného doménového uživatele, který útočníkovi umožní získat kontrolu nad celou doménovou infrastrukturu a možná i nad doménami, které jí důvěřují. Je důležité vědět, že každá důvěra, ať už se jedná o doménu, nebo prostě heslo uložené na vzdáleném počítači v dávkovém souboru, rozmělňuje hranici bezpečnosti a zvyšuje rizika. [8]

Vyplácí se být obzvláště paranoidní, pokud jde o externí interface. Celkové množství potenciálních slabin v síti se může zdát obrovské, ale je třeba se zaměřit na ty, které v současné situaci představují největší riziko. Jedná se o ty, které jsou často spojeny se systémy, jako např. web server, které čelí veřejným sítím. [8]

Jednoduchý systém jde snáze zabezpečit než složitý systém. Jednoduchostí je myšleno snížená pravděpodobnost výskytu chyb nebo trhlin. Důsledkem tohoto principu je koncept výhradní funkce nebo modularita. Systém nebo jeho komponenty by měly být jednoúčelové, aby se zamezilo případným konfliktům nebo redundancím, které by mohly vést k bezpečnostním odkrytím. [8]

Technologie systém neochrání před společenskými útoky. Některé nejničivější útoky nezahrnují žádnou technologii. Takzvané sociální inženýrství využívá klamání lidí lidmi za účelem získat neautorizovaný přístup k datům. Mezi takové útoky patří např. phishing a jeho účinkům lze předejít dobrou komunikací a cvičeními. Důležité je tedy připravit zaměstnance na možné snahy o narušení bezpečnosti informačního systému zneužitím jejich důvěřivosti nebo nevědomosti. [8]

Další zásadou je, že neexistuje ideální řešení, klíčem je řízení rizik. Smysl pro bezpečnost by neměl narušit podnikové cíle a naopak. Poslední zásadou je znát své počítačové prostředí a aplikace lépe než nepřítel. [8]

3.8. Obecný postup provádění auditu

Audit má charakter projektu a proto prochází svým životním cyklem. Tento životní cyklus je složen z etap, jejíž nástroje, činnosti, vstupy a výstupy jsou popsány v rámci jednotlivých metodik. Etapy dané metodikami mohou být vynechávány nebo upravovány podle toho, co je objektem auditu. [1]

3.8.1. Etapa 0

Tato etapa se zabývá uzavřením smlouvy na audit v případě, že se jedná o audit externí. Úlohou této předběžné etapy je vymezit základní parametry auditu, jako je předmět, cíle, rozsah, organizace, časový úsek, odměna, výstupy, standardy, podle kterých se bude objekt auditu posuzovat. Bez znalosti auditovaného subjektu může být problematické správně tyto parametry stanovit. Stejně tak může být překážkou neschopnost zadavatele přesně specifikovat své požadavky na audit. Další obtíží může být odhad míry podrobnosti auditu, která je potřebná požadované ujištění o kvalitě zkoumané oblasti IS/IT. Za takové situace se doporučuje uzavřít dohodu na provedení auditu ve dvou krocích. V prvním kroku je proveden obecný audit se zaměřením na obecné kontroly. V druhém kroku je pak proveden důkladný audit se zaměřením na nejrizikovější oblasti. [1]

Pokud se jedná o interní audit, v této etapě místo toho dochází k vymezením statutu interního auditu a jeho postavení v rámci organizace. Také by měla být vymezena odpovědnost za audit IS, popis požadavků na jeho obsazení, popis odpovědností a práv. [1]

3.8.2. Etapa 1

Etapa předběžného plánování slouží k tomu, aby auditor mohl naplánovat svoji činnost. K tomu je potřeba porozumět podnikovým procesům, architektuře IS organizace, používaným IT a systému vnitřních kontrol. Míra porozumění se odvíjí od cíle auditu. Potvrzení porozumění je podmínkou pro pokračování auditu. Pro získání jistoty o správnosti porozumění by auditor měl prezentovat své poznatky odpovědným pracovníkům. [1]

Vnitřní kontrolní systém nesmí být opomenut u žádného auditu. Identifikace a hodnocení kontrol je základem šetření. Pokud je hodnocení kontrol zahrnuto v zadání auditu, je třeba navíc provést testování účinnosti a dopadů těchto kontrol v praxi. Potřebné informace mohou být shromážděny prostřednictvím studia dokumentace, pozorováním v pracovním prostředí nebo dotazováním zaměstnanců. [1]

Pokud organizace nedisponuje aktuální požadovanou dokumentací, jedním z cílů této etapy by mělo být vytvoření chybějící dokumentace ve spolupráci s odpovědnými pracovníky podniku. Jestliže je auditorovi odepřen přístup k relevantním informacím, může od auditu odstoupit. Pokud by se vytvoření dodatečné dokumentace mělo projevit na časovém harmonogramu auditu, je třeba to zohlednit formou dodatku ke smlouvě. [1]

Dalším výstupem této etapy je dokumentace auditu, která zahrnuje popis práce a výstupů auditora, evidenci všech informací, které byly podkladem pro nálezy a závěry auditora. Dokumentace by měla být jasná, kompletní a srozumitelná. S ohledem na citlivost a povahu informací musí organizace vytvořit patřičná pravidla pro nakládání s touto dokumentací. [1]

V této etapě by měl vzniknout také program auditu, který určuje základní body auditu, ve kterých se auditor a zadavatel neshodnou v tom, zda je nutné některou etapu opakovat, nebo je možné postupovat dál. Změny plánu se promítají i do programu tak, aby byly oba dokumenty konzistentní. [1]

3.8.3. Etapa 2

V této etapě auditor provede analýzu získaných a ověřených informací z etapy předchozí a rozhodne, zda v auditu pokračovat. Pokud audit pokračuje, na základě odsouhlasených výstupů se vytvoří plán auditu. Oblasti, které audit odhalí jako závažné, budou předmětem podrobnější analýzy efektivnosti a adekvátnosti jejich kontrol. Pro hodnocení efektivnosti není pro auditory stanovená žádná konkrétní norma a je tedy spoléháno na úsudek auditora. Pokud kontroly nejsou efektivní, auditor později navrhne nové. Pokud kontroly efektivní jsou, auditor upřesní zdroje, které budou vyžadovány pro pozdější testování jejich realizace v praxi. Výstupem této etapy je tedy upřesněný plán auditu, který zahrnuje upřesnění cílů auditu, výsledky hodnocení kontrol a zdůvodnění dalšího postupu, časový plán testů, určení potřebných zdrojů pro audit a jejich rozvrh. [1]

3.8.4. Etapa 3

Samotná realizace auditu spočívá v testování kontrol, které byly identifikovány a analyzovány jako efektivní. Podstatou této etapy je testování souladu popisu, záměru a praktické realizace kontrol. Pokud testování prokáže nesoulad, zjišťuje se velikost způsobované škody prostřednictvím tzv. substantivního testu, jehož předmětem již není kontrola, ale jednotlivé transakce. Jestliže není vhodné nasazení substantivního testu, používá se metody výběru vzorků. Výstupem této etapy jsou zdokumentované výsledky testů a předběžná auditorská zpráva. [1]

3.8.5. Etapa 4

Předposlední etapou je závěr a vydání auditorské zprávy. Předběžná auditorská zpráva by měla být konzultována s příslušnými odpovědnými pracovníky, popř. se zadavatelem auditu. Předběžné projednání auditorské zprávy má význam pro auditora jako kontrola, že jeho nálezy a závěry jsou relevantní a nebyla přehlédnuta významná rizika. Zpráva má význam také pro organizace, které byly předmětem auditu, aby zřídily rychlou nápravu méně podstatných pochybení, čímž můžou redukovat konečnou zprávu na skutečně závažné problémy. Poté je možno vytvořit výstup této etapy, tedy konečnou verzi auditorské zprávy. [1]

3.8.6. Etapa 5

Poslední etapa se zabývá sledováním uskutečňování závěrů auditorské zprávy. U interního auditu se tato etapa považuje za přirozenou odpovědnost auditora. Ten by měl vytvořit plán sledování skutečného plnění auditu a podávat o něm průběžná hlášení a doporučení. Tato etapa není zaváděna v případě externího nebo jednorázového auditu, kde auditor nemá možnost dohlížet na uskutečňování doporučení. [1]

3.9. Nástroje auditu

3.9.1. Kontroly

Kontroly slouží pro eliminaci nebo snížení rizik. Kontroly se nejčastěji dělí na aplikační a obecné. Aplikační se týkají aplikačních systémů, zatímco obecné se vztahují k počítačovému prostředí, ve kterém jsou aplikace provozovány a které je společné všem aplikacím, prakticky se jedná o útvar IT. [1; 14]

Obvykle jsou auditorem prováděny nejprve obecné kontroly, protože jestliže existuje slabina v obecných kontrolách, dá se předpokládat, že existuje i v kontrolách aplikačních. Naopak pokud jsou obecné kontroly pořádku, není nezbytné provádět kontroly aplikační. V závislosti na organizaci podniku se vyskytuje mnoho úrovní obecných kontrol. Obecné kontroly zajišťují vývoj, zavádění a vykonání IT postupů předem naplánovaným způsobem. Slouží vedení podniku ke stanovení, jakým způsobem se v dlouhodobém hledisku bude využívat nasazení IT v podniku. Management vývoje systémů je zodpovědný za návrh, zavádění a údržbu jednotlivých aplikací, management programování je zodpovědný za programování nových a provoz starých systémů. Administrátoři databáze jsou zodpovědní za kontrolu a užívání podnikové databáze nebo knihovny aplikací. Operační management kontroluje každodenní fungování IS, dále je zodpovědný za přípravu dat, datový tok při instalaci, udržbu hardwaru a někdy údržbu programů a fyzickou bezpečnost dat. [3; 14; 15]

Aplikační kontroly zajišťují, že každá aplikace chrání aktiva, udržuje integritu a efektivně zpracovává data. Tyto kontroly se provádějí v různých stupních toku dat v IS a zajišťují, že všechna přenášená data jsou autorizovaná, kompletní a správná. Jedná se o kontroly získávání dat na úrovni zápisu databáze. Dále kontroly přípravy na úrovni importu dat, kde se navíc kontroluje, že jsou všechna přenášená data v kompatibilním formátu. Kontroly přístupu k systému zajišťují, že výpočetnímu vybavení mají přístup pouze povolané osoby. Vstupní kontroly dat na úrovni ručního zadávání také zajišťují možnost odhalit chyby a znovu vložit opravený záznam. Kontroly přenosu zajišťují, data přenesená počítačovou sítí a nakonec výstupní kontroly. Auditová kontrola cest sleduje, zda jsou všechna data vysledovatelná ze svého cíle k jejich zdroji a naopak. Dále pak sleduje, jestli je možné obnovit ztracená nebo poškozená data v průběhu procesu. [3; 14]

3.9.2. Testování

Předmětem substantivního testování jsou transakce. Smyslem tohoto testování je vytvořit detailní rozbor a testovat vzorky jednotlivých transakcí v různých oblastech. Na základě vytvořeného rozboru se stanoví správnost. Druhým přístupem je testování kontrol, předmětem tohoto testování jsou kontroly a jejich praktické dodržování. Při testování kontrol se prověří způsob zpracování transakcí a jejich kontrol. Testovány by měly být nejdříve kontroly obecné a poté teprve aplikační. Síla obecných kontrol ovlivňuj důvěru vůči hodnocení kontrol aplikačních. [1]

Test lze realizovat třemi způsoby. První způsob je tzv. testování kolem počítače. Testování probíhá na klientském systému s modelovými daty, mezi kterými jsou ukryty nepřípustné záznamy, které pokud kontrolou projdou, chybu odhalí. Auditor ručně zpracovává výsledky a na konec je porovná s výsledkem automatizované kontroly. Druhý způsob, tzv. testování s počítačem, je ověření klientských dat na nepřípustné záznamy. Tento způsob usnadňuje speciální auditorský software CAAT (Computer Assisted Audit Techniques). Poslední způsob je užití počítače nezávislého na klientském systému a datech. Takový způsob ovšem probíhá výhradně přes specializovaný software. [1; 3]

3.9.3. Penetrační test

Tento typ testu je založen na principu simulace bezpečnostního útoku, jehož cílem je získat přístup k vnitropodnikovým informacím, vyřadit veřejné služby a servery podniku. Útoky lze rozlišovat podle lokality jejich původu vzhledem k počítačové síti podniku, tedy na vnější a vnitřní. Za vněší útok se považují i např. WWW stránky se škodlivým obsahem. Nebezpečné stránky mohou být i původně bezpečné, ale kompromitované útočníkem, který zaměnil jejich obsah nebo přesměroval přístup jinam. Častější je ale využívání neznalosti uživatelů, kteří sice nevědomě, ale dobrovolně poskytnou informace k provedení závažnějšího útoku. Vnitřní útok může provést např. nespokojený zaměstnanec nebo i cizí osoba, pokud selžou fyzická bezpečnostní opatření. K takovým útokům ale dochází jen zřídka. [5]

