Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Bezpečnostní prověrka IT zabezpečení finanční organizace

Bc. Filip Honč

! ! !

Místo této strany vložíte zadání diplomové práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnostní prověrka IT zabezpečení finanční 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 2.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval RNDr. Dagmar Brechlerové, Ph.D. za odborné vedení a cenné připomínky při zpracovávání této práce.

Bezpečnostní prověrka IT zabezpečení finanční organizace

Information Technology Audit of Financial Organization

Souhrn

Tato diplomová práce se zabývá tématem bezpečnosti IT, které je velice aktuální a váže se s pojmy audit nebo systém řízení bezpečnosti informací. V teoretické části je nastíněna teorie auditu a s ním souvisejících procesů, jehož výsledky a analýzy pomáhají vedení sledované organizace efektivně zacílit a odstranit nalezené nedostatky. Praktická část se věnuje otázce možností bezpečnostních testů prověřujících ochranu cílových systémů ve vybrané konkrétní instituci.

Cílem práce je prověření a kritické zhodnocení stavu IT bezpečnosti ve vybrané finanční instituci nebankovního sektoru a vytvoření návrhu změn pro zlepšení jejího stavu, a zároveň představení hlavních metod a postupů, jak hodnotit stav IT zabezpečení, a zásad podle kterých by se mělo firemní IT řídit.

Summary

The thesis deals with IT security, which is quite a topical issue that is linked with concepts as audit or data security management system. In its theoretical part the conception of audit and connected processes are outlined. Their results and analyses help the management of the audited company to target effectively on the deficiencies found and eliminate them. The practical part deals with the issue of security tests examining the protection of target systems in a chosen existing institution.

The objective of the work is to critically evaluate and examine the state of IT security in a chosen financial institution from a non-bank sector and to develop draft modifications to improve its state. At the same time, the thesis aims to introducing basic

methods and procedures to evaluate the state of IT security and principles the company IT should respect.

Klíčová slova:

Bezpečnost IT, bezpečnostní audit, bezpečnost finanční organizace, bezpečnostní prověrka, penetrační testy, řízení bezpečnosti informací

Keywords:

IT security, security audit, security of financial organisation, security clearance, penetration testing, information security management

Obsah:

Seznam grafik:

1 Úvod

Bezpečnost informatiky a jejích systémů, to je téma, které poslední léta hýbe světem IT. Vzhledem k narůstající internetové kriminalitě je to velmi aktuální a bolestivé téma. Dle odhadu FBI je v USA průměrná škoda po útoku hackerů s cílem ukrást peníze z velkých společností cca 1 milion USD a počet nahlášených skutků je pouze cca 10% z důvodu obavy o negativní dopad zveřejnění této události v tisku a na veřejnosti. Ale jsou na to u nás jednotlivé firmy připraveny? Věnují se firmy svojí IT bezpečnosti opravdu důkladně a zodpovědně?

*[**4**, s.22]*

Diplomová práce se zabývá bezpečnostní prověrkou IT zabezpečení ve smyslu auditu informačních systémů a technologií. Audit IT jako takový je poměrně mladá a rychle se rozvíjející disciplína. O přínosu auditu IT ve velkých podnicích již není pochyb, otázky vyvolává pouze kvalita provedeného auditu. V této práci se proto věnuji možnostem auditu IS/IT v menším podniku ve spojení s testy bezpečnosti řízení informací.

Představím základní techniky a koncepce řízení IT oddělení a pokusím se je aplikovat na zkoumaný podnik. V průběhu studia norem a standardů jsem dospěl k závěru, že většina norem a standardů je vytvořena pro využití ve velkých společnostech, a proto bude zajímavé, jak lze aplikovat zvolené metodiky při řešení auditu IT ve společnosti menší, případně střední.

Motto:

Bezpečnost je tak účinná, jak je silný její nejslabší článek.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem mé práce je zjistit současný stav bezpečnosti informačního systému v menším finančním podniku v nebankovní sféře. V současnosti je kritizována u menších podniků nedostatečná IT bezpečnost, což vede k přeorientování útočníků (hackerů) v posledních letech na malé a střední firmy. Jako základ pro srovnání bezpečnosti použiji standardy a metodiky pro auditování IS/IT.

Dále mám za cíl zjistit, jaké mají tyto podniky protiopatření proti útoku zvenčí i zevnitř sítě a vyzkoušet testovací útoky na průnik do vnitřní sítě z internetu, případně ohrozit stabilitu webových služeb.

Na základě těchto dat chci provést analýzu rizik a porovnat s očekáváním nižší úrovně zabezpečení. V poslední části je mým cílem vytvořit návrh na zlepšení stavu zabezpečení s konkrétním doporučením a výběrem technik nebo produktů, které jsou v současnosti na trhu nebo v souladu s mezinárodními normami.

Tato práce nemá za cíl do nejmenších podrobností rozebrat teorii auditu a samotný průběh, ale praktická část se věnuje otázce skutečných testů na zjištění ochrany cílových systémů. Jedním z dalších cílů je vytvořit komplexní přehled metod a nástrojů, jak by se mělo moderní IT řídit. Dále se hledá odpověď na otázku, jestli má smysl provádět na menších firmách kompletní audit IS/IT dle mezinárodních standardů. Celkově je práce na pomezí dvou větších informatických celků a těmi jsou audit IS/IT a řízení bezpečnosti informací.

2.2 Metodika

Analýza skutečného prostředí podniku, sběrem informací na místě a pomocí dotazování na vedoucího IT oddělení. Dalším krokem je vypracování analýzy rizik a SWOT analýzy. Pomocí dostupných zdrojů určit vhodné testování cílového podniku na základě metodik nebo jejich kombinací.

2.2.1 Audit IS/IT a systém pro řízení bezpečnosti informací

Předpokladem kvalitního auditu je využití existující metodiky, případně standardu, či normy, proto provedu porovnání nejznámějších metodik auditu, což jsou ITIL a COBIT. Následně provedu z pohledu zvolené metodiky hodnocení stavu IT v menším podniku. V další části diplomové práce popíšu návrh změn s cílem uzpůsobit fungování IT oddělení v souladu s moderním řízením IT a postup, jak zapracovat systém řízení bezpečnosti informací ISMS.

2.2.2 Penetrační testy

Největší důraz věnuji penetračním testům, které jsou metodou pro hodnocení počítačového a síťového zabezpečení. Jedná se o simulaci útoku na systém zevnitř nebo zvenčí. Jediným rozdílem oproti skutečnému útoku je, že nemá za cíl nějakým způsobem poškodit cílový subjekt, ale pouze zjistit nedostatky vycházející z chybného nastavení systému, případně chybějících bezpečnostních komponent. Vychází ze známých softwarových a hardwarových nedostatků. Analýza je provedena z pohledu potencionálních útočníků.

3 Teorie auditu a řízení bezpečnosti informací

3.1 Pojem audit

*Zpracováno podle [**1**, s.9-28]*

Audit ve zjednodušené podobě lze chápat jako „hloubkovou kontrolu či kritickou analýzu. Tento pojem má kořeny již v období starověkého Říma, historie auditorské činnosti je tedy ve společnosti zakotvena už v dávné historii.

Audit jakožto výraz pochází z latinského slova odvozeného od slovesa „naslouchat, poslouchat“. Primitivní formy auditu nad stavem dobytka se realizovala již ve starém Egyptě a Babylonu. Je však vhodné uvést, že historie zná pouze audit typu finančního či účetního. Nutno dodat, že problematika dalších typů auditů je o dost novější a jejich historie sahá pouze do 20. století.

Americký Institute of Certified Public Accountants pro změnu definuje audit jako „systematický proces získávání a vyhodnocování důkazů, týkajících se informací o činnostech a událostech, s cílem zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a sdělit výsledky zainteresovaným zájemcům.“

Dá se říci, že audit je systematický a dokumentovaný proces, který se snaží dokázat, zda provádíme činnosti správným způsobem.