První fází penetračního testu je shromažďování informací, jejímž cílem je vytvořit profil odolnosti testovaného subjektu vůči průnikovým metodám. Dojde k určení síťových prvků internetového připojení (ping scan), služeb poskytovaných na těchto komponentách (port scan), aktivních uživatelských účtů (finger, smtp). V neposlední řadě dojde k prohledání volně přístupných složek (ftp, http). [5]

V druhé fázi je realizován samotný průnik. Testují se chyby v operačním systému, firewallu, používaných aplikacích, dále chyby konfigurace firewallu, pokus o uhádnutí hesla, spoofing (falšování zdrojové adresy), zfalšování informací na DNS serveru, využití chyb konfigurace WWW serveru, zneužití skriptů atd. Předposlední fází je eskalace, kdy v případě získání kontroly dojde k jejímu využití a sledují se reakce administrátorů. Poslední fází je analýza, ve které dojde k vypozorování nedostatků a návrhu testování dalších slabin. Na závěr je vypracována zpráva obsahující výsledek testu a doporučení technického i organizačního charakteru. [5]

3.9.4. Architektura systému

Architektura systému představuje obecný plán informačního systému a zachycuje jeho jednotlivé komponenty a vazby. Celková architektura popisuje jednotlivé bloky, každý blok je popsán několika dimenzemi. Dále popisuje vazby mezi bloky i s okolím jejím obsahem. Architektura systému je součástí informační strategie podniku a stále se vyvíjející model. [1]

Součásti informačního systému tvoří veškerý software, hardware, data, lidé, procedury a sítě, které jsou nezbytné pro nakládání s informací jako se zdrojem. Uvedené součásti umožňují, aby systém přijal, zpracoval a uchoval informaci. Každá ze součástí má své silné a slabé stránky, své vlastní rysy a každá součást má své vlastní nároky na bezpečnost. [16]

Softwarová část informačního systému zahrnuje aplikace, operační systém a nejrůznější ovládací nástroje. Software je jednou z nejobtížněji zabezpečitelných částí informačního systému. Softwarové produkty jsou vytvářeny s omezeními daných projektovým řízením, kterými jsou omezený čas, náklady, a pracovní síla. Bezpečnost informací je často do produktu implementována až dodatečně, místo aby byla do softwaru začleněna jako nedílná součást produktu už od počátku jeho vývoje. Zneužitelnost chyb a nedostatků v programovém kódu softwaru vytváří příležitost pro případného útočníka, který se snaží dostat k informaci, se kterou software nakládá, nebo jí poškodit. Ze softwarových programů stává snadný cíl záměrných i nezáměrných útoků. [16]

Hardware zahrnuje fyzickou technologii, která zastřešuje a provozuje software, uchovává a přenáší data a poskytuje rozhraní pro vložení a odstranění informací z e systému. Podnikové směrnice pro fyzickou bezpečnost nakládají s hardware jako s hmotným majetkem a snaží se ho ochránit před poškozením nebo krádeží. Toho je docíleno běžnými prostředky fyzické bezpečnosti, jako zámky, omezený přístup osob k manipulaci s hardwarovými komponentami informačního systému. Zabezpečením nejen počítače jako takového, ale i jeho prostředí je důležité, protože narušení fyzické bezpečnosti může mít za následek ztrátu informací. [16]

Uchovávaná, zpracovávaná a přenášená data musejí být v počítačovém systému chráněna. Data jsou mnohdy nejcennějším majetkem, který organizace má a mnohdy jsou cílem záměrných útoků. Databázové systémy, pokud jsou správně realizovány, umožňují zabezpečení dat v nich uložených. Ne všechny databázové systémy ale poskytují dostatečnou úroveň zabezpečení a některé implementace databází poskytují menší zabezpečení, než klasické souborové systémy. [16]

Přestože jsou lidé, konkrétně zaměstnanci podniku, jsou při plánování počítačové bezpečnosti často přehlíženi, vždy jsou pro bezpečnost informací hrozbou. Právě zaměstnanci můžou být nejslabším článkem v zabezpečení informací podniku. Jestliže se správně využije podnikových směrnic, školení, osvěty a technologie, lze zabránit, aby zaměstnanci, ať už cíleně nebo omylem, znehodnocovali nebo ztráceli informace. Využitím slabiny informačního systému v lidech, kteří v něm pracují, se zabývá sociální inženýrství. Sociální inženýrství je založeno na využití lidské chyby a manipulaci s lidmi za účelem získat od nich informace potřebné pro přístup do systému. [16]

Procedury jsou další přehlíženou součástí informačního systému. Procedurami jsou myšleny psané instrukce pro splnění určitého úkolu. Kdyby neoprávněný uživatel získal procedury podniku, znamenalo by to pro integritu informací hrozbu. Většina organizací poskytuje procedury svým zaměstnancům, aby jim umožnily přístup do informačního systému. Hodně z nich ale selhává v zajištění školení pro tyto zaměstnance o ochraně procedur. Učení zaměstnanců k ochraně procedur je pro bezpečnost informačního systému stejně důležité, jako všechna jeho zabezpečení. Znalost procedur by měla být stejně jako všechny kritické informace omezena jen na členy organizace, kteří je musejí nezbytně znát. [16]

Další součástí informačního systému je počítačová síť. Právě počítačové sítě jsou hlavním důvodem potřeby zvyšování bezpečnosti informací. Když se počítače propojí místní sítí a místní sítě se připojí k veřejné síti, jako internet, vznikají nové bezpečnostní hrozby. Technologie, která poskytuje síťové funkce je stále dostupnější i pro menší organizace. Přestože je stále důležité využívání fyzického zabezpečení, jako zámky, pro omezení přístupu k hardware informačního systému, se síťováním počítačů tento postup již nestačí. Je stejně nezbytné provést opatření k poskytnutí síťové bezpečnosti, jako zavedení detekce vniknutí do systému a upozornění odpovědné osoby na probíhající ohrožení. [16]

3.9.5. Výstupní auditorská zpráva

Výstupní auditorská zpráva je základním výstupem auditora. Cílem auditorských zpráv je informovat management, zdůraznit dodržování vnitřních standardů, informovat management o rozsahu a omezeních závěrů, mechanismus pro auditované prosadit své cíle, motivace pro odstranění nedostatků. [16]

3.9.6. Počítačová podpora auditu

Pro usnadnění a urychlení auditorského procesu se využívá software, někdy speciálně navržený pro potřeby auditorů. Obecný auditní software je takovým speciálním typem softwaru. Slouží k prověření automatizovaných funkcí počítačů jako je čtení souborů, výběr a manipulace s daty atd. Software pro analýzu dat. Tento typ softwaru umožňuje výběr vzorků, identifikaci chybějících dat, statistickou analýzu atd. Software typu utility jsou takové programy, které prověřují zpracování, testování programů, systémové činnosti. Testovací data slouží k simulaci transakcí, kterými se testuje logika zpracování. Mapující a monitorující aplikační software zahrnuje specializované nástroje pro analýzu toku dat, dokumentaci logiky, cesty, podmínky kontrol a posloupnosti operací. Auditní a expertní systémy poskytují auditorům podporu při rozhodování. [1]

3.10. Normy pro Audit bezpečnosti IS

Existují tři světově nejrozšířenější normy a směrnice, které jsou při auditu IS aplikovány. Každá z těchto směrnic je vytvořena pro potřeby různých úrovní IT Governance. Jednou směrnicí je COBIT, který je z hlediska IT Governance koncipovaný jako manažerský rámec IT auditu na nejvyšší, velmi obecné úrovni. COBIT lze využít jako směrnici zastřešující všechny etapy IT auditu. Standardy pro podrobnější procesy související s praktickou aplikací auditu jsou popsány směrnicí ITIL, zaměřený na IT správu služeb a v neposlední řadě normou ISO/IEC 17799:2000, jako rámec standardu pro bezpečnost informací. [17]

3.10.1. COBIT

COBIT je tematicky zaměřen na přístup k auditu z hlediska podniku. Není tedy navržen pouze pro použití auditory, ale jako srozumitelný průvodce pro řízení podniku a vlastníky procesu. Právě vlastníci procesu jsou zodpovědní za všechny aspekty procesu, které zahrnují i uplatnění přiměřených kontrol. COBIT vlastníkovi procesu poskytuje nástroj, který usnadňuje zproštění se této zodpovědnosti. Rámec vychází z myšlenky, že k poskytnutí informace, kterou podnik potřebuje k dosažení svých cílů, je IT zdroje třeba spravovat sadou přirozeně seskupených procesů. [17]

Rámec se skládá z 34 kontrolních cílů, jeden pro každý IT proces, seskupených do čtyř domén: Plan and Organise, Acquire and Implement, Deliver and Support, Monitor. Toto uspořádání pokrývá všechny aspekty informace a technologie pro manipulaci s ní. COBIT také zahrnuje průvodce IT Governance, jenž poskytuje strukturu, která spojuje IT procesy, IT zdroje a informace s podnikovými cíli a strategiemi. IT Governance začleňuje optimální způsoby plánování a organizování, pořízení a implementace, dodávání a podporování, monitorování a vyhodnocování výkonu IT. IT Governance podniku umožňuje plně využít své informace, čímž maximalizuje zisky, zpeněžuje příležitosti a získává konkurenční výhodu. [17]

COBIT dále obsahuje 318 detailních kontrolních pravidel, které jsou přiřazeny ke zmíněným 34 kontrolním cílům. Pomocí těchto pravidel lze zhodnotit IT procesy, získat podnět ke zlepšení kontrol a také poskytnout manažerskou jistotu. Pokyny k řízení dále umožňují efektivněji vyjít s potřebami a požadavky IT Governance. Pokyny jsou obecné, jsou procesně orientovány a poskytují manažerské směrnice za účelem získání kontroly nad podnikovými informacemi a souvisejících procesech, dohledu nad plněním organizačních cílů , sledování výkonu v každém IT procesu a porovnání organizačních výkonů. Pokyny k řízení jsou obecné a procesně orientované za účelem zodpovězení následujících typů manažerských otázek: Jak daleko bysme měli zajít a jsou náklady ospravedlněné ziskem? Jaké jsou ukazatele dobrého výkonu? Jaké jsou kritické faktory úspěchu? Jaké je riziko nedosažení našich cílů? Co dělají ostatní? Jak máme měřit a srovnávat? [17]

COBIT přináší tzv. „maturity models“ pro kontrolu IT procesů, takže management může vyznačit, kde se organizace nachází nyní, kde se nachází ve srovnání s nejlepšími hráči ve svém oboru, s mezinárodními standardy a kde se organizace chce nacházet. Kritické faktory úspěchu (CSFs) definují nejdůležitější pokyny k řízení zaměřené na implementaci k získání kontroly nad IT procesy i jejich podprocesy. Ukazatele klíčových cílů (KGIs) definují měřítka, která managementu ukazují, jestli IT proces splnil podnikové požadavky. Ukazatele klíčových cílů jsou vodící ukazatele, která definují měřítka toho, jak dobře si IT proces vede ve snaze plnit cíle. [17]

3.10.2. ITIL

Organizace jsou ve snaze splnit podnikové cíle a naplnit své obchodní potřeby stále závislejší na IT. Tato vzrůstající závislost vede ke kvalitním IT službám na úrovni šité na míru obchodním potřebám a požadavkům uživatelů podle toho, jak se objevují. [17]

Řízení IT služeb se zabývá dodáním a podporou IT služeb, které jsou přiměřené podnikovým požadavkům organizace. ITIL poskytuje komplexní, konzistentní a ucelenou sadu postupů pro management IT služeb a souvisejících procesů přístupem zvyšování kvality k dosažení podnikové efektivity a efektivity využívání IS. Správa procesů služeb je v ITILu zamýšlena jako podpora, nikoli nařízení pro podnikové procesy. V normě ITIL jsou popsány obecné procesy, které mohou být použity jako základ k dosažení standardu ISO/IEC 20000. [17]

Hlavní operační procesy řízení IT služeb jsou popsány ve dvou ITIL publikacích: *Service Support* (podpora služeb) a *Service Delivery* (dodání služeb). Popsané procesy podpory služeb jsou: řízení událostí, řízení problémů, řízení konfigurace, řízen změn, řízení spouštění, funkce služební sekce. Procesy dodání služeb popsané v ITILu jsou: řízení kapacity, řízení dostupnosti, finanční řízení pro IT služby, řízení úrovní služeb, řízení návaznosti IT služeb. V širším měřítku ITIL zahrnuje vývoj nových systémů, návrh a plánování informačních a infrastrukturu komunikačních technologií, provoz a údržbu existujících systémů, přizpůsobení dodání služeb konstantně se vyvíjejícím požadavkům jádra podnikání. [17]

Základní myšlenku ITILu charakterizují dva hlavní koncepty. Prvním konceptem je tzv. celkové řízení managementu (Holistic service management) ve vztahu k manažerům IT služeb. Cílem je zajistit uvážení funkčních na nefunkčních nároků, zajistit aby služby byly před použitím v provozu přiměřeně testovány, vyhodnotit možná rizika a dopad na existující infrastrukturu způsobený novým nebo pozměněným systémem, definovat budoucí nároky na služby. Druhým konceptem je orientace na zákazníka ve vztahu k IT službám, poskytovaných na určité úrovni kvality, která umožňuje trvalou důvěru v tyto služby. K zajištění takové kvality, je přidělena zodpovědnost osobám, které: se radí s uživateli a pomáhají jim využívat služby optimálním způsobem, sbírají a přeposílají názory a doporučení uživatelů, řeší problémy, sledují výkon poskytovaných služeb, řídí změny. [17]

ITIL se skládá z dalších publikací rozdělených podle témat. Kniha plánování implementace řízení služeb se zabývá klíčovými záležitostmi plánování a implementace řízení IT služeb. Také vysvětluje kroky nutné k implementaci a zlepšení doručení IT služeb. Kniha o řízení infrastruktury pokrývá všechny aspekty infrastruktury ICT od určení podnikových požadavků po předkládání procesu k testování, instalaci, zavádění a následná podpora a údržba komponent ICT a IT služeb. Hlavní procesy zahrnuté v řízení všech oblastí a aspektů technologie jsou pojaty v: návrhu a plánování procesů, zavádění procesů, provoz procesů, technická podpora procesů. Řízení aplikací pojednává o vývoji softwaru využitím přístupu životního cyklu a rozšiřuje otázky podnikových změn s důrazem na jasnou definici požadavků a implementaci řešení na míru podnikovým potřebám. Řízení bezpečnosti se zaměřuje na proces plánování a řízení dané úrovně bezpečnosti informací a ICT služeb včetně všech aspektů spojených s reakcí na bezpečnostní události. [17]

3.10.3. ISO 17799

Základní části ISO 17799 Informační Technologie, zásady postupu pro řízení informační bezpečnosti byly vypracovány a publikovány jako britský standard BS 7799-1:1999. Původní standard byl rozdělen do dvou částí. První část pojednávala o zásadách postupu pro řízení informační bezpečnosti v informačních technologiích, druhá část o výkazu s průvodcem pro použití v systémech pro řízení informační bezpečnosti. ISO/IEC 17799:2000 poskytuje informace zodpovědným stranám pro implementaci informační bezpečnosti v podniku. Na standard lez nahlížet jako na základy pro vývoj bezpečnostních standardů a řízení postupů v podniku za účelem zlepšení spolehlivosti informační bezpečnosti v mezipodnikových vztazích. [17; 18]

Průvodní zásady jsou počátečním bodem při implementaci informační bezpečnosti. Opírají se o buď legislativní požadavky, nebo obecně přijímané postupy. Měřítka založená na legislativních požadavcích zahrnují: ochranu a neodhalení osobních dat, ochranu interních informací, ochranu práv duševního vlastnictví. Zmíněné postupy jsou: politika informační bezpečnosti, přidělení zodpovědnosti informační bezpečnosti, stupňování problému, řízení plynulosti podnikání. [17; 18]

Při implementaci systému informační bezpečnosti je třeba zvážit některé faktory rozhodujících o úspěchu projektu. Bezpečnostní politika, její cíle a činnosti odrážejí podnikové cíle. Implementace zohledňuje kulturní aspekty podniku. Je vyžadována otevřená podpora a zapojení vrchního managementu. Je vyžadováno důkladné obeznámení s bezpečnostními nároky, hodnocením a řízením rizik. Účinný marketing bezpečnosti zasahuje všechny zaměstnance včetně členů vedení. Bezpečnostní politika a bezpečnostní opatření jsou sdělovány zainteresovaným třetím stranám. Uživatelé jsou příslušně zaučeni. Pro měření výkonu je dostupný srozumitelný a vyvážený systém, který podporuje trvalé zlepšování prostřednictvím zpětné vazby. [17; 18]

Po představení úvodních informací je představen rámec pro vývoj informačního bezpečnostního systému na míru podniku. Takový systém by se měl skládat přinejmenším z těchto částí: bezpečnostní politika, podniková bezpečnost, roztřídění a řízení aktiv, osobní bezpečnost, fyzická bezpečnost a bezpečnost prostředí, řízení přístupů, vývoj a údržba systému, souvislé podnikové řízení, shoda. [17; 18]

3.10.4. Sladění norem COBIT, ITIL, ISO 17799

Efektivní politika řízení a procedury pomáhají zajistit, že je IT spravováno jako běžná část každodenních aktivit. Přijmutí standardů a ověřených postupů pomůže k rychlé implementaci správných procedur a vyhnout se dlouhým zdržením znovuvynalézáním kola a procesu shody na přístupu k problematice. Nicméně přijaté postupy musejí být konzistentní s řízením rizik a řídícím rámcem vhodným pro podnik a sjednocený s ostatními metodami a postupy, které jsou využívány. Standardy a přijaté postupy ale nejsou všelékem a jejich účinnost závisí na tom, jak byly ve skutečnosti implementovány a udržovány aktuální. Standardy a přijaté postupy jsou nejužitečnější, když se aplikují jako sada zásad a jako výchozí bod pro přizpůsobení zvolených procedur. Při využívání zásad je nutné, aby management i zaměstnanci věděli co a jak dělat a proč je to důležité. Přijaté postupy jsou účinné, pokud jsou formulovány běžnou řečí a standardizovaný postup je zaměřený na reálné podnikové požadavky. Takto je všem umožněno sledovat stejný seznam cílů, problémů a priorit. [17]

Každý podnik musí přizpůsobit použití standardů a postupů, aby vyhovovaly jednotlivým požadavkům. COBIT a ISO 17799 pomáhá definovat co by mělo být uděláno, ITIL managementu služeb poskytuje návod jak to udělat. Typické využití standardů a postupů je podpořit governance poskytnutím politiky řízení a rámec kontrol, zavedením vlastnictví procesů a vymezit odpovědnost za IT aktivity, sladěním cílů IT s podnikovými cíly a nastavením priorit a rozdělením zdrojů, ujištěním o návratu investic a optimalizaci nákladů. Governance lze podpořit ujištěním managementu o účinnosti zavedených kontrol, ujištěním že byla odhalena významná rizika a jsou pro management zřetelná, že byla přidělena zodpovědnost za řízení rizika a to začleněno do organizace. Ujištění, že zdroje byly efektivně rozděleny a že je k dispozici dostatečná kapacita pro výkon IT strategie. Ujistit se, že kritické IT aktivity lze sledovat a měřit, takže problémy mohou být odhaleny a opraveny. [17]

Aby se podnik vyhnul nákladným a nezaměřeným implementacím standardů a přijímaných postupů, je třeba stanovit priority kde a jak tyto standardy a postupy použít. Podnik potřebuje efektivní akční plán, který vyhovuje jeho konkrétním situacím a potřebám. V první řadě je důležité, aby kolegium převzalo vlastnictví IT governance a stanovilo směr, který by měl management sledovat. Toho se nejlépe docílí ujištěním se, že kolegium bere na vědomí IT governance. Kolegium by se mělo ujistit na svém programu, pomoci managementu sladit snahy IT se skutečnými podnikovými potřebami a ujistit ho, že potenciální dopad zasáhne podniková rizika spojená s IT, trvat na tom, aby se měřený výkon hlásil kolegiu, ustanovit správní skupinu IT nebo radu IT governance s odpovědností vykomunikovat problémy v IT mezi kolegiem a managementem, trvat na vytvoření řídícího rámce pro IT governance založeného na společném přístupu, jako je COBIT a rámce přijímaných postupů pro řízení IT služeb založeného na uznávaném standardu, jako je ITIL. [17]

S takovou směrnicí může management zahájit postup implementace a také pomůže managementu rozhodnout kde začít a ujistit ho, že implementační procesy přinesou kladné výsledky tam, kde jsou nejvíce potřeba. K tomu se doporučuje sestavit organizační rámec, nejlépe jako část celkové činnosti IT governance, s jasnou odpovědností, cíly a účastí všech účastněných stran, který posune implementaci kupředu. Dále se doporučuje sladit IT strategii s podnikovými cíly. Ve kterých současných podnikových cílech má IT významný přínos? Dobře porozumět podnikovému prostředí, ochotě riskovat a podnikové strategii, jak se vztahuje k IT. Manažerský průvodce COBITu a jeho kriteria pomáhají stanovit IT cíle. Použitím v kombinaci s normou ITIL, služby a svolené úrovně služeb mohou být definovány v mluvě koncového uživatele. [17]

Dalším doporučením je porozumět a definovat rizika. Jaká jsou rizika spojená se schopností IT vyhovět stanoveným podnikovým cílům? K tomu je třeba zvážit dosavadní průběh a vzorce ve výkonu, současné IT organizační faktory, složitost a měřítko současného nebo plánovaného IT prostředí, průvodní zranitelnost sou časného a plánovaného prostředí, povahu uvažovaných kroků v IT. Procesy pro řízení rizika, použití řídícího rámce a kritéria informací COBITu pomáhají zajistit, že jsou rizika odhalena a vlastněna. Zavádění ITILu vyjasňuje provozní rizika a ISO 17799 vyjasňuje bezpečnostní rizika. Dalším doporučením je definovat cílové oblasti a identifikovat oblasti procesů v IT, které jsou rozhodující pro řízení těchto oblastí rizik. Rámec procesů COBITu může být použit jako základ podpořený ITIL definicí klíčových procesů pro doručení služeb a bezpečnostními cíly ISO 17799. Dále se doporučuje analyzovat současné schopnosti a odhalit mezery, udělat vyhodnocení schopností a zjistit, kde je nejvíce potřeba zlepšení. Pokyny řízení poskytují základy pokryté detailněji v přijatých postupech ITILu a ISO 17799. [17]

Dalším doporučením je vyvinout strategie vylepšení a rozhodnout, které projekty s vysokou prioritou pomůžou zlepšit řízení a správu těchto důležitých oblastí. Toto rozhodnutí by mělo být založeno na potenciálním přínosu, snadno implementovatelné a mělo by se zaměřit na důležité IT procesy a hlavní kompetence. Konkrétní projekty ke zlepšení by měly být navrženy jako část probíhajících zlepšení. Tuto oblast pokrývá COBIT svými kontrolními cíly a kontrolními postupy, podrobněji je rozebrána ve směrnicích ITIL a ISO 17799. Posledním doporučením je měřit výsledky. Pro měření stávajícího výkonu zavést a sledovat mechanismus výsledkových listin pro uvažování nových vylepšení. Přinejmenším by se mělo zvážit. Zda organizační struktura podporuje strategii implementace, zda je v organizaci přidělena odpovědnost za řízení rizika, zda existuje infrastruktura, která usnadňuje a podporuje vytváření a sdílení životně důležitých podnikových informací, zda byly cíle strategie účinně sděleny všem v podniku, kdo je potřebuje znát. [17]

Také existují některá zřejmá, ale užitečná pravidla, kterými by se měl management řídit. Jedním takovým pravidlem nahlížet na implementaci spíše jako na aktivitu projektu, rozdělenou na několik fází, než jako jeden krok. Druhým pravidlem je pamatovat, že implementace, stejně jako nový proces, zahrnuje kulturní změnu, takže klíčovým faktorem úspěchu je ochota a motivace ke změnám. Dále je dobré ujistit se, že cíle jsou snadno pochopitelné. V mnoha podnicích vyžaduje úspěšné zmapování IT čas a jedná se o průběžně se zdokonalující proces, proto je dobré řídit očekávání. Dále je vhodné se nejprve zaměřit na oblasti, kde jsou změny nejsnadněji proveditelné a vylepšení odtud začít jedno po druhém. Vyhnout se tomu, aby činnost začala být vnímána jako čistě byrokratická záležitost a rovněž se vyhnout přístupu nezaměřeného seznamu cílů. [17]

Přijaté postupy musejí být sladěny s požadavky podniku, ucelené mezi sebou a s vnitřními procedurami. COBIT může být použit na nejvyšší úrovni. Poskytuje celkový rámec kontrol založený na modelu IT procesů, které všeobecně sednou každému podniku. Konkrétní postupy a standardy jako ITIL a ISO 17799 pokrývají jednotlivé oblasti a můžou být začleněny do rámce COBIT, takže poskytují strukturu průvodních materiálů. [17]

4. Analytická část

4.1. Stanovení parametrů auditu

Jednalo se o interní audit společnosti. Předmětem auditu byl informační systém prodejního call centra. Cílem auditu bylo určit hlavní bezpečnostní rizika informačního systému v rámci vybraného detašovaného pracoviště a navrhnout adekvátní řešení. Zadavatel si nepřál auditovat bezpečnost serverů, nicméně bylo povoleno zhodnotit oprávnění přístupu uživatelů do sítě a ke službám na straně serverů. Rozsah auditu byl tedy vymezen na klientské PC stanice, jejich softwarové vybavení a uživatele těchto stanic. Žádný test nesměl ovlivnit kvalitu služeb poskytovaných auditovaným informačním systémem.