3.1.1 Důvod vzniku

Důvodem vzniku auditu vůbec je, že lidé, kteří dostávají informace o výsledcích firem, či oddělení v rámci jednoho podniku, jim nedůvěřují a audity je mají zbavit pochybností.

Existují dva hlavní důvody, proč se nadále rozvíjí audit jakožto disciplína, a tím je obava z:

1) podvodu,

2) neúmyslné chyby.

Z toho plyne, že důvodem vzniku kontrolních opatření již v počátcích disciplíny auditu byla nedůvěra v čest lidí, prezentující nějaké výsledky. Toto doprovází společnost až do dneška, důsledkem je rozvoj disciplíny auditu, kde kontrolován není pouze auditovaný subjekt, ale důraz je kladen také na morální kvality, nezávislost a bezúhonnost osoby auditora.

Již v době průmyslové revoluce začaly vznikat první společnosti registrované státem, což vedlo ke vzniku zákonů předepisujících zhotovení přehledů o hospodaření společností pro své vlastníky - akcionáře. V porovnání se současností však pro tehdejší audit neexistovala žádná omezení, zajišťující objektivitu auditu. Jediným požadavkem bylo, že auditoři provádějící kontrolu nesměli mít v auditované společnosti žádnou výkonnou funkci. Hlavním cílem takového auditu bylo porovnání výsledků ve výroční zprávě s položkami v účetních knihách a prověření, že jsou všechny údaje správné a dokladovatelné.

V současnosti se audit jako takový rozdělil na mnoho odnoží, z nichž je pro nás nejzajímavější audit informačního systému, z něhož se stala inženýrská disciplína. Původní asociace EDP se přetransformovala do organizace ISACA (Information Systems Audit and Control Association). Tato organizace dnes zaujímá místo největší mezinárodní organizaci sdružující auditory informačních systémů.

3.1.2 Význam a účel

Jak už ze samotné definice plyne, význam auditu spočívá v porovnání reálného stavu a stavu požadovaného. Účel auditu je v základu vždy zjištění současného stavu, ve kterém se auditovaný subjekt nachází. Dalším smyslem pak může být i optimalizace podnikových procesů v případě, že hlavním cílem prováděného auditu je pouze zjištění aktuálního stavu.

Cílem auditu může být například:

1) informovat management,
2) motivace pro odstranění nedostatků.
3) zdůraznit dodržování vnitřních standardů,

Bohužel se často audit provádí až v okamžiku, kdy si již firma uvědomuje existenci problémů a tyto problémy jsou natolik závažné, že ohrožují její další činnost. Což v souvislosti s bezpečností IT platí dvojnásob.

Výsledkem auditu je auditorská zpráva, což je formální písemný dokument pro management. Pro auditorskou zprávu existují různé standardy, ale ty ošetřují pouze základní náležitosti zprávy, vlastní obsah pak záleží na auditovaném objektu. Standard organizace ISACA o auditorské zprávě říká: „Závěrečná zpráva musí obsahovat aktuální a objektivní obraz situace, umožňuje managementu uskutečnit potřebná opatření. Management používá tuto zprávu jako základ přesných, spolehlivých a vhodných informací, na jejichž základě lze učinit informované rozhodnutí. Management si také uvědomuje, že jeho efektivnost je měřena externími pozorovateli, kteří mohou použít

auditorskou zprávu jako východisko pro investiční či regulační rozhodnutí, pokud bude zpráva zveřejněna, či je její zveřejnění požadováno zákonem.“.

3.1.3 Osoba auditora

Osoba auditora by měla splňovat podobu člověka znalého příslušných standardů i vybaveného praktickými zkušenostmi, díky nimž může zmíněné pochybnosti vyvrátit či zcela odbourat.

Vzhledem k celkové odlišnosti mezi jednotlivými typy auditů je prakticky nemyslitelné, aby jeden auditor odpovědně ovládal více než jeden z typů auditu. Proto vznikají specialisté na jednotlivá odvětví.

Základním předpokladem pro auditora je výborná znalost oblasti, na kterou se specializuje. A, což je pro oblast IT nejdůležitější – auditor musí znát a sledovat všechny trendy vývoje odvětví i ve vztahu k místně příslušné legislativě.

3.1.4 Specifika auditu IS/IT

Na počátku auditu IS se auditor zaměřoval na hodnocení procesů, jež proběhly v minulosti. Ale v posledních dvou dekádách se audit IS/IT již chápe jako zcela samostatná disciplína a jako vynikající preventivní nástroj zvyšování kvality a obzvláště bezpečnosti informačních systémů.

Přestože význam auditu IS v České republice podobně jako ve světě stále roste, stále zůstává velké množství i velkých společností bez jakékoliv systematické kontroly natož auditu, čímž se vystavují potencionálním hrozbám. Nicméně především v nadnárodních společnostech a bankách se postupně zřizují funkce vnitřních auditorů. Z těchto vnitřních auditorů se pak se v rámci útvarů oddělují auditoři IS. Vzhledem k obrovské závislosti těchto organizací na informačních systémech bude postupem času audit IS/IT běžnou součástí fungování útvaru IT.

3.1.5 Typy auditu IS

Audit IS lze dělit podle různých hledisek, jimiž lze ke konkrétnímu auditu přistupovat. Základní hlediska uvádí následující tabulka:

Hledisko:	**Typ auditu:**
Věcné zaměření auditu	– legálnosti programového vybavení – bezpečnosti – kontrolního systému – operační audit (audit efektivnosti provozu) – audit projektu nového sytému
Úroveň auditu	– programového vybavení – systémového SW – databázového SW

Obrázek 1 – typy auditu podle hledisek – „autor“ podle [1, s.22-24]

3.2 Koncepce řízení informatiky

*Zpracováno podle [**3**, s.22]*

V současnosti jsou populární zejména dvě rozdílné koncepce řízení informatiky. Těmito koncepcemi jsou IT Governance – jakožto nástupce Corporate Governance a dále koncepce označovaná jako IT Service management, jež se zaměřuje na nižší úroveň řízení IT a cílí především na poskytování kvalitních služeb.

3.2.1 IT Governance

IT Governance je nástupcem Corporate Governance, jejímž propagátorem byla OECD (Organizace pro ekonomickou spolupráci a rozvoj), základem bylo formulovat a rozvíjet právní a výkonné metody a postupy mezi organizací a akcionáři. Později

přepracována organizacemi ISACA a ITGI do formy Enterprise Governance, která jako hlavní přidává i souhrn odpovědností pro vedení podniků.

Aplikací myšlenek a principů Corporate a Enterprise Governance do IT vznikla nová forma – IT Governance, která se zabývá odpovědným řízením a chováním vlastníků a vedení organizací ve vztahu k informačním technologiím. Vytváří základní rámec pro rozhodování, jehož cílem je zajistit propojení informačních technologií s kulturou a strategií podniku.

Hlavními cíli IT Governance je transparentnost rizik organizací a ochrana hodnot vlastníků, což má za cíl i jiná oblast řízení informatiky, a to řízení bezpečnosti informací.

3.2.2 ITSM

ITSM, IT Service management, neboli v češtině řízení služeb informačních technologií je postup, jenž respektuje principy a praktiky pro návrh dodávku i správu IT služeb. Vše v kontextu odpovídající jakosti s podporou klíčových aktivit zákazníka. Nejedná se tedy o srovnatelného konkurenta IT Governance, ale spíše o protínající se množinu stejných principů, kde IT Governance je v mnohem širším pojetí, ale ITSM jde do větší hloubky. Hlavním cílem ITSM je tedy účelně a účinně realizovat cíle vytýčené řízením informatiky.

3.3 Metodiky řízení IT

V této podkapitole si představíme metodiky relevantní pro problematiku řízení IT. Provedeme srovnání jednotlivých metodik, analýzu vazeb mezi těmito metodikami a jejich stručný popis.

Bohužel standardy vztahující se jak k řízení IT, tak k auditu lze v původním znění stěží využít i v menších podnicích. Další problém tkví v tom, že menší podnik se v oblasti informatiky většinou oficiálně neřídí žádnou konkrétní normou, metodikou nebo standardem. Tuto situaci je pak třeba řešit úpravou metodik pro potřeby menšího podniku a možná nejlépe využít kombinací různých technik a standardů. Pro potřeby kontroly a auditu je možno využít:

1) odborné znalosti a zkušenosti auditora

2) kritéria dohodnutá se zadavatelem auditu

3) obecnější principy některé z uznávaných metodik pro řízení informatiky, jako například COBIT, ITIL, IT Governance, apod.

Zejména kombinace prvního a třetího bodu se mi zdá obzvláště výhodná.

*[**3**, s.48]*

3.3.1 ITIL

Information Technology Infrastructure Library (ITIL) tvoří souhrn prověřených konceptů a postupů, které popisují způsoby procesního řízení služeb a infrastruktury IT, jež jsou tímto způsobem poskytovány. Projekt vznikl ve Velké Británii v 80. letech 20. století, jakožto koncepce vládní agentury CCTA (Central Computer and Telecomunications Agency) a cílem tohoto konceptu bylo zlepšení IT služeb v centrálních britských úřadech. Celý koncept byl po roce 2001 přepracován britskou agenturou OGC (Office of Govermment Commerce) na novou verzi 2 (ITIL V2). Po tomto přepracování ji začaly využívat společnosti v mnoha zemích jako standard v poskytování IT služeb.

V roce 2007 po internetovém průzkumu u uživatelů ITIL vznikla nová verze 3 (ITIL V3). Zde proběhla zásadní redukce počtu knih této metodiky a podřízení celkové koncepce životnímu cyklu služeb IT.

V roce 2011 byla verze ITIL V3 naposledy změněna. Tato verze se značí jako ITIL 2011 Edition. Oproti původnímu vydání ITIL V3 z roku 2007 jsou změny spíše kosmetické - proběhlo především sjednocení osnovy všech 5 ústředních knih, a tím se zpřehlednily veškeré struktury procesů. Další změnou je, že se v ITILu nepoužívá označení V3.

Souhrnně se dá říct, že je to metodika založená na procesním řízení organizace a je určena hlavně pro střední a vyšší management. V kontextu s typy řízení informatiky se jedná se o rámec pro oblast ITSM (IT Service Management), vycházející z nejlepších

praktických zkušeností, ale zároveň ponechává velkou volnost při implementaci. ITIL je taktéž v současnosti nejrozšířenější metodikou pro v oblasti řízení IT služeb.

*[**3**, s.53]*

3.3.1.1 Charakteristika ITIL V3

ITIL v3 (a zároveň i 2011 edition) je nejnovější verzí metodiky ITIL. Celá metodika je položena na stejném základu jako verze starší, tedy na takzvaných nejlepších metodách - „best practice“. Oproti předchozí verzi se ale jádrem metodiky stává IT služba a její životní cyklus, přes vývoj, implementaci až po dodání. Knihovna metodiky ITIL je dělena do čtyř základních bloků.

První blok obsahuje tzv. síťově zaměřené produkty, jež mají za úkol podpořit jádro metodiky. Tento první blok pojednává o základních ITIL definicích, ale obsahuje i procesní mapy a příklady.

Druhý blok obsahuje to nejdůležitější, a to jádro metodiky, které obsahuje základní zásady, principy a nejlepší metody. Jádro je tvořeno těmito pěti knihami sledujícími model životního cyklu IT služby:

1) Service Strategy (strategické procesy)

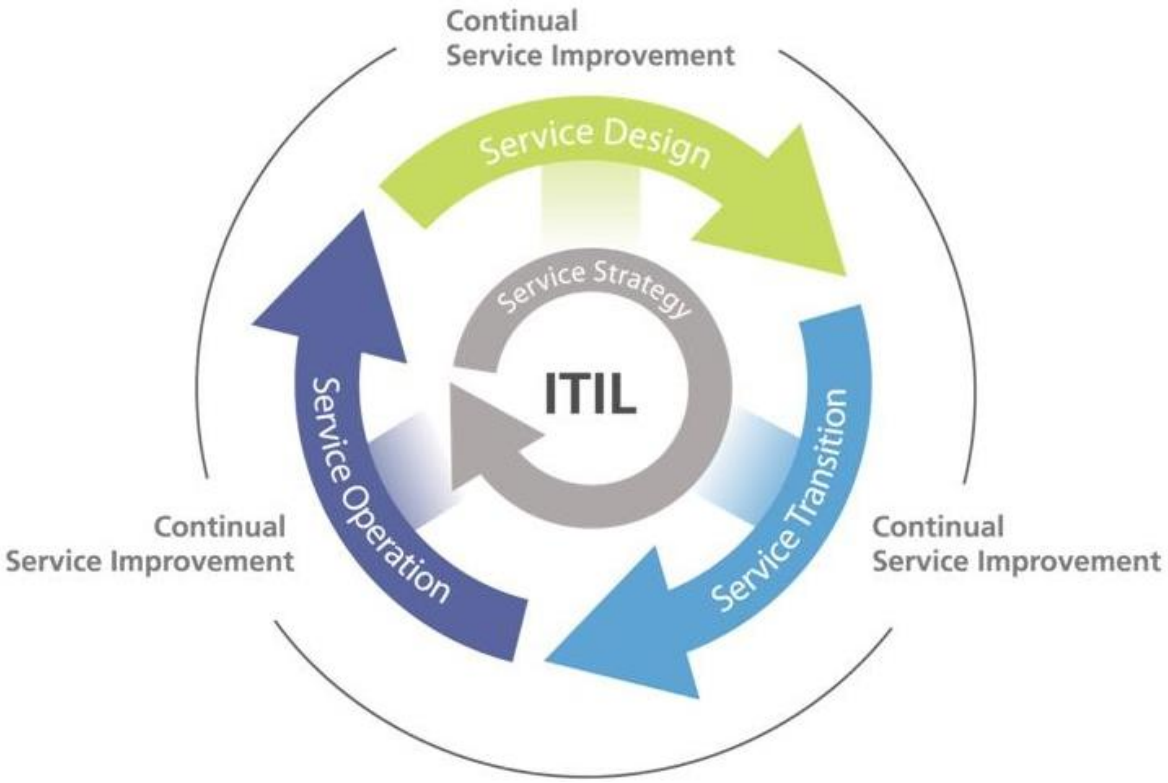
2) Service Design (návrh služeb)

3) Service Transition (uvedení služby do provozu)

4) Service Operation (provoz služeb)

5) Continual Service Improvement (neustálé zlepšování služeb)

Princip závislostí mezi těmito knihami jádra vyjadřuje následující obrázek:



Obrázek 2 – vizualizace ITIL – „http://www.alvao.cz/alvaocz/wp-content/uploads/2014/09/itil_cycle_20081030_180417.jpg“

Třetí a čtvrtý blok obsahuje publikace, odrážející aktuální vývoj a jednotlivé potřeby odvětví.

Jako poslední novinku ITIL v3 uvedu její těsné napojení na normu ISO/IEC 20000 – o tom ale až dále v práci.

3.3.2 COBIT

COBIT je zkratka anglické názvu „Control Objectives for Information and Related Technology“ a jedná se o metodologii řízení a hodnocení IT a souvisejících IS. Tato metodika je vydávána organizací ISACA, jež stála už u vzniku první verze COBIT v roce 1996. Obecně je potom tato metodika definovaná jako mezinárodně aplikovatelná a přijímaná metodika pro skloubení IT Governance a systému kontrol s obchodními cíli organizace.