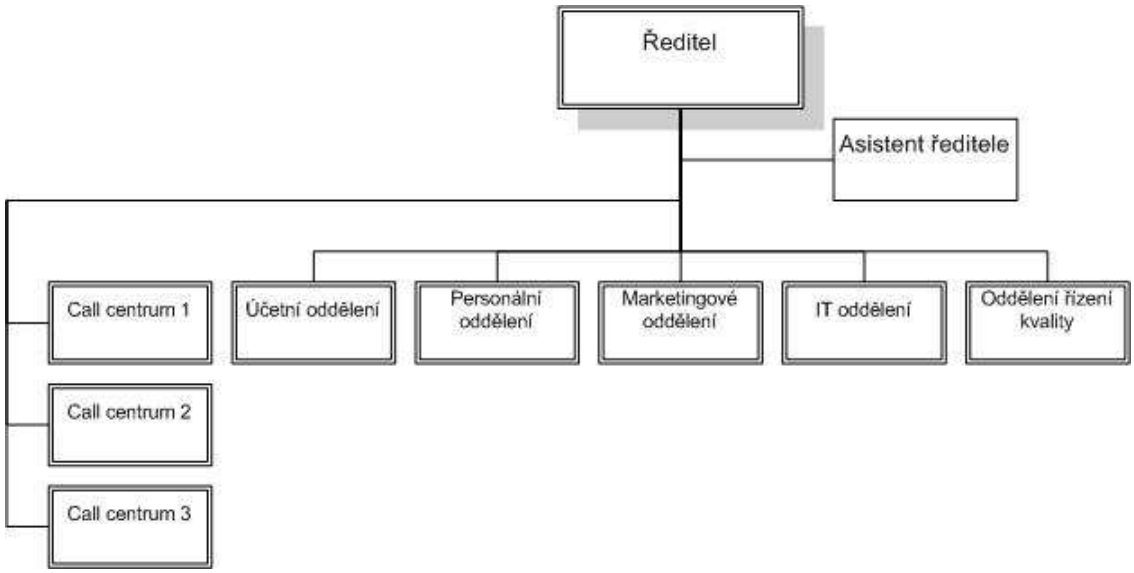
Audit řídila a prováděla jedna osoba po dobu čtyř pracovních týdnů. První týden byl vyhrazen pro poznávání organizace, struktury informačního systému a interní podnikové dokumentace relevantní pro audit. Druhý a třetí týden proběhlo zjišťování stavu bezpečnosti na vybraných objektech. Čtvrtý týden byly výsledky zjišťování vyhodnocovány a na jejich základě byla formulována doporučení pro snížení hlavních bezpečnostních rizik. Odměna za audit byla vzhledem k povaze interního auditu určena na základě smluvené hodinové sazby.

Audit nesměl významně ovlivnit chod pracoviště. Vedoucí dílčích pracovních skupin zahrnutých do auditu byli informováni o povaze auditu a byli svým nadřízeným vyzváni ke spolupráci. Pokud audit vyžadoval zásah do pracovní rutiny, byl takový požadavek v dostatečném předstihu konzultován s příslušným zodpovědným vedoucím. Za případné vlivy nebo dopady auditu na provoz společnosti zodpovídal vedoucí IT oddělení, přímý nadřízený osoby vykonávající audit.

Jako výstup auditu byla určena zpráva obsahující zhodnocení nalezených bezpečnostních rizik a návrh na jejich snížení včetně odhadu nákladů na realizaci.

4.2. Charakteristiky podniku

Jedná se o poměrně mladou firmu, která na trhu působí teprve několik let. Firma má základní kapitál přes 1 milion Kč a zaměstnává přibližně 150 zaměstnanců. Zadavatelská firma působí v oblasti telemarketingu. Organizační struktura podniku se skládá z ředitele, který strukturu zastřešuje a disponuje jedním asistentem. Řízení podniku je rozděleno mezi účetní oddělení, personální oddělení, marketingové oddělení a IT oddělení a oddělení řízení kvality. Provozními pilíři jsou tři dedikovaná call centra.



Obr. č. 1: Organizační struktura podniku

Hlavními předměty podnikání jsou zprostředkování obchodu, služeb a reklamní činnost, marketing. Svým klientům firma nabízí služby aktivního i pasivního telemarketingu. Z aktivního telemarketingu se jedná o přímý prodej a nabídka produktu po telefonu, přímé kontaktování stávajících i potencionálních zákazníků, průzkum trhu přes telefon. Z pasivního marketingu pak příjem objednávek po telefonu, zákaznické linky, infolinky, help linky.

4.3. Podnikové cíle a strategie

Podnik se nyní ještě nachází ve fázi vzniku. Pro podnik je hlavní prioritou získat si na trhu dobré jméno a odlišit své služby nabízené klientům od konkurence. Pro firmu je zásadní, aby byla potencionálními zákazníky vnímána v dobrém světle, a chce založit svojí propagaci na zdůrazňování důvěryhodnosti a spolehlivosti firmy.

Současný stav IT infrastruktury do značné míry představuje slabou stránku podniku, kterou bylo za účelem dosažení zmíněných cílů rozhodnuto odstranit. Podnikovou strategií, která zároveň podnítila audit bezpečnosti, bylo získat mezinárodně uznávaný certifikát o bezpečnosti podnikového informačního systému a informačních technologií podniku. Dílčí strategií pak bylo zvýšit bezpečnost klientských informací na úroveň mezinárodně uznávaných norem.

Kladné reference stávajících i bývalých klientů firmy by jí umožnily lépe pronikat na trh a získávat lukrativnější zakázky. Pro klienty firmy je důležité, aby strategické informace, které jsou podniku přístupné, jakou je například databáze zákazníků, nepadly do rukou konkurence. Potencionální zákazníci firmy při výběru poskytovatele služby do svého rozhodování můžou zahrnout i faktor certifikátu o úrovni bezpečnosti informací uvnitř podniku. Rovněž důležitým faktorem může být pro klienty firmy spolehlivost poskytovaných služeb, protože prostřednictvím těchto služeb dosahují vlastních cílů. Firma tedy zamýšlela zvýšit svojí důvěryhodnost prostřednictvím kladení důrazu na uchování důvěrných informací svých klientů, na spolehlivost a kvalitu nabízených služeb. Uvedené dílčí cíle byly shrnuty do jednoho podnikového cíle a to řízení podnikových rizik, který byl klíčový při stanovení cílů IT.

4.4. Cíle IT

Pro IT bylo klíčovým podnikovým cílem řízení podnikových rizik. Na základě čehož IT oddělení stanovilo dále uvedené cíle IT.

Prvním cílem bylo zajistit, aby ke kritickým a důvěrným informacím neměly přístup nepovolané osoby. Splnění tohoto cíle vyžadovalo formulaci, zavedení a dodržování politiky přístupových oprávnění uživatelů v rámci podnikového informačního systému. Dalším požadavkem pro splnění cíle bylo, aby používaný software byl nakonfigurován tak, aby pro případného narušitele nepředstavoval příležitost pro vyhnutí se zavedené politiky přístupových oprávnění. Dále omezit pohyb osob do prostor, kde probíhá vizuální nebo zvuková výměna důvěrných informací a tyto osoby nemusejí v takovém prostoru nezbytně pobývat pro výkon své práce. Další podmínkou bylo využití směrových mikrofonů pro vzdálenou hlasovou komunikaci pro omezení úniku informací mimo podnik. Nakonec také formulovat pravidla pro ukládání dat na externích datové nosiče a zabezpečení takto uložených dat a fyzické omezení přístupu nepovolaných osob k těmto nosičům.

Druhým cílem bylo zajistit, aby IT služby a infrastruktura odolaly a případně se zotavily ze selhání způsobených chybou, záměrným útokem nebo pohromou. Splnění tohoto cíle bylo podmíněno pořízením bezpečnostního softwaru a důslednou konfigurací zabezpečení serverů. Další podmínkou bylo zavedení bezpečnostních pravidel pro přístup do podnikové sítě. Dále pořízením a konfigurací firewallu, antiviru a používaného software na uživatelských stanicích. Další podmínkou bylo zavedení komplexního automatizovaného zálohovacího systému. Poslední podmínkou bylo pořízení automatizovaného záložního napájecího systému a přepěťových ochran pro klíčové prvky systému. Pro záložní napájecí systém byl stanoven požadavek, aby klíčovým prvkům sítě poskytoval elektrickou energii nejméně 15 minut po přerušení dodávky elektrické energie, což byl stanovený čas pro bezpečné odstavení serverů. Vyžadována byla také provázanost zálohovacího a záložního napájecího systému.

Dalším cílem bylo zajistit minimální dopad na podnik v případě výpadku nebo změny IT služby. Splnění cíle bylo podmíněno souběžným, případně záložním provozem kritických IT služeb, jako připojení k telefonní síti, připojení k internetu, služby DNS serveru, e-mail serveru.

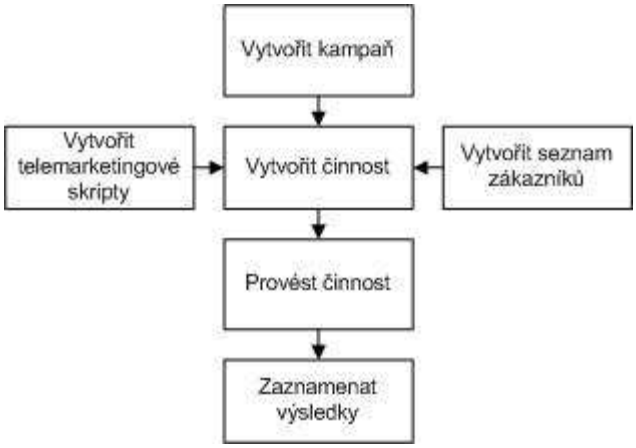
Dalším cílem bylo zajistit, aby výměna informací a automatizované transakce v podniku byly důvěryhodné. Podmínkou splnění cíle bylo zavedení šifrování pro přenos dat přes veřejné sítě a sítě využívající sdílené médium. Předpokladem splnění cíle bylo využít pro přenos dat mezi vzdálenými pracovišti zabezpečené virtuální privátní sítě.

Dalším cílem bylo objasnit dopad podnikových rizik na zdroje a cíle IT. Podmínkou splnění cíle bylo odhalit hrozby pro podnikový informační systém, provést analýzu odhalených hrozeb, stanovit rizika a ohodnotit velikost a pravděpodobnost jejich dopadu na IS/IT podniku.

Předposledním cílem bylo chránit IT vybavení. Předpokladem splnění cíle bylo zpracování a realizace koncepce fyzické ochrany především hardwarové vrstvy podnikového informačního systému. Primární podmínkou bylo zamezit fyzický přístup nepovolaných osob do serverovny. Předpokladem pro splnění cíle bylo také zamezit možnost fyzického přístupu nepovolaných osob do vnitřního prostoru skříně uživatelských stanic. Další podmínkou bylo zavedení pravidel pro bezpečnou práci s počítačem. Dále byla stanovena podmínka zavedení fyzické ochrany nákladného hardwarového vybavení před nepovolanou manipulací nebo krádeží. Podmínkou bylo rovněž zavedení evidenčního systému IT vybavení a politiku odpovědnosti za IT vybavení v podniku.

4.4.1. Podnikové procesy

Proběhlo obeznámení s podnikovými procesy, které přímo souvisejí s hlavní činností call centra. Proces *Vytvořit kampaň* zahrnuje vytvoření koncepce prodeje podle požadavků stanovených klientem. V tomto procesu se na základě komunikace s klientem stanoví atributy kampaně jako styl, velikost, rozsah, nebo specifická přání.

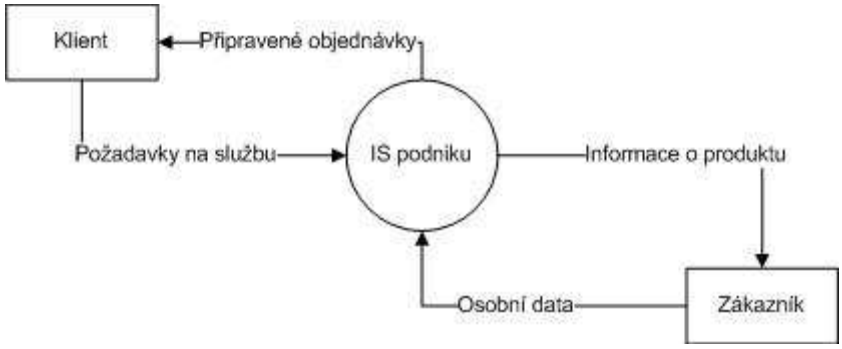


Obr. č. 2: Podnikové procesy call centra

Vlastníkem podnikových procesů call centra je supervizor, který tedy za jejich průběh zodpovídá. Proces *Vytvořit telemarketingové skripty* zahrnuje vytvoření postupu, podle kterého budou operátoři produkt klienta nabízet. Proces *Vytvořit seznam zákazníků* zahrnuje import zákazníků z databáze buď poskytnuté klientem, nebo vlastní databáze telefonních čísel. V procesu *Vytvořit činnost* dochází ke spojení zmíněných procesů. Dojde zde k přidělení zákazníků a telemarketingových skriptů jednotlivým operátorům. Proces *Provést činnost* se skládá z činností stanovených ve vytvořeném telemarketingovém skriptu. Jedná se o samotnou realizaci hovoru, tedy nabídku produktu klienta, sběr informací potřebných pro vytvoření objednávky a jejich zanesení do informačního systému. Nakonec v procesu *Zaznamenat výsledky* dochází k sumarizaci, uložení a předání telemarketingových výsledků klientovi.

4.4.2. Funkční struktura podnikového IS

Na nejvyšší úrovni abstrakce existují v informačním systému call centra čtyři hlavní datové vstupní a výstupní toky.

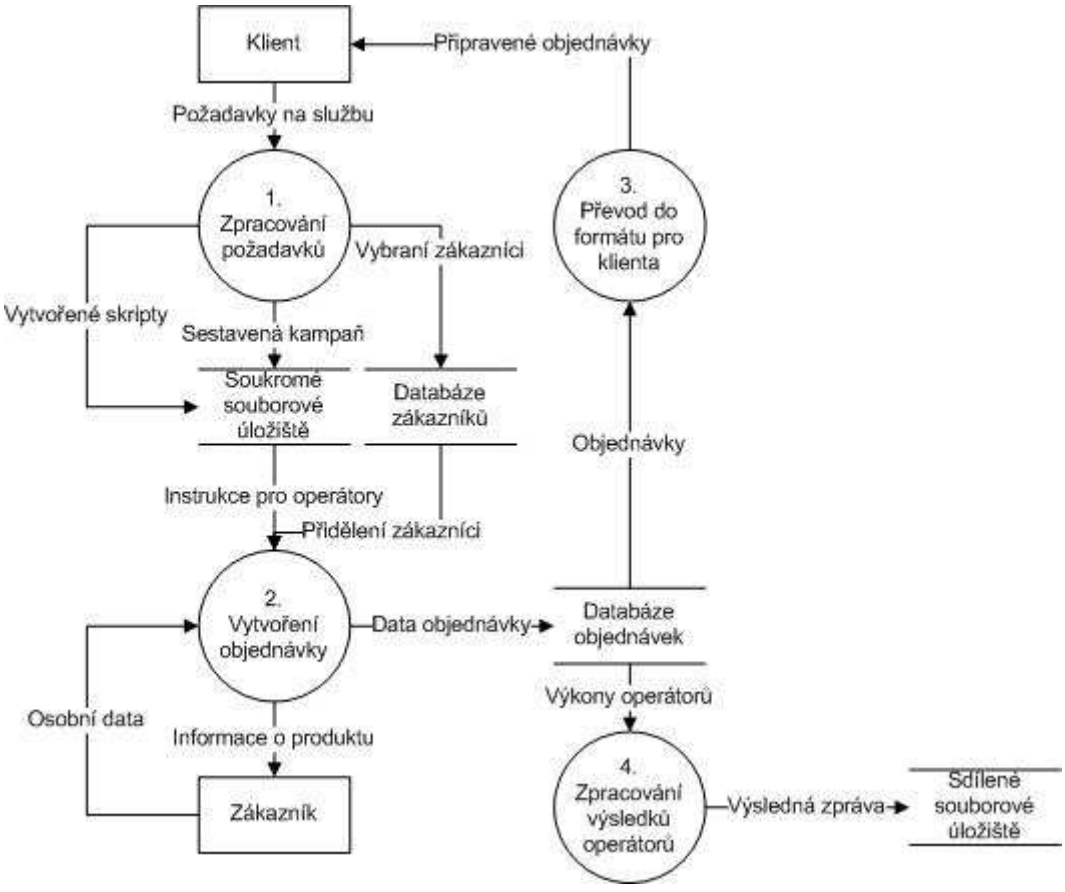


Obr. č. 3:Kontextový diagram datových toků IS podniku

Objekt *Klient* reprezentuje klienta firmy, jedná se o objednatele telemarketingových služeb. Objekt *Zákazník* reprezentuje klientova potencionálního zákazníka, jedná se o kupujícího produktu klienta. Datový tok *Požadavky na službu* vyjadřuje vstupní komunikaci ze strany klienta, ve které specifikuje své požadavky a očekávání od poskytované telemarketingové služby. Datový tok *Informace o produktu* vyjadřuje výstupní komunikaci ze strany informačního systému, konkrétně operátorů k potencionálním zákazníkům klienta, ve které probíhá prezentace nabídky klientova produktu. Datový tok *Osobní data* vyjadřuje vstupní datový tok ze strany zákazníka do informačního systému podniku, konkrétně k operátorovi, kterému sdělí nezájem anebo v případě zájmu osobní údaje potřebné k sestavení objednávky, jako jméno a příjmení, adresu, způsob platby, pokud klient zákazníkům nabízí širší portfolio produktů, tak vybraný produkt a případně množství. Datový tok *Připravené objednávky* vyjadřuje předání získaných objednávek klientovi.

4.4.3. Datové toky podnikového IS

V procesu *Zpracování požadavků* dochází ke sběru požadavků od klienta. Na základě těchto požadavků je vytvořena kampaň, která definuje styl a cíle telemarketingové propagace. Supervizor v tomto procesu také sestaví telemarketingové skripty, které jsou prostřednictvím datového toku *Vytvořené skripty* uloženy do datového skladu *Soukromé souborové úložiště*. *Soukromé souborové úložiště* reprezentuje diskovou kapacitu na uživatelské stanici, která je přístupná pouze jejímu uživateli. Do stejného datového skladu jsou uloženy i dokumenty kancelářského balíku, které obsahují zpracovanou telemarketingovou kampaň.



Obr. č. 4:Diagram datových toků IS podniku

Dále je v procesu *Zpracování požadavků* na základě požadavků klienta vybrána, případně obdržena databáze potencionálních zákazníků, kteří budou postupně kontaktováni. Tyto úpravy v databázi jsou v diagramu reprezentovány datovým tokem *Vybraní zákazníci*, který je vstupem do datového skladu *Databáze zákazníků*.

Jednotlivým operátorům jsou přiděleny kontakty na zákazníky, které budou oslovovat datovým tokem *Přidělení zákazníci*, který je výstupem z datového skladu *Databáze zákazníků*. Operátoři také obdrží instrukce, kterými se mají při jednání se zákazníky řídit datovým tokem *Instrukce pro operátory*. Instrukce operátoři obdrží e-mailem od svého supervizora.

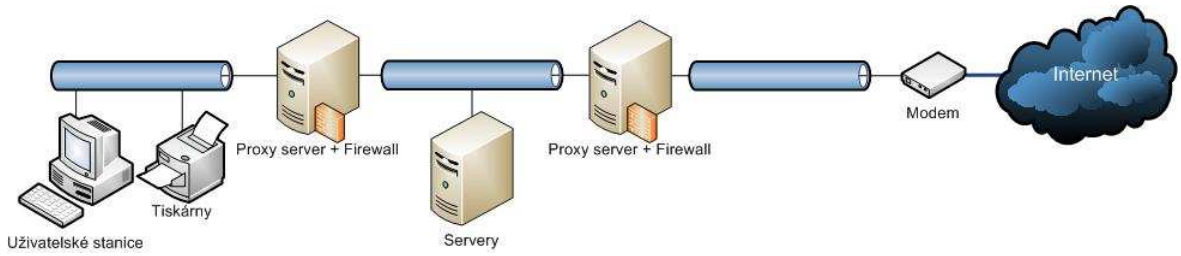
V procesu *Vytvoření objednávky* dochází k vytvoření objednávky prostřednictvím telefonického rozhovoru operátora s potencionálním zákazníkem. Operátor na základě obdrženého telemarketingového skriptu získá od zákazníka požadovaná data, která následně zaznamená do elektronické podoby. Výstupem procesu je datový tok *Data objednávky*, který vyjadřuje objednávku zpracovanou do podoby, se kterou může informační systém dále zpracovat.

Takto zpracovaná objednávka se uloží do datového skladu *Databáze objednávek* z datového skladu *Databáze objednávek* je čerpáno datovým tokem *Objednávky*, který vyjadřuje pouze data z databáze, která a jsou nezbytná pro realizaci objednávky a klient je tedy vyžaduje. V procesu *Převod do formátu pro klienta* dochází ke změně formátu výstupů z databáze do formátu, který může být zpracován informačním systémem klienta. Výstupem procesu je datový tok *Připravené objednávky*, který reprezentuje takto přeformátovaná data objednávek do podoby, jak je obdrží klient.

Z databáze objednávek je rovněž čerpáno datovým tokem *Výkony operátorů*. Jedná se pouze o data, která supervizor potřebuje k ohodnocení výsledků jednotlivých operátorů i kampaně jako takové. Datový tok *Výkony operátorů* je vstupem procesu *Zpracování výsledků operátorů*. V tomto procesu supervizor zpracuje výkony operátorů do dokumentů kancelářského balíčku, konkrétně textovým a tabulkovým procesorem.

4.4.4. Technická struktura

Počítačová síť call centra je rozdělena na tři fyzické podsítě. Na následujícím obrázku v první podsíti vpravo, je umístěn modem s připojením na internet a přední firewall. V podsíti na diagramu uprostřed se nachází demilitarizovaná zóna ohraničená dvěma firewally, ve které jsou umístěny servery. V podsíti na diagramu vlevo jsou všechny uživatelské stanice a periferie chráněné zadním firewallem.



Obr. č. 5: Diagram podnikové počítačové sítě

Call centrum je připojeno k internetu přes optickou páteřní síť. V klimatizované serverovně je rack se třemi 24 portovými switchi, oba proxy servery, doménový server, directory server, e-mail server, file server, databázový server a telefonní centrála. Do podnikové sítě je připojeno přibližně 50 uživatelských stanic a tři tiskárny. Prvky jsou k síti připojeny výhradně UTP kabely, které jsou vedeny k jednotlivým uživatelským stanicím pod podlahou, zásuvky se síťovými konektory jsou označeny evidenčním číslem.

Uživatelské stanice jsou osazeny dvoujádrovým procesorem, 4 GB operační paměti, grafickou kartou, integrovaným zvukovým adaptérem, integrovaným síťovým adaptérem, pevným diskem s kapacitou 500 GB a mechanikou DVD-ROM. Vstupy uživatelské stanice jsou dvanáct USB 2.0 port, jeden sériový port, dva PS/2 porty a jeden port RJ-45.

5. Vlastní řešení

5.1. Zhodnocení vnitřních směrnic a dokumentace

Zkoumané podnikové směrnice pokrývaly problematiku provozu oddělení informačních technologií, řád pro obsluhu výpočetní techniky, definovaly zodpovědnost za majetek a kritické procesy podniku jako celky.

Nedostatkem směrnic o provozu oddělení informačních technologií byla jejich neúplnost. Úpravy směrnic nebyly nikdy provedeny, směrnice byly od svého vzniku nezměněny. Činnosti, které byly ve směrnicích popsány, zachycovaly potřeby ICT podniku před více než rokem. Směrnice tedy popisovaly činnosti, které již kvůli změně architektury ICT nejsou prováděny a naopak v nich byly opomenuty důležité aktuální činnosti, jako zálohování nebo způsob ohlašování poruch ICT. V pořádku byla směrnice pro přidání nového uživatele systému.

Dokumentace podnikové počítačové sítě byla aktuální a změny v ní byly prováděny v dostatečném intervalu, aby odpovídala současnému stavu. Dokumentace ale nebyla ucelená. Jednotlivé aspekty sítě byly zachyceny v několika dokumentech a většinou nebyly okomentovány, takže bez slovní interpretace mohlo dojít k chybnému pochopení zaznamenaných informací. V pořádku byla stanovena globální pravidla pro přístup do podnikové sítě.

Předpis o zodpovědnosti za kritické procesy byl zformulován na vysoké úrovni abstrakce a jako odpovědné osoby zmiňoval výhradně vedoucí oddělení. Nedostatkem předpisu tedy byla absence rozdělení odpovědnosti zaměstnanců IT oddělení za jednotlivé podprocesy, které se významně podílejí na poskytování kritických služeb podnikového informačního systému.

Řád pro obsluhu výpočetní techniky byl pořádku, obsahoval problematiku bezpečného zacházení s výpočetní technikou jak z pohledu ochrany majetku, tak ochrany zaměstnanců před úrazem.