Následující verze vznikají v letech 1998, 2000, 2007. Verzi z r. 2012 již vydává ITGI (IT Governance Institute). Tato poslední verze COBIT 5 přidává několik nových oblastí, ale základ zůstává v COBITu 4.1 z roku 2007. V následujícím textu bude popsán základ Cobitu 4.1a hlavní rozšíření verze 5.

Ve svých počátcích byl COBIT primárně určen jako nástroj k auditu IT. S dalšími verzemi přicházela nová rozšíření nad rámec auditu, jako třeba směrnice určené pro management (Management Guidelines). COBIT se tedy dostal do podvědomí odborné IT veřejnosti coby komplexní systém pro správu a řízení IT. Metodika je využívána pro nastavení a audit IT procesů ve větších společnostech.

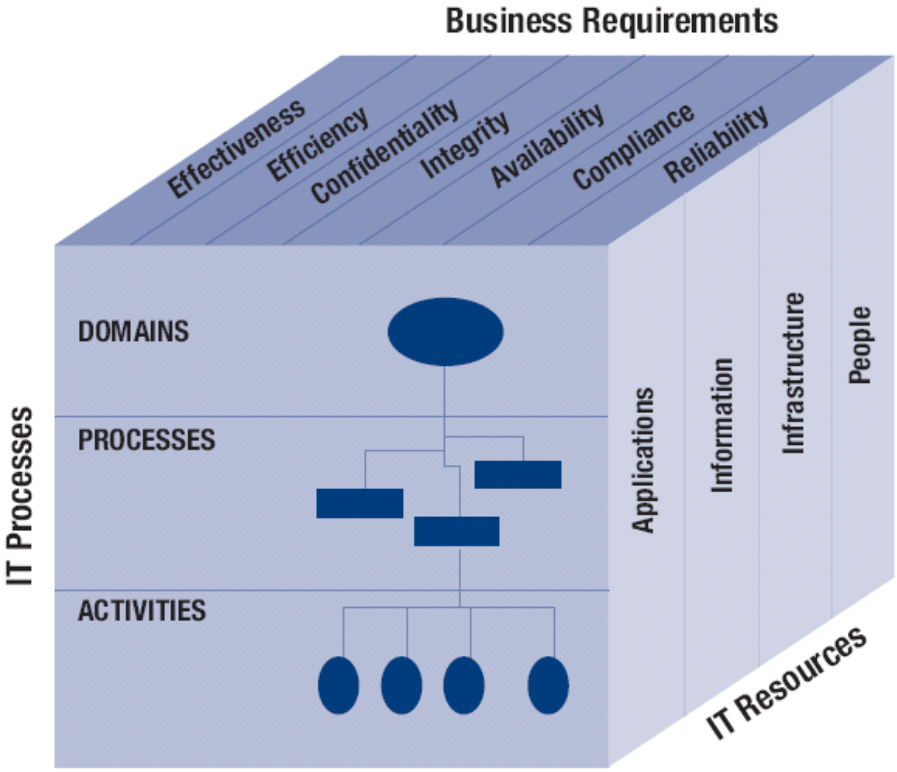
*[**3**, s.48]*

COBIT taktéž vychází ze základní koncepce IT Governance, odkud bere organizační strukturu a procesy informatiky. Metodika obsahuje pět základních myšlenek:

1) Cíle podnikové informatiky musí mít vazbu na cíle podniku.
2) Informatika musí vytvářet přidanou hodnotu.
3) Musí existovat systém řízení, který umožní minimalizovat rizika spojená s podnikovým IT.
4) Systém řízení musí zaručovat šetrné nakládání s IT zdroji.
5) Systém řízení informatiky by měl mít zabudován systém měření výkonnosti.

A právě těchto pět zásad lze využít při auditu IT i v menších podnicích, pakliže se se tam neinklinuje k jiné metodice či standardu. Z toho plyne, že podnik musí investovat, řídit a kontrolovat IT zdroje pomocí vhodně nastavených procesů tak, aby byly zajištěny požadované informace v odpovídající kvalitě. Dále z tohoto plyne, že nezbytnou součástí celého procesu je rovněž řízení rizika.

Další principy COBITu, tentokrát ve smyslu informačních kritérií, dokládá takzvaná kostka COBIT, na následujícím obrázku:



Obrázek 3 – kostka COBIT – „http://iea.wdfiles.com/local--files/cobit/COBIT_Cube.png“

Požadavky Informačních kritérií (Business Requirements) metody COBIT na informace jsou následující:

1) Efektivnost (Effectiveness)

2) Výkonnost (Efficiency)

3) Důvěrnost (Confidentiality) – zajistit ochranu důvěrných informací

4) Integrita (Integrity) - ve smyslu integrity dat

5) Dostupnost (Availability) – informace musí být k dispozici vždy, kdy je třeba

6) Shoda (Compliance) – ve smyslu shody s platnou legislativou

7) Hodnověrnost (Reliability) – spolehlivost dodávaných informací

*[**3**, s.49]*

Výše uvedená kritéria je opět možné využít jako při auditování IS/IT v menších podnicích podobně jako principy IT Governance uvedené dříve v této kapitole.

COBIT Quickstart 4.1

Pro potřeby menších podniků potom ITGI (IT Governance Institute, 2007) vydal zajímavou publikaci „COBIT Quickstart, second edition“, která vychází z COBIT verze 4.1. Tato publikace je určena pro menší až střední podniky. V zásadě jde o výběr nejdůležitějších komponent z kompletního COBITu.

Procesy COBITu jsou pak členěny do následujících čtyř domén:

1) **PO** - Plan and Organise - Plánování a organizace

2) **AI** - Acquire and Implement - Nákup a implementace

3) **DS** - Deliver and Support - Poskytování služeb a podpora

4) **ME** -Monitor and Evaluate - Monitoring a hodnocení

Plánování a organizace

Doména se zabývá strategickým a taktickým plánováním a zároveň řeší, jak využít IT k naplňování podnikatelských cílů organizace. To vše za předpokladu podpory dostatečné technologické infrastruktury.

Nákup a implementace

Doména udává, že k realizaci naplánované strategie je třeba identifikovat vhodné IT řešení. Toto řešení musí být následně vyvinuto (případně zakoupeno) a naimplementováno, tak aby umožňovalo podporu strategických procesů podniku.

Poskytování služeb a podpora

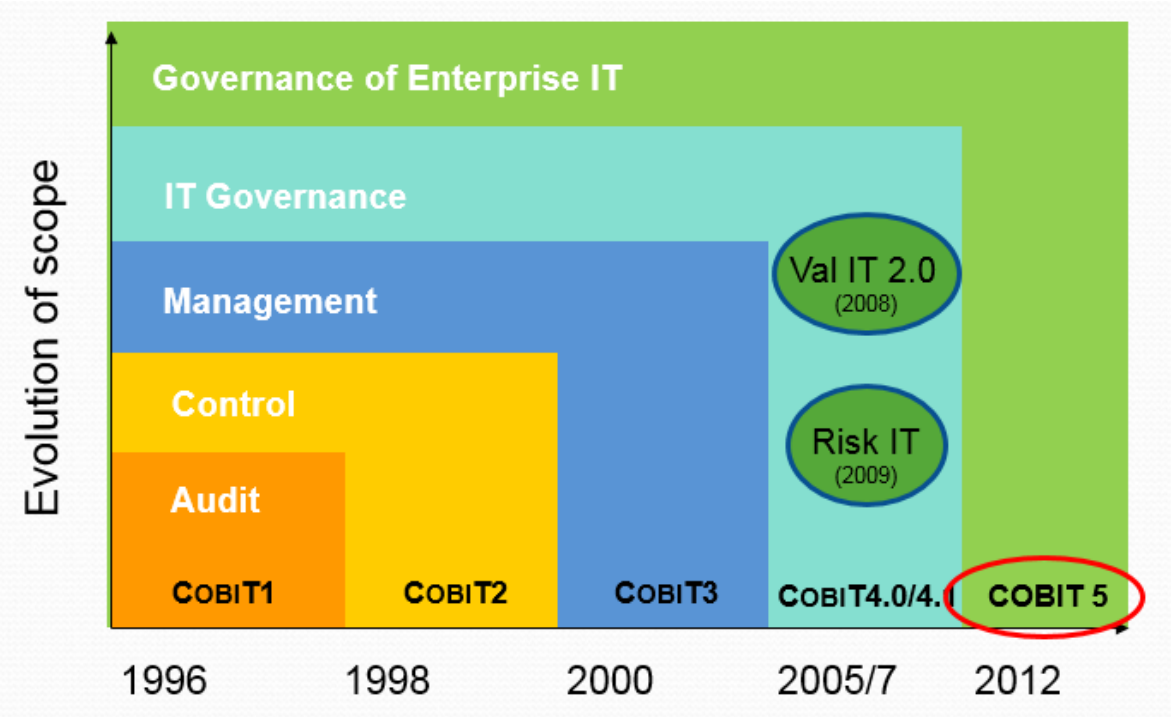
V této doméně se definují procesy spojené se zajištěním požadovaných služeb a řízením bezpečnosti aplikací, spolu s podporou a školením uživatelů.

Monitoring a hodnocení

Doména po každému IT procesu vyžaduje monitorovat vnitřní kvalitu a soulad s definovanými požadavky.

3.3.2.1 Změny přinášející COBIT 5

COBIT 5 ve svém důsledku přináší konsolidaci metodiky Cobit 4.1 s Val IT 2.0 a Risk IT frameworkem. Přičemž Val IT je dokument vydaný taktéž organizací ISACA, jako odpověď na poptávku po praktických nástrojích pro hodnocení, alokaci a identifikaci investic v oblasti IT. Risk IT oproti tomu představuje samostatnou oblast řízení rizik v rámci IT Governance. Tento dokument z roku 2009 má na svědomí organizace ITGI (IT Governance Institute) spadající opět pod organizaci ISACA. Dále také COBIT 5 čerpá například z dokumentu Business Model for Information Security a nebo IT Assurance Framework. Vývoj jednotlivých verzí COBITu můžeme vidět na následujícím obrázku:



Obrázek 4 – vývoj COBIT – „http://www.peratech.org/wp-content/uploads/2014/08/cobit_1.JPG1.png“

3.3.3 IT Assurance Guide

Tato součást COBITu se považuje za stěžejní dokument ohledně použití COBITu k auditu IS/IT. Je v něm pokryta fáze plánování, určení rozsahu auditu a také samotné ověřování. Detailněji rozděluje jednotlivé fáze auditu dokument IT Assurance Guide na:

1) Plánování (Planning)

2) Určení rozsahu (Scoping)

3) Realizaci (Execution)

Významnou část také představuje sekce "Process Assurance Steps", kde dokument poskytuje návody a doporučení na provádění jednotlivých kontrol. Pro tyto kontroly doporučuje vznik dokumentu s následujícími sekcemi:

1) Cíl kontroly

2) Hodnotové ukazatele

3) Ukazatele rizika

4) Test designu kontrol

5) Test výstupu kontrolních cílů

6) Dokumentace dopadu zjištěných slabin

Z uvedené struktury můžeme dedukovat, že auditování podniku, který se adaptoval podle metodiky COBIT, je značně jednodušší, jelikož se stačí držet COBITem poskytnutého návodu a není třeba vytvářet složitou strukturu dokumentů, jelikož ta již vytvořena je.

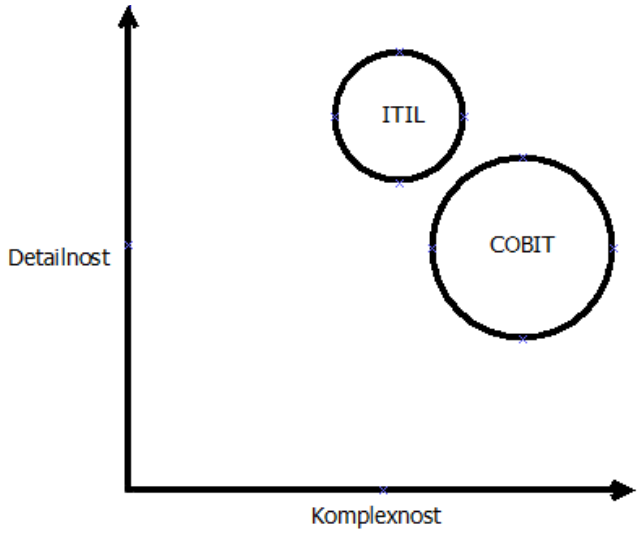
*[**1**, s.92]*

3.3.4 Srovnání ITIL a COBIT

Porovnání obou zmíněných metodik provedl Information Technology Governance Institute, který konstatoval, že ITIL je metodika mnohem podrobnější než COBIT, věnuje se ale podstatně užší oblasti IT/IS než právě COBIT. Nicméně lze konstatovat, že s každou novou verzí těchto metodik, dochází k vzájemnému sblížení i přesto, že si ponechávají svá specifika.

*[**2**, s.57]*

Porovnání metodik COBIT a ITIL je zobrazeno v grafu na následujícím obrázku a tabulce.



COBIT domény	ITIL (řeší x neřeší)
PO	Částečně
AI	Podrobněji
DS	Podrobněji
ME	Neřeší

Obrázek 5 – srovnání ITIL / COBIT – „Literatura 3, s58“

3.4 Legislativa a normy

*Zpracováno podle [**3**, s.161-199]*

Jedním z cílů této diplomové práce je i porovnání cílového podniku co do shody s legislativou a normami, proto je třeba se seznámit se základem v této oblasti. Různé organizace se snaží vytvořit standardy, návody a doporučení, které by audit pomohly formalizovat a objektivizovat. Z pohledu řízení bezpečnosti informací jsou tu zase zákony

s charakterem nařízení, které se musí dodržovat, a dále normy, které jsou doporučující, ale pokud chce organizace dosáhnout shody, tak jejich principy taktéž musí dodržovat.

3.4.1 Organizace vydávající IT standardy

Mezinárodní standardy týkající se IT jsou vydávány řadou mezinárodních profesních organizací. Mezi organizace, které se zabývají standardy informačních systémů ve větší míře, patří hlavně mezinárodní organizace ISO.

Tabulka nám osvětlí základní organizace vydávající standardy IT a normy:

Standardy	**Název dokumentů**
European Union	Direktiva EU
American National Standards Institute	ANSI
IEEE	IEEE
IETF	RFC
BSI - British Standards Institution	BS
Normy	
International Standards Organisation	ISO
CEN - Evropská komise pro normalizaci	EN / CEN
ISACA	Metodiky / normy
České instituce	
ÚNMZ - Úřad pro technickou normalizaci, metrologii a státní zkušebnictví	ČSN
Ministerstvo vnitra ČR	Metodické dokumenty

Organizace ISACA vydává standardy, které jsou závazné jak pro interní, tak i pro externí auditory – držitele titulu CISA (Certifikovaný auditor informačních systémů).