5.2. Zjištění povědomí zaměstnanců o bezpečnostních směrnicích

Pro zjištění, jak jsou zaměstnanci obeznámeni se základními bezpečnostními principy, byl vybrán způsob vyplnění dotazníku. Nejprve bylo určeno, že dotazník by měl přinést náhled o tom, jak by zaměstnanci řešili některé situace, které by mohly mít za následek snížení bezpečnosti informačního systému. Dotazník byl proveden v papírové formě a distribuován byl osobně. Dotazovaní měli na zodpovězení otázek pět minut a vyplňovali ho pod dohledem dotazovatele, aby nedocházelo k výměně informací mezi účastníky dotazování. Cílovou skupinou byli operátoři a supervizoři. Zjišťování se účastnil každý z cílové skupiny, kdo byl v době zjišťování přítomen na pracovišti.

Následně bylo zkonstruováno deset uzavřených výběrových otázek s několika alternativami. Dotazovaní měli vybrat vždy jen jednu alternativu. Do dotazníku byly zahrnuty dvě otázky z oblasti fyzické bezpečnosti, dvě otázky z oblasti datové bezpečnosti, dvě otázky z oblasti bezpečnosti:

- Při práci s počítačem je dovoleno: pít z hrnku i z lahve; pít pouze z lahve; není dovoleno pít
- Myš, klávesnice a monitory je dovoleno: odpojovat podle potřeby; odpojit, pokud je na to upozorněn nadřízený; není dovoleno odpojovat
- Do počítače je dovoleno stahovat soukromá data prostřednictvím:hardwarového média i internetu; pouze prostřednictvím internetu; není dovoleno.
- V pracovním prostoru je dovoleno použití mobilního telefonu k: pořízení zvukového i obrazového záznamu; vyřízení soukromého hovoru; není dovoleno používat mobilní telefon.
- Pokud si zaměstnanec IT oddělení vyžádá heslo uživatelského účtu, heslo mu: sdělím; nesdělím.
- Pracovní stanici je povinnost uzamknout, pokud se její uživatel vzdálí na: méně než 5 minut; 5 - 10 minut; 10 a více minut; není povinnost uzamknout.

Dotazování se zúčastnilo 38 respondentů. Nasbírané údaje byly převedeny do elektronické formy k dalšímu zpracování v tabulkovém procesoru. Po převedení do elektronické formy byla ověřena věrohodnost údajů kontrolou minimálních a maximálních hodnot a průměru. Odpovědi v jednotlivých formulářích jsou uvedeny v příloze č.1.

5.3.Stav bezpečnosti

Zjišťování stavu bezpečnosti proběhlo na vybraném vzorku deseti uživatelských stanic. Jednalo se o tři krátkodobě nepoužívané stanice a sedm využívaných stanic, na kterých bylo provedeno hodnocení v době přestávky uživatele. Zjištěné nedostatky byly většinou společné pro všechny zkoumané stanice. Ve všech kontrolovaných případech operátoři využívali směrový mikrofon.

Z hlediska fyzické ochrany uživatelských stanic neexistoval žádný bezpečnostní mechanismus pro omezení manipulace uživatelů s hardware. BIOS stanice nebyl zaheslován. Pro přístup do podnikové sítě musela mít uživatelská stanice MAC adresu schválenou pro danou podsíť, IP adresa byla stanici přidělena serverem. Uživatelské stanice se přihlašovaly do domény a uživatelé se do systému přihlašovali prostřednictvím uživatelských účtů v Active Directory. Na stanicích byl nainstalován výhradně operační systém Windows 7 Professional 64-bit.

Aktualizovaný operační systém měly pouze tři stanice. Software nezbytný pro práci uživatele zahrnoval pouze internetový prohlížeč, v tomto případě Internet Explorer 8 a e-mailového klienta Micorsoft Office 2007. Bezpečnostní software, který měl být na uživatelských stanicích aktivní, byl Symantec Endpoint Protection. Nicméně přestože nepoužívané stanice byly považovány za připravené pro nové uživatele, zmíněný software nebyl na dvou z nich vůbec nainstalován. Na čtyřech stanicích nebyl bezpečnostní software aktualizován a podle záznamů probíhala pravidelná kontrola disku pouze na jednom z nich. Na ostatních stanicích byla kontrola vždy zrušena uživatelem.

Na stanicích byla pro uživatele nastavena administrátorská práva, v důsledku čehož se na nich nacházel neschválený software jako ICQ klient a data nesouvisející s prací, jako videozáznamy nebo hudba. Dodatečnou kontrolou antivirem byl zjištěn na jedné z nepoužívaných stanic jeden virus, který ale nepředstavoval reálnou hrozbu. Na všech kontrolovaných stanicích byly nalezeny účty bývalých uživatelů z doby před zavedením Active Directory s administrátorským oprávněním.

5.4.Analýza rizik

Chráněným aktivem byly určeny uživatelské stanice, které přechodně obsahují strategické podnikové informace. Jedná se o výstupy z databáze zákazníků a vstupy do databáze objednávek, komunikaci se zákazníkem a vnitropodnikovou komunikaci. Jako slabina byla určena absence politiky uživatelských práv na uživatelských stanicích

Jako hlavní hrozby byly určeny hrozby. Hlavní hrozbou byl určen škodlivý software, čímž je myšlen veškerý software, který se samovolně instaluje na uživatelské stanice a nějakým způsobem komplikuje fungování procesu nebo kompromituje bezpečnost, jako viry, trojské koně, spyware apod. Další hrozbou bylo využití slabin využívaného software, a to jak těch, které lze odstranit aktualizací, tak těch které odstranit nelze, protože aktualizace odstraňující slabinu ještě nebyla vydána. Jako další hrozba byli určeni uživatelé a to z hlediska cíleného jednání za účelem poškodit firmu nebo jednotlivce i z hlediska nedbalosti. Jako další hrozba byly stanoveny sociální sítě, prostřednictvím kterých hrozí šíření škodlivého software a únik citlivých informací. Další hrozbou byly mobilní zařízení, těmi je rozuměno mobilní telefony, smartphony a podobně. Ty disponují stále více možnostmi interakce s jinými elektronickými zařízeními a možností zaznamenávat a odesílat zvukový i obrazový záznam. V neposlední řadě bylo jako hrozba určeno sociální inženýrství, které pro sběr citlivých informací využívá např. phishing.

Na základě IT cílů, struktury podnikového IS, technické struktury a určení hrozeb byla stanovena rizika:

- uniklé informace vlivem úmyslného i neúmyslného jednání uživatele
- snížená funkcionalita stanice vlivem škodlivého software
- poškození nebo krádež hardware
- přítomnost nelegálního software nebo jiné porušení autorských práv vlivem uživatele

Pro hodnocení efektivnosti zavedených kontrol bylo užito metody DREAD. Před samotným stanovením rizika byla stanovena jeho přijatelná hranice. Ukazatele hrozeb byly ohodnoceny hodnotou ve spojitém intervalu 0 až 10. Hodnota 0 pro ohodnocení způsobené škody (D_1 - damage) by vyjadřovala zanedbatelnou škodu způsobenou v případě nastání rizikové situace. Naopak hodnota 10 by vyjadřovala škodu takového rozsahu, která by měla za následek zničení informačního systému včetně dat v něm uložených. Nejnižší hodnota opakovatelnosti (R - reproducibility) by vyjadřovala nemožnost znovu využít stejné slabiny. Nejvyšší hodnota by pak vyjadřovala velmi snadné využití stejné slabiny opakovaně. Hodnota 0 využitelnosti (E - exploitability) by vyjadřovala vysokou složitost provedení útoku k realizaci hrozby. Naopak hodnota 10 by vyjadřovala tak nízkou složitost provedení, že by ho zvládnul i uživatel s minimálními znalostmi. Nejnižší hodnota počtu ovlivněných uživatelů (A - affected users) by vyjadřovala, že by nastalým rizikem nebyl nikdo ovlivněn, Nejvyšší hodnoty by pak vyjadřovala, že postiženi by byli všichni uživatelé. Hodnota 0 objevitelnosti (D_2 – discoverability) by vyjadřovala, že riziko je pro útočníka velmi obtížně zjistitelné. Hodnota 10 by vyjadřovala, že riziko by bylo pro útočníka patrné při získání základní orientace v systému.

Risk =(DAMAGE+REPRODUCIBILITY+EXPLOITABILITY+AFFECTED_USERS+DISCOVERABILITY)/5

Hrozba	D_1	R	E	A	D_2	Velikost rizika	Požadované max. riziko
Škodlivý software	9	10	4	4	5	6,4	3
Uživatelé	7	8	8	5	6	6,8	5
Sociální sítě	4	9	6	2	7	5,6	4
Mobilní zařízení	5	10	9	4	8	7,2	6
Sociální inženýrství	9	7	4	6	5	6,2	5

Tab. č. 1: Rizika metodou DREAD

Cílem auditu nebylo navrhnout opatření snižující náklady, nicméně byla provedena zevrubná analýza ztrát kvůli zprávě o doporučených opatření pro vedení. Pro ohodnocení ekonomických dopadů efektivnosti kontrol bylo využito metody očekávaných ztrát. Ztráta zpracovávaných dat by měla za následek obtížně vyčíslitelnou hodnotu ztráty ve formě snížení důvěryhodnosti z pohledu klienta. Velikost škody při ztrátě dat byla vyčíslena na základě odhadu supervizora ohodnocení nákladů na pořízení těchto dat. Velikost škody vlivem snížené funkcionality byla vyčíslena vedoucím IT oddělení na základě přiměřených nákladů na odstranění škodlivého software a ztrátami z ušlé příležitosti vzniklé nemožností využívání stanice. Škody na hardware byly odhadovány na základě ceny periferií, které bývají nejčastěji postiženy neopatrným zacházením, jako monitory, klávesnice a myši. Odhad velikosti škody na hardware byl rovněž odhadnut vedoucím IT oddělení. Velikost škody způsobené nelegálním software je do značné míry spekulativní, protože se nejedná o reálnou způsobenou škodu. Velikost škody způsobené nelegálním software byla vedoucím IT oddělení stanovena na základě přibližné pořizovací ceny běžně instalovaného stahovaného software, ceny hudby a filmů. Pravděpodobnost výskytu pak byla odhadnuta na základě odborného odhadu specifických vedoucích.

Popis rizika	Velikost škody [Kč/výskyt]	Pravděpodobnost výskytu [%/rok]	Očekávané ztráty [Kč/rok]
Unik informací způsobený uživatelem	1200	3200	38400
Snížená funkcionalita vlivem malware	550	11500	63250
Škody na hardware	900	600	5400
Nelegální software	2000	1700	3400

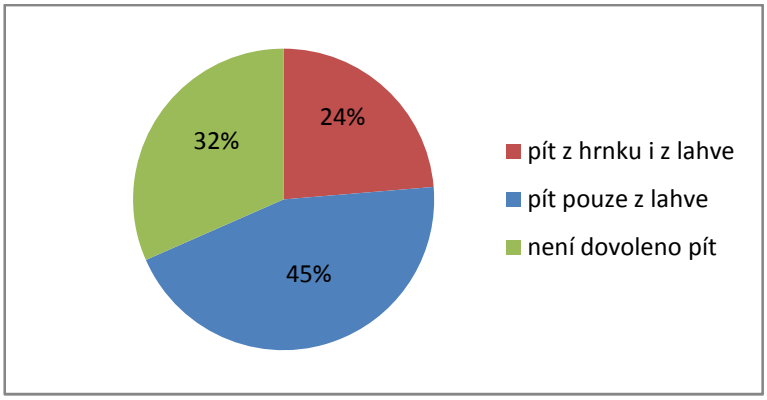
Tab. č. 2:Rizika metodou očekávaných ztrát

Celkové náklady na nápravu škod zaviněných slabou bezpečností informačního systému činí 141 050 Kč ročně.

6. Zhodnocení výsledků a doporučení

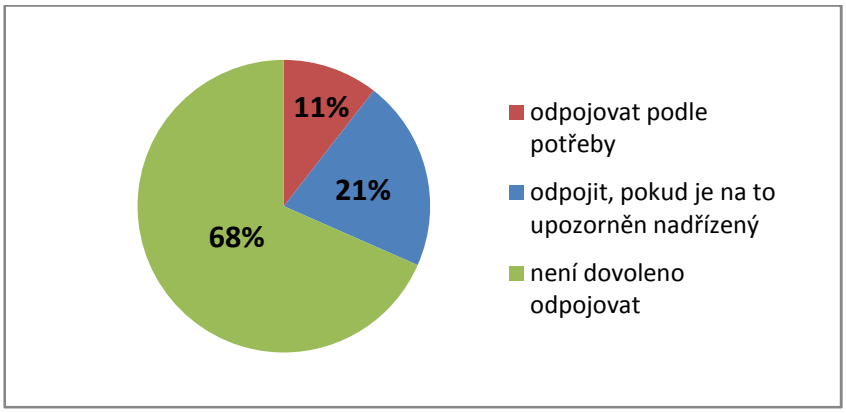
6.1.Zhodnocení povědomí o bezpečnostních směrnicích

Výsledek dotazování na otázku, z fyzické bezpečnosti majetku, zda je zaměstnancům dovoleno při práci na počítači se nejvíce uživatelů se domnívalo, že můžou pít při práci z lahve. To ale není podle směrnice pravda, zaměstnanci mají k občerstvení využít k tomu určené prostory mimo pracovní plochu. Přibližně čtvrtina zaměstnanců by se pak nezdráhala pít u počítače i ze sklenice či hrnku.



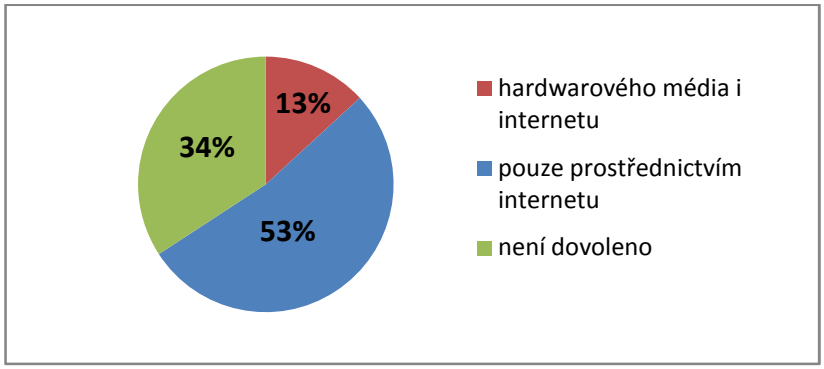
Obr. č. 6: Graf odpovědí na dotaz: Při práci s počítačem je dovoleno…

V další otázce zaměstnanci odpověděli na dotaz, zda je jim dovoleno odpojovat počítačové periferie tak, že většina se správně domnívá, že směrnice jim periferie odpojovat nedovoluje, avšak přibližně pětina dotázaných se domnívá, že pokud by nastala potřeba periferii odpojit, povolení k tomu jim může dát jejich přímý nadřízený. Desetina účastníků dotazníku by o odpojení periferie nikoho neinformovala.



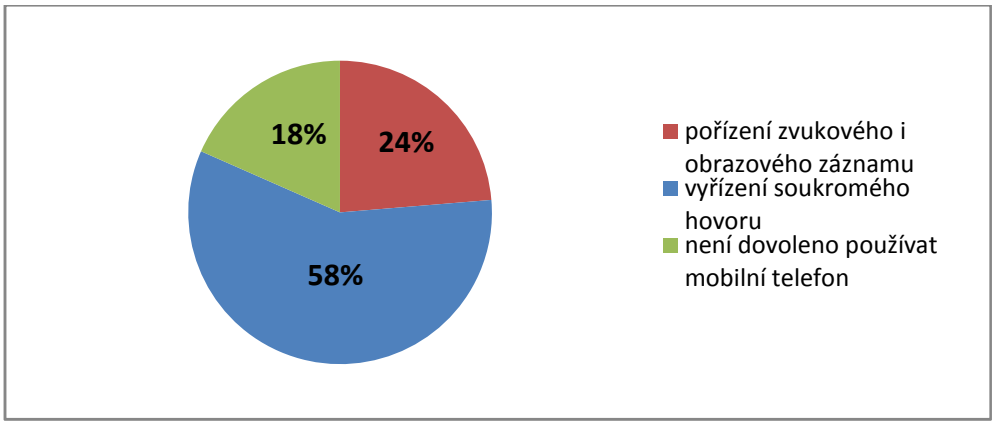
Obr. č. 7: Graf odpovědí na dotaz: Myš, klávesnice a monitory je dovoleno…

Z odpovědí na otázku z oblasti bezpečnosti informací, do jaké míry je dovoleno stahovat soukromá data na uživatelskou stanici, bylo zjištěno, že přibližně polovina dotazovaných si se domnívá, že stahovat elektronický obsah z internetu je v pořádku. Směrnice nedovolují žádné neschválené přenosy dat z nebo na uživatelské stanice ať už prostřednictvím internetu, nebo fyzických datových nosičů.



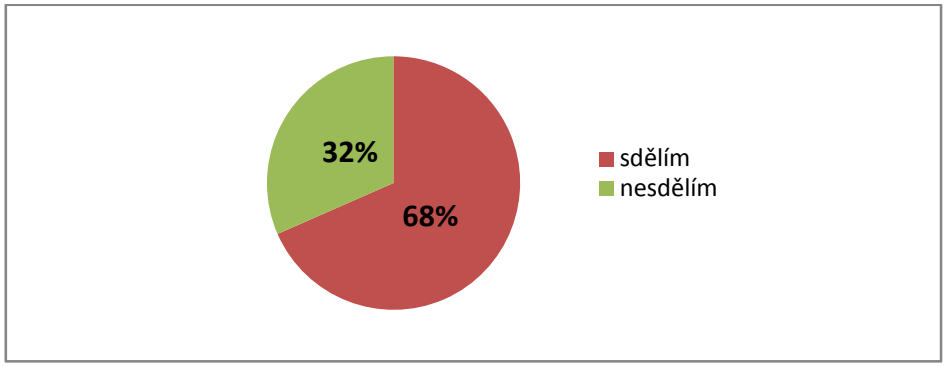
Obr. č. 8: Graf odpovědí na dotaz: Do počítače je dovoleno stahovat soukromá data prostřednictvím…

Na otázku, jakým způsobem je dovoleno využívat v pracovním prostoru mobilní telefon bylo odpovězeno tak, že přibližně čtvrtina dotazovaných si je vědoma, že směrnice nepovoluje užívání mobilního telefonu v blízkosti pracovního prostoru. Naopak přibližně pětina dotazovaných by při práci pořídila obrazový i zvukový záznam. Téměř 60% dotazovaných se domnívá, že je v pořádku vyřídit si v pracovním prostoru soukromý hovor.



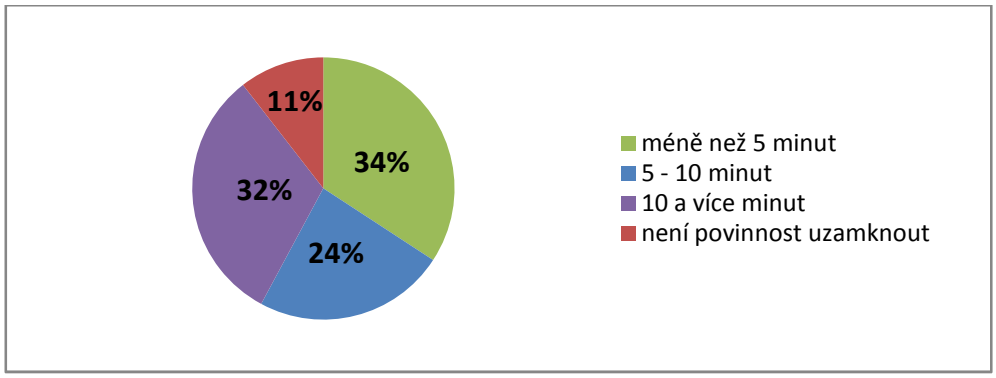
Obr. č. 9: Graf odpovědí na dotaz: V pracovním prostoru je dovoleno použití mobilního telefonu k…

Odpovědi na otázka z bezpečnosti přístupu, zdali by dotazovaní poskytli zaměstnanci IT heslo, pokud by o ně požádal vyplynulo, že přibližně dvě třetiny dotazovaných by tak učinilo. Směrnice vyžaduje, aby hesla uživatelských účtů nebyla sdělována jiným osobám. Uživatelé tedy představují kritickou slabinou informačního systému, v případě napadení metodou sociálního inženýrství.



Obr. č. 10: Graf odpovědí na dotaz: Pokud si zaměstnanec IT oddělení vyžádá heslo uživatelského účtu, heslo mu…

Výsledky posledního dotazu poukázaly na to, jak důsledně uživatelé uzamykají přístup ke svému účtu a tedy i pracovní stanici, když se mají vzdálit od pracovišť. Směrnice stanovuje, že uživatel musí stanici uzamknout při každém odchodu od pracovní stanice. Přibližně třetina uživatelů účet uzamkne, pokud se vzdálí i jen na kratší dobu. Více než polovina uživatelů stanici uzamyká, pokud se vzdálí na delší dobu a přibližně desetina stanici vůbec neuzamyká.



Obr. č. 11: Graf odpovědí na dotaz: Pracovní stanici je povinnost uzamknout, pokud se její uživatel vzdálí na…

Z výsledků dotazování vyplynulo, že uživatelé nejsou dostatečně obeznámeni s podnikovými směrnicemi. Kromě ochoty uživatelů sdělit své heslo jiným osobám ale nebyly odhaleny kriticky závažné nedostatky. Vzhledem k přiměřeným výsledkům dotazování by tedy bylo neefektivní zavádět hromadné pravidelné semináře o principech bezpečnosti. Místo toho bylo doporučeno, aby zaměstnanci IT oddělení vypracovali krátké poučky o bezpečnosti s nejdůležitějšími pokyny a ty postupně např. jednou týdně rozeslali formou vnitropodnikového oběžníku prostřednictvím hromadného e-mailu.

6.2. Bezpečnostní doporučení

Na základě odhalených slabin informačního systému byla formulována doporučení pro jejich minimalizaci. Doporučeno bylo zakázat v BIOSu pro nevyužívaná rozhraní IDE a SATA, včetně rozhraní, přes které je připojena pro operátory nepotřebná DVD mechanika. Rovněž bylo doporučeno deaktivovat v BIOSu nadbytečné USB porty. Doporučeno bylo nastavit zavádění operačního systému pouze z pevného disku a z žádného jiného vstupu. Posledním, ale neméně významným doporučeným nastavením BIOSu bylo aktivovat pro vstup do nastavení přiměřeně složité heslo.

Z oblasti správy účtů bylo doporučeno odebrat uživatelům administrátorská práva. Dále pak odstranit staré lokální účty po bývalých uživatelích. Jako bezpečnostní opatření bylo doporučeno vytvořit lokální administrátorský účet s netradičním jménem, nastavit na něj složité heslo a původnímu defaultnímu administrátorskému účtu odebrat administrátorská oprávnění. Takový falešný administrátorský účet by pak posloužil pro případné narušitele jako návnada.

Doporučeno bylo rovněž zakázat spouštění nepotřebných služeb operačního systému, dále odebrání pro operátory nepotřebných oprávnění jako změna nastavení, především instalace nových programů. Také bylo doporučeno odebrat uživatelům přístup k nepotřebným hardwarovým prostředkům a zařízením a odebrání oprávnění k instalaci nového hardware. Rovněž bylo doporučeno nastavit pro uživatele přiměřenou diskovou kvótu.

Doporučeno bylo nastavit aktualizace systému i bezpečnostního software na automatické vyhledávání, stahování i instalování bez nutnosti souhlasu uživatele. Nastavení činnosti bezpečnostního software bylo doporučeno provádět antivirovou kontrolu s upozorněním uživatele, ale nastavit načasování pravidelných kontrol na dobu obědové přestávky. V bezpečnostním software bylo navíc doporučeno nastavit adekvátní heslo potřebné pro změnu jeho nastavení. Bylo doporučeno nastavit firewall stanic na zablokování příchozí i odchozí komunikace na portech, které nejsou využívány a zakázat síťovou komunikaci všem aplikacím, které nejsou uvedeny v seznamu výjimek.

V internetovém prohlížeči bylo doporučeno nastavit automatické aktualizace a využívání šifrovaného přenosu dat. Dále bylo doporučeno nastavit zabezpečení prohlížeče tak, aby byly zakázány ovládací prvky ActiveX označené jako bezpečné, protože jejich označení není zárukou bezpečnosti. Dále bylo doporučeno zakázat parametr META REFRESH, jelikož ten dovoluje načítat další stránky bez uživatelovy iniciativy, zakázat spouštění programů a souborů v sekci IFRAME, protože je využíváno ke spuštění potencionálně nebezpečného kódu.

6.3.Předpokládaný efekt na bezpečnost po zavedení opatření

Nastavení doporučená BIOSu by měla za následek snížení využitelnosti ze strany hrozby uživatele a mobilních zařízení. Doporučené změny ve správě účtů by měly za následek rovněž snížení využitelnosti ze strany hrozby uživatelem, dále snížení škody, která může být touto hrozbou napáchána a došlo by i ke snížení množství postižených uživatelů hrozbou nejen ze strany uživatele, ale i ze strany škodlivého software sociálního inženýrství. Změny v uživatelských oprávněních v operačním systému by se projevily snížením rizika ze strany všech sledovaných hrozeb z hlediska využitelnosti. Doporučeným nastavením aktualizace software a konfigurace bezpečnostního software by došlo ke snížení rizika ze strany všech hrozeb z hlediska opakovatelnosti. Doporučená nastavení na internetovém prohlížeči by snížila škody, opakovatelnost i využitelnost slabiny ze strany hrozby škodlivého software. Výsledné předpokládané riziko podle hrozeb je uvedeno v následující tabulce.