Pro zajímavost uvedu dva body etického kodexu auditora z české odnože ISACA CRC, které by se daly doporučit jako základ etického kodexu jakéhokoliv IT oddělení:

ISACA® stanovuje tento Etický kodex, který poskytuje návod pro profesionální a osobní jednání členů asociace a držitelů certifikátů CISA®, CISM®, CRISC® a CGEIT®

Členové ISACA a držitelé těchto certifikátů musí:

- *Sloužit v zájmu vlastníků společnosti, legálním a čestným způsobem, dodržovat vysoké standardy chování a neúčastnit se žádných činností, které by diskreditovaly profesi.*
- *Udržovat důvěrnost a utajení informací získaných při plnění povinností, pokud jejich poskytnutí nebude vyžadováno oprávněnými orgány. Takto získané informace nesmí být použity pro osobní prospěch nebo poskytnuty nepatřičným subjektům.*

*[Lit **9**]*

3.4.2 Legislativa ČR a EU

Na úrovni Evropské unie je problematika související s auditem a IT bezpečností upravována prostřednictvím direktiv a směrnic. Tyto direktivy potom vytvářejí základní rámec, který by měly do své legislativy implementovat členské státy, tedy včetně ČR. Sbližování legislativy ČR a EU se pak nazývá harmonizací.

Vybral jsem několik nejzásadnějších zákonů a ve zkratce je popíši s tím, že ten nejaktuálnější dostane samostatnou podkapitolu.

Zákon č. 101/2000 Sb. – o ochraně osobních údajů

Zákon je v souladu se směrnicí EU – směrnice Evropského parlamentu a Rady 95/46/ES z roku 1995. Smyslem zákona je ochrana osobních údajů zaručené Listinou základních práv a svobod, kde je zaručeno právo na neoprávněné zasahování do soukromého života zveřejněním nebo jiným zneužitím osobních údajů. Dále jsou zde vymezeny termíny z hlediska ochrany dat na osobní údaje, citlivé údaje a anonymní údaje. Ustanovuje především uchovávání a likvidaci osobních dat a celkově nutnost kodifikace způsobu jejich zpracování. Zpracovatel musí mít popsány procesy pro opatření personální bezpečnosti, způsob zabezpečení objektu a místností a zabezpečení automatizovaného zpracování (přístupová práva, antivirová ochrana, kryptografická ochrana). Vše musí být v souladu s následujícím zákonem č. 412/2005 Sb.

Zákon č. 412/2005 Sb. – o ochraně utajovaných informací a bezpečnostní způsobilosti

Zákon upravuje zásady pro stanovení informací jako utajovaných informací, podmínky přístupu k nim a požadavky na ochranu. Vymezuje pojmy, jako je utajovaná informace, stupně utajení, zajištění informační ochrany a kryptografické bezpečnosti. Definuje náležitosti bezpečnostních informačních systémů a požadavky na jejich certifikaci.

Zákon č. 227/2000 Sb. – o elektronickém podpisu

Zákon vymezuje pojmy, jako je elektronický podpis, zaručený elektronický podpis, datová schránka, certifikát, elektronická značka a časové razítko. V zásadě definuje požadavky na podpis a určuje prostředky pro bezpečné vytváření a ověřování elektronického podpisu. Tento zákon se vztahuje na všechny právnické osoby (což jsou veškeré podniky).

Zákon č. 365/2000 Sb. – o informačních systémech veřejné správy

Zákon stanovuje práva a povinnosti související s celým cyklem informačních systémů veřejné zprávy. Vymezuje pojmy jako informační systém, datový prvek nebo bezpečné rozhraní informačního systému. Zákon je tedy významný přímo pro systémy veřejné správy.

3.4.2.1 Zákon o kybernetické bezpečnosti

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

Tento zákon je v současnosti úplnou novinkou, vstoupil v platnost 1. 1. 2015 a přináší výrazné změny pro různé provozovatele IS a to nejen veřejné správy.

Úvodní ustanovení:

§1
Předmět úpravy

(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

(2) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

§2
V tomto zákoně se rozumí

a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací,

b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,

§3

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací1), pokud není orgánem nebo osobou podle písmene b)

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury a

e) správce významného informačního systému

[Lit 7]

Zákon dále specifikuje významný IS, významnou síť a hlavně bezpečnostní opatření, která jsou pak rozvedena ve **vyhlášce č. 316/2014 Sb. Vyhláška č. 317/2014 Sb.** pak specifikuje kritéria, podle nichž se určí, který systém do těchto kategorií spadá. Tento zákon je primárně zaměřen na zvýšení bezpečnosti kritické infrastruktury státu a významných informačních systémů.

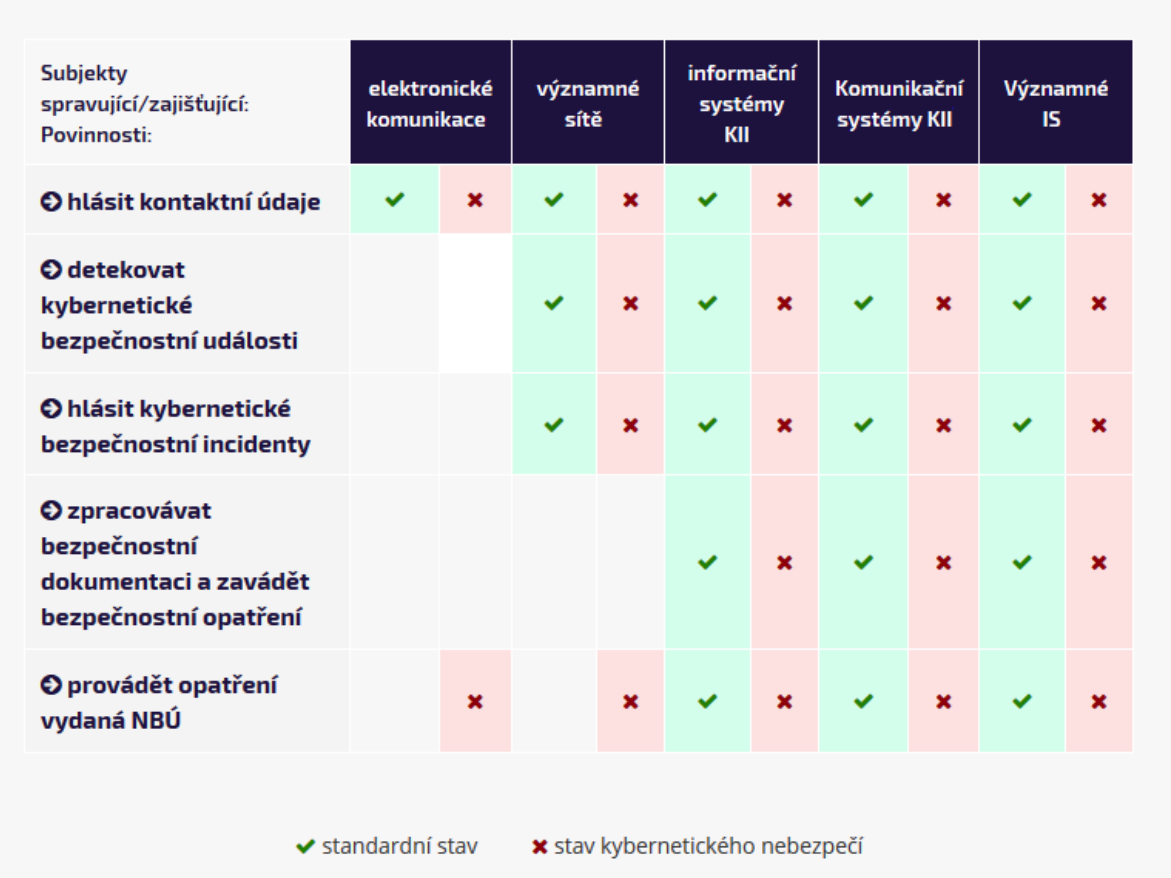
Smysl nových pravidel je předcházení závažným bezpečnostním hrozbám a jejich řešení v reálném čase. Dohled nad kybernetickou bezpečností je svěřen Národnímu bezpečnostnímu úřadu a Národnímu centru kybernetické bezpečnosti. V případě, že dojde k bezpečnostnímu incidentu, může NBÚ nově vydat ochranné opatření nebo vyhlásit stav kybernetického nebezpečí.

Celý zákon je postaven na systému řízení bezpečnosti informací podle norem ISO/IEC řady 27000. Proto podniky, které tyto normy respektují, respektive je mají

implementovány, jsou z pohledu zákona připraveny, ale musí zavést nové role a způsob hlášení incidentů.

Souhrn povinností jednotlivých subjektů ukazuje následující obrázek:

*[Lit **8**]*



Obrázek 6 – povinnosti podle Kybernetického zákona - „http://www.kybernetickyzakon.cz/“

3.4.3 Normy

*Zpracováno podle [**1**, s.51]*

V této kapitole bude představeno několik základních norem, které mají zásadní vliv na řízení IT a souvisejících oblastí.

3.4.3.1 Řada ISO 9000

Tato řada norem se netýká přímo IT, ale představuje vznik systému řízení kvality, který má svůj původ v první polovině 20. století. Norma stanovuje jednoduchou zásadu, aby vedení firmy stanovilo své cíle a plány v oblasti kvality produkce. Specifikuje požadavky na systémy řízení kvality ve společnostech, které chtějí prokázat svou schopnost dlouhodobě poskytovat produkty, jež vyhovující technickým i legislativním předpisům a zároveň odpovídající rostoucím požadavkům zákazníků.

Příkladem je převzatá norma **ČSN EN ISO 9001 „Systémy managementu kvality – Požadavky“**

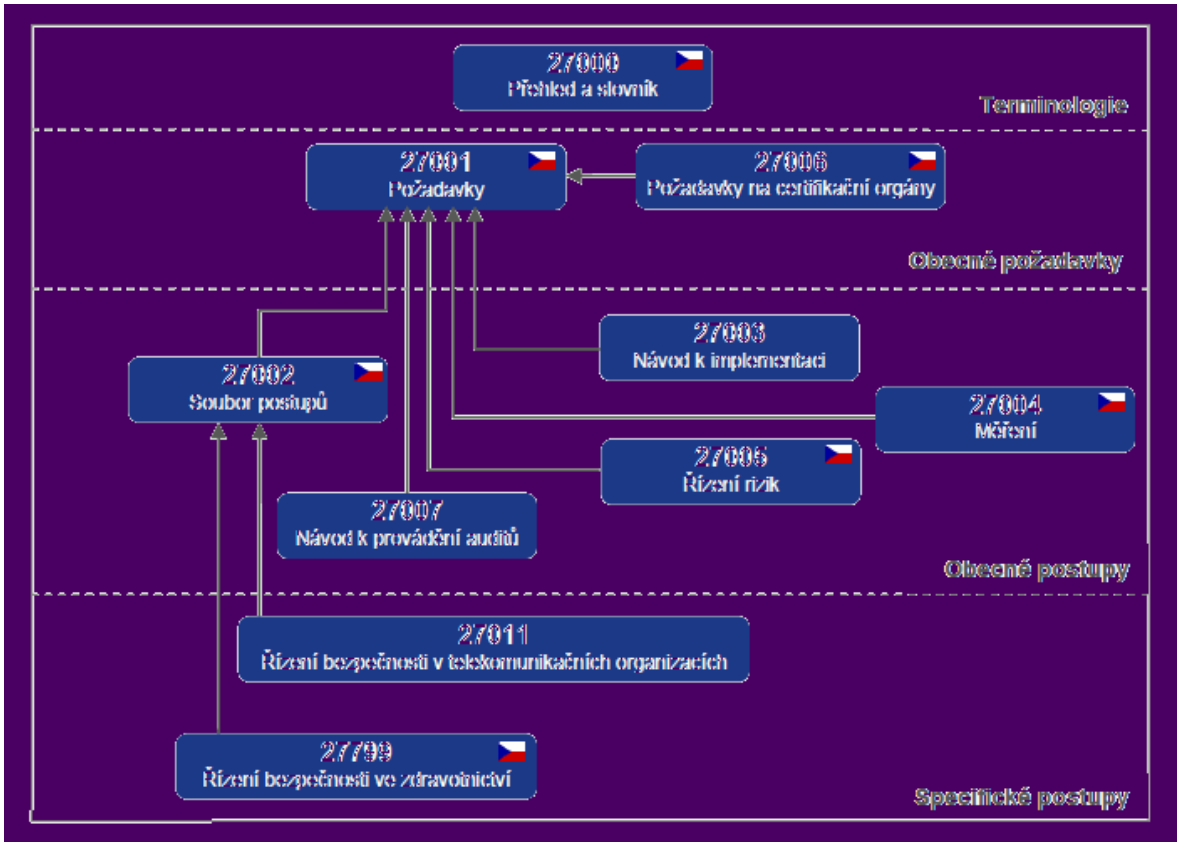
Norma slouží jako základ pro certifikaci systémů řízení kvality v jednotlivých podnicích, či jejich částech.

3.4.3.2 Řada ISO/IEC 27000

Za tyto normy, jež jsou v současnosti v popředí zájmu, zodpovídá organizace ISO, konkrétně její subkomise ISO/IEC/JTC1/SC27 – IT Bezpečnostní techniky. Tato řada norem vychází z požadavku na sjednocení norem řešící problematiku řízení bezpečnosti informací.

ČSN ISO/IEC 27001 “Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky” poskytuje model, jak zavést a spravovat efektivní systém řízení bezpečnosti informací. Stanovuje jednoznačné požadavky na systém řízení a kontrolu zavedení ISMS (Information Security Management Systém). V rámci přístupu k vývoji a zdokonalování systému řízení bezpečnosti informací v organizaci norma používá model PDCA (více v následující kapitole). ISO/IEC 27001 plně staví na principech z ISO 9001 a je i v souladu s dokumenty OECD z roku 2002. Poslední revize byla vydána v říjnu 2013

Systém norem zobrazuje následující obrázek:



Obrázek 7 – struktura norem ISO 27000 – „http://www.qcom.cz/home/cesky/systemy_rizeni/isms/struktura_27k.gif“

3.4.3.3 ISO/IEC 20000

Tato norma v sobě kombinuje doporučení z metodiky ITIL, což původně shrnula britská norma BS 15000 v roce 2000, ze které pak byla následně odvozena tato mezinárodní norma

ČSN ISO/ IEC 20000 „Informační technologie – Management služeb“.

Norma zavádí princip identifikace procesů, podporujících kvalitní poskytování IT služeb. Dále zavádí princip interních auditů pro získání zpětné vazby a neustálého zlepšování úrovně IT služeb. Norma v sobě dále kombinuje normy ISO 9001 pro systém řízení kvality a ISO 27001 pro bezpečnost informací. Což znamená, že je v podstatě shrnutím všech předchozích doporučení pro efektivní řízení prostřednictvím IT.

3.4.3.4 Certifikace

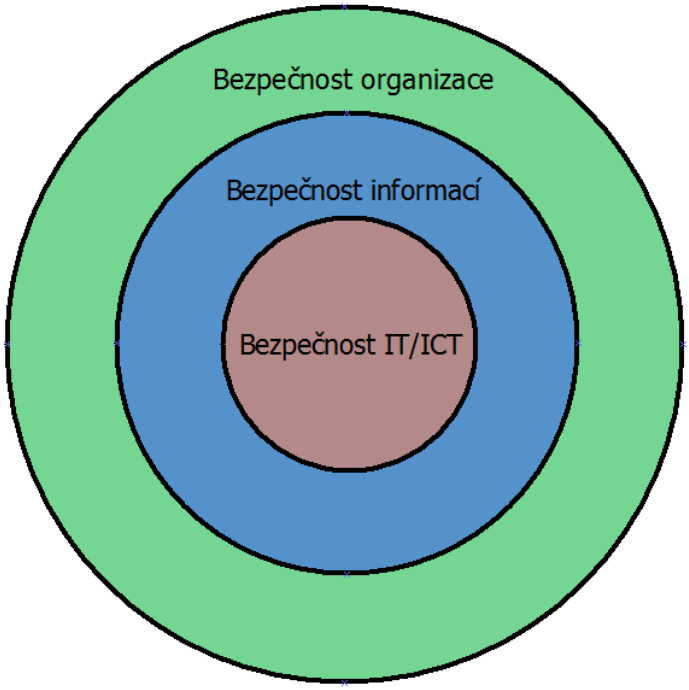
Certifikace podle normy, neboli ověření funkčnosti a shody s normou znamená, že nezávislý akreditovaný certifikační orgán (v ČR se tím zabývá několik desítek firem) ověří, zda vybudovaný systém nebo systém řízení odpovídá požadavkům normy. Následně po úspěšném skončení auditu vystaví vybraná certifikační společnost příslušný certifikát. Tento certifikát je platný po omezenou dobu a musí být v pravidelných intervalech obnovován.

*[**3**, s.204]*

3.5 Řízení bezpečnosti informací

*Zpracováno podle [**3**, s.95]*

Bezpečnost informací a jakýkoliv z ní vycházející systém přichází společně s pojmy bezpečnost organizace a bezpečnost IS/ICT, což ukazuje následující cibulový model:



*Obrázek 8 – cibulový model bezpečnosti – „Autor, podle Lit **3** s.60“*

Nejvyšší kategorií je bezpečnost organizace, jejíž součástí je ochrana majetku organizace, zajištění bezpečnosti objektu a obzvlášť přístupu do objektu nebo podstatných místností. Zároveň v sobě zahrnuje i podoblast řízení bezpečnosti informací, jejímž cílem je shrnout zásady bezpečné práce s informacemi všeho druhu, tedy nejen v digitální podobě. Bezpečnost IT/ICT pak chrání výběrově aktiva, která jsou přímo součástí informačních systémů.

Základní koncept bezpečnosti IT/ICT představuje vztahy mezi aktivy organizace, potencionálními hrozbami a možnými dopady na organizaci. Nejdůležitější součást je potom opatření proti těmto hrozbám a určení míry zranitelnosti vůči jednotlivým případům.

3.5.1 TCSEC a ITSEC

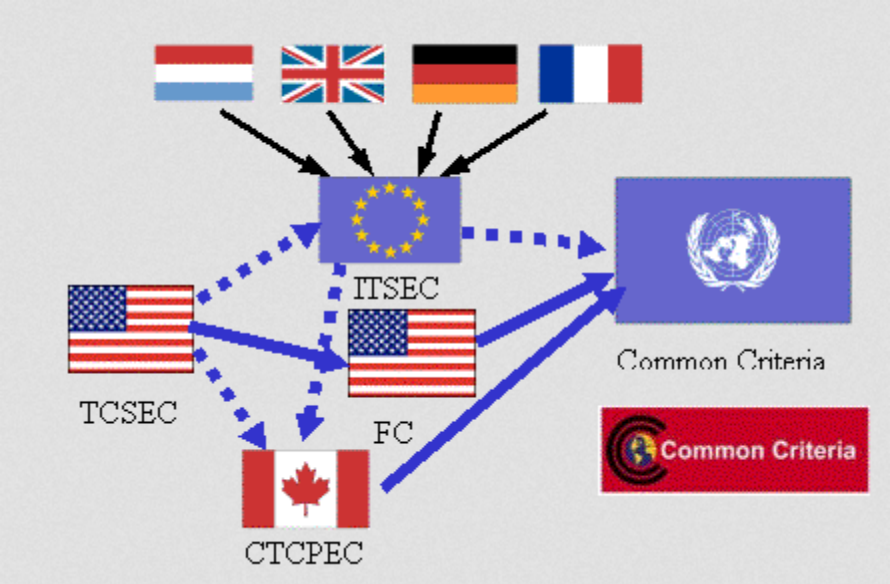
Historicky se jako první systémům řízení a hodnocení bezpečnosti informací věnoval dokument **TCSEC** (Trusted Computer Security Evaulation Criteria), vytvořený již v roce 1983 v USA národním střediskem počítačové bezpečnosti USA (NCSC). Dle tohoto dokumentu (později uznán jako norma Ministerstva obrany USA) se posouzení bezpečnosti informací opírá o míru splnění požadavků dělených do tří částí, a to zásady, odpovědnost a záruky. Podle míry splnění požadavků potom rozděluje informační systémy do čtyř základních skupin D C B A (řazeno od nejhoršího hodnocení po nejlepší).

V ovlivnění této metodiky vzniká v Evropě roku 1990 **ITSEC** (Information Technology Security Evaluation Criteria) jako společný projekt Francie, Německa, Nizozemí a Velké Británie. Základem této metodiky je rozdělení požadavků na předmět hodnocení, na míru záruk a funkčnost. S tím, že míru záruk rozděluje na záruky za správnost a záruky na efektivnost.

*[**3**, s.64-69]*

3.5.2 CC- Comon Criteria

Jelikož vznikaly i další metodiky pro hodnocení bezpečnosti IT systémů, v roce 1993 všechny hlavní světové vládní organizace přistoupily ke společnému projektu, jehož výsledkem byl vznik Společných kritérií (CC – Comon Criteria) Vznik dokládá další obrázek:



Obrázek 9 – cibulový model bezpečnosti – „https://akela.mendelu.cz/~lidak/bis/ccvyvoj.gif“

Společná práce vyvrcholila na konci roku 1999, kdy organizace ISO převzala verzi 2.1 a implementovala ji jako normu ISO/IEC 15408 – v současnosti je již do této normy implementována verze CC s číslem 3.1 revize 4.

Tento model hodnocení rozlišuje společná kritéria pro uživatele, tvůrce a hodnotitele. Uživatelům je zde dovoleno vymezit bezpečnostní požadavky, pro tvůrce jsou prostředkem postihujícím bezpečnostní vlastnosti výsledného produktu a pro hodnotitele mají kritéria nástroj pro stanovení míry bezpečnosti a tím pádem úrovně produktu podle předem stanovených úrovní záruk.

Společná kritéria vymezují tři typy hodnocení:

1) Profil bezpečnosti - PP
2) Specifika bezpečnosti - ST
3) Předmět hodnocení – TOE

*[**3**, s.73]*

Podle výsledků a důvěryhodnosti jsou pak produkty děleny na „úrovně hodnocení záruk“ (Evaluation Assurance Level – EAL)

Common Criteria Evaluation Assurance Level (EAL)	Process rigor required for development of an IT product
EAL 1	Functionally tested.
EAL 2	Structurally tested.
EAL 3	Methodically tested and checked.
EAL 4	Methodically designed, tested and reviewed.
EAL 5	Semi-formally designed and tested.
EAL 6	Semi-formally verified, designed and tested.
EAL 7	Formally designed and tested.

*[**3**, s.84-85]*

3.5.3 Životní cyklus PDCA

PDCA (plan-do-check-act), tedy „plánuj, dělej, kontroluj, jednej“ jsou základní kroky konceptu životního cyklu systému řízení, na který navazují veškeré systémy řízení bezpečnosti informací (ISMS). Původně vytvořil tento koncept Walterem Shewhart v roce 1930. Následně koncept modelu PDCA pro zlepšování jakosti využil Edwards Deming, kterému je celý koncept často mylně připisován

PDCA je připraven zvláště pro efektivní řešení a zlepšování výrobních aktivit a systému. PDCA by měl být znám každému, jenž pracuje v oblastech systémů kvality, ekologických systémů nebo zajištění bezpečnosti, včetně bezpečnosti IT.