Hrozba	D_1	R	E	A	D_2	Velikost rizika	Požadované max. riziko	Původní velikost rizika
Škodlivý software	4	2	1	2	5	2,8	3	6,4
Uživatelé	5	6	5	3	6	5	5	6,8
Sociální sítě	3	6	3	1	7	4	4	5,6
Mobilní zařízení	4	8	6	4	8	6	6	7,2
Sociální inženýrství	7	3	3	6	5	4,8	5	6,2

Tab. č. 3:Předpokládaný efekt doporučených opatření na bezpečnost IS

Tabulka znázorňuje, že by se realizací doporučených opatření podařilo snížit riziko hrozeb na požadovanou úroveň. Nejvyšší dopad by opatření měla na hrozbu ze strany škodlivého software.

6.4.Předpokládaný efekt na rozpočet po zavedení opatřeni

Navrhovaná opatření by se do nákladů projevila následovně. Pravděpodobnost úniku informací způsobených uživatelem by se snížila díky omezení datových vstupů uživatelské stanice a osvětě zaměstnanců o bezpečnosti informací. Náklady způsobené sníženou funkcionalitou vlivem škodlivého software by se snížila důsledkem omezení uživatelských oprávnění a nastavení bezpečnostního software. Škody na hardware lze snížit rovněž osvětou uživatelů o bezpečnosti práce. Potencionální ztráty prostřednictvím pokut za umístění nelegálního software by se snížily vlivem omezených uživatelských oprávnění a zavedením diskových kvót.

Popis rizika	Velikost škody [Kč/výskyt]	Pravděpodobnost výskytu [%/rok]	Očekávané ztráty [Kč/rok]
Únik informací způsobený uživatelem	1200	800	9600
Snížená funkcionalita vlivem malware	550	1200	6600
Škody na hardware	900	500	4500
Nelegální software	600	200	1200

Tab. č. 4:Rizika metodou očekávaných ztrát

Původní celkové teoretické náklady na nápravu škod činily 141 050 Kč za rok. Očekávané náklady na nápravu škod po zavedení doporučených opatření činily 21 900 Kč za rok. Na těchto nákladech by tedy podnik mohl ročně ušetřit 119 150 Kč.

Přibližná doba potřebná pro provedení doporučených nastavení včetně očekávaných prostojů činí 50 minut. Nastavení bylo nutné provést na přibližně 50 uživatelských stanicích. Z toho vyplývá, že uvedení doporučení do praxe by si vyžádalo přibližně 42 člověkohodin. Náklady na zavedení, při předpokládané hodinové mzdě IT pracovníků 125 Kč, činily 5 250Kč. V případě, že by se opatření zaváděla mimo obědovou přestávku uživatelů, bylo by nutné do výpočtu zahrnout i ušlý zisk, který vyplývá z nemožnosti využívat pracovní stanici po dobu provádění úkonu.

7. Závěr

Výsledkem práce byl interní audit bezpečnosti IT, který byl v souladu s podnikovými cíly a cíly IT. Audit se pevně držel vymezeného pole působnosti a kompetencí. Proces vykonání auditu rovněž nepostihl provoz podniku.

V práci byly zhodnoceny vnitřní směrnice a odhaleny jejich nedostatky. Hlavním nedostatkem směrnic byla nízká aktuálnost. Rovněž byl zhodnocen efekt směrnice pro obsluhu výpočetní techniky formou dotazování uživatelů na vybrané body této směrnice. Výsledek dotazování se ukázal jako poměrně uspokojivý, ale bylo doporučeno zlepšit povědomí o bezpečnosti informací formou pravidelného vnitropodnikového oběžníku na téma bezpečnost informací.

Dále byly v práci vyhodnoceny hrozby a rizika auditované části informačního systému. Jako hlavní hrozba z hlediska bezpečnosti informací byly vyhodnoceny mobilní telefony, prostřednictvím kterých může dojít nejsnáze k úniku informací mimo podnik a které můžou rovněž posloužit jako datové médium, prostřednictvím kterého může dojít k přenosu dat do nebo z uživatelské stanice. Na přibližně stejné úrovni se umístily hrozby ze strany škodlivého software, jednání uživatelů a sociálního inženýrství. Hlavním rizikem, který produkoval nejvyšší náklady na své odstranění za rok, byl škodlivý software.

Byla formulována doporučení pro snížení hlavních rizik z hlediska nastavení BIOS, operačního systému a software uživatelských stanic. Doporučení byla stanovena na základě cílů IT a odhalených hrozeb a rizik auditované části informačního systému. Hlavním doporučením bylo odebrat uživatelům administrátorská práva k jejich stanicím. Druhým nejdůležitějším opatřením byla doporučená nastavení bezpečnostního software. Další doporučení zahrnovala nastavit operační systém pro blokování nepotřebných datových vstupů, blokování přidání nového hardware a zároveň odebrat oprávnění uživatelů spravovat hardwarová zařízení.

Podle ohodnocení uvedeného v práci by se podařilo snížit riziko vlivem hrozeb na požadovanou úroveň. Největší účinek navrhovaných opatření byl na snížení rizika vlivem hrozby škodlivého software, kdy se podařilo snížit velikost rizika z hodnoty 6,4 na hodnotu 2,8. To činí snížení rizika z původní úrovně přibližně o polovinu. Rizika vyplývající z hrozeb ze strany uživatelů, sociálních sítí a sociálního inženýrství by byla realizací doporučení snížena z původní úrovně přibližně o čtvrtinu. Nejmenší účinek doporučených nastavení by mělo na hrozbu mobilních zařízení, kde došlo ke snížení rizika přibližně o šestinu. Je to dáno tím, že audit byl vymezen na uživatelské stanice a opatření ošetřovala datovou výměnu mezi mobilními zařízeními a uživatelskými stanicemi. Pro další snížení hrozby by bylo nutné zavést fyzická opatření pro užívání mobilních komunikačních zařízení.

Původní náklady na odstranění škod způsobených hrozbami činil ročně přibližně 141 000 Kč. Navrhovanými opatřeními by se podařilo snížit náklady na ročně přibližně 22 000 Kč, což činí snížení nákladů o přibližně 85%. Největší absolutní úspory byly docíleny snížením počtu výskytů škodlivého software, a úniku informací způsobených uživatelem. Největší relativní úsporou pak bylo téměř eliminování nelegálního software na uživatelských stanicích.

Odhadnuté náklady na zavedení navržených opatření do praxe činily 5 250 Kč. Roční úspory by tyto náklady bohatě pokryly. Do částky však nejsou zohledněny náklady na ušlé zisky, které by vznikly, pokud by bylo zavedení opatření prováděno za plného provozu podniku. Vytvořit konkrétní plán realizace doporučení ale nebylo cílem auditu.

8. Seznam použitých zdrojů

1. **SVATÁ, VLASTA.** *Audit informačního systému.* Praha : Oeconomia, 2005. str. 168. ISBN 978-80-245-0975-4.
2. **BASU, S. K.** *Auditing Principles and Techniques.* Delhi : Dorling Kindersley Pvt. Ltd, 2006. str. 616. ISBN 81-7758-178-3.
3. **PATHAK, JAGDISH.** *Information Technology Auditing.* Windsor : Springer-Verlag Berlin Heidelberg, 2005. str. 209. ISBN 978-3-540-22155-5.
4. **PIATTINI, MARIO.** *Auditing information systems.* London : Idea Group Publishing, 2000. str. 246. ISBN: 978-1-8782-8975-9.
5. **POUR, J. - VOŘÍŠEK, J.** *Audit informačních systémů nebo penetrační testy?* Praha : Vysoká Škola Ekonomická, 2007. stránky 86 – 92. ISBN 978-80-245-1373-7.
6. **VAN GREMBERGEN, WIM - DE HAES, STEVEN.** *Enterprise Governance of Information Technology.* New York : Springer, 2009. str. 218. ISBN 978-0-387-84881-5.
7. **CHAMBERS, ANDREW - RAND, GRAHAM.** *Operational Auditing Handbook: Auditing Business and IT Processes.* Chichester : John Wiley and Sons, 2010. str. 900. ISBN 978-0-470-74476-5.
8. **SCAMBRAY, JOEL.** *Hacking Exposed Windows.* New York : McGraw-Hill Education, 2008. str. 451. ISBN 978-0-07-149426-7.
9. **TIPTON, HAROLD F. - KRAUSE, MICKI.** *Information Security MAnagement Handbook.* Boca Raton : CRC Press, 2008. str. 436. ISBN 978-1-4200-6708-8.
10. **DUBE, D. P. - GULATI, V. P.** *Information system audit and assurance.* New Delhi : Tata McGraw-Hill Education, 2005. str. 671. ISBN 978-0-07-055869-0.
11. Threat Risk Modelling. *OWASP.* [Online] [Citace: 29. 01 2011.] http://www.owasp.org/index.php/Threat_Risk_Modeling.
12. **VACCA, JOHN R.** *Computer and information security handbook.* Burlington : Morgan Kaufmann, 2009. str. 844. ISBN 978-0-12-374354-1.
13. **HEROLD, REBECCA.** *Managing an Information Security and Privacy Awareness and Training Program.* Boca Raton : CRC Press, 2010. str. 538. ISBN 978-1-4398-1050-7.
14. **SENFT, SANDRA - GALLEGOS, FREDERICK.** *Information technology control and audit.* Boca Raton : CRC Press, 2008. str. 768. ISBN 978-1-4200-6550-3.
15. **PICKETT, SPENCER K. H. - PICKETT, JENNIFER M.** *The Internal Auditing Handbook.* Wiltshire : John Wiley and Sons, 2010. str. 1088. 978-0-470-51871-7.
16. **WHITMAN, MICHAEL E. - MATTORD, HERBERT J.** *Principles of Information Security.* Boston : Course Technology, 2009. str. 599. ISBN 978-1-4239-0177-8.
17. Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary. *IT Governance.* [Online] 25. 10 2005. [Citace: 6. 10 2010.] http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf.
18. ČSN ISO/IEC 17799. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.* 2006.
19. ČSN ISO/IEC TR 13335-1,2,3. *Informační technologie - Směrnice pro řízení bezpečnosti.* 2000.
20. **VANSTAPEL, FRANKI.** INTOSAI. *http://www.intosai.org/.* [Online] prosinec 2004. [Citace: 16. leden 2011.] http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf.

9. Přílohy

Příloha 1

Výsledky dotazování na znalosti uživatelů v oblasti bezpečnosti informací.

Vysvětlivky:

Otázky:

A Při práci s počítačem je dovoleno
1. pít z hrnku i z lahve
2. pít pouze z lahve
3. není dovoleno pít

B Myš, klávesnice a monitory je dovoleno
1. odpojovat podle potřeby
2. odpojit, pokud je na to upozorněn nadřízený
3. není dovoleno odpojovat

C Do počítače je dovoleno stahovat soukromá data prostřednictvím
1. hardwarového média i internetu
2. pouze prostřednictvím internetu
3. není dovoleno

D V pracovním prostoru je dovoleno použití mobilního telefonu k
1. pořízení zvukového i obrazového záznamu
2. vyřízení soukromého hovoru
3. není dovoleno používat mobilní telefon

E Pokud si zaměstnanec IT oddělení vyžádá heslo uživatelského účtu, heslo mu
1. nesdělím
2. sdělím

F Pracovní stanici je povinnost uzamknout, pokud se její uživatel vzdálí na
1. méně než 5 minut
2. 5 - 10 minut
3. 10 a více minut
4. není povinnost uzamknout

Tabulka:

	A	B	C	D	E	F
1	2	3	3	2	2	1
2	3	3	2	2	2	1
3	2	1	2	1	1	3
4	1	1	2	1	2	4
5	2	3	2	2	2	1
6	3	2	3	2	2	3
7	3	2	2	1	2	2
8	3	3	3	2	2	1
9	2	3	1	2	2	2
10	3	3	2	3	2	1
11	3	3	2	3	2	1
12	2	3	3	3	2	1
13	2	2	3	2	2	2
14	2	3	2	1	1	2
15	3	3	2	2	2	2
16	1	1	2	2	1	4
17	3	3	2	2	2	2
18	1	1	1	1	2	4
19	3	2	2	3	1	3
20	3	3	2	3	2	1
21	2	2	3	2	1	2
22	2	1	2	1	2	3
23	3	3	3	3	2	1
24	3	3	2	1	1	3
25	1	2	3	1	2	3
26	3	3	3	1	1	1
27	2	3	2	1	1	1
28	2	3	1	3	1	2
29	3	3	3	1	2	3
30	3	3	3	2	2	2
31	2	1	1	1	1	4
32	2	2	3	1	1	3
33	1	2	2	1	2	3
34	3	3	2	2	1	1
35	3	3	1	2	2	3
36	1	3	3	3	1	1
37	2	3	2	2	2	3
38	1	1	2	2	2	3

Příloha 2

Seznam tabulek:

Příloha 3

Seznam obrázků: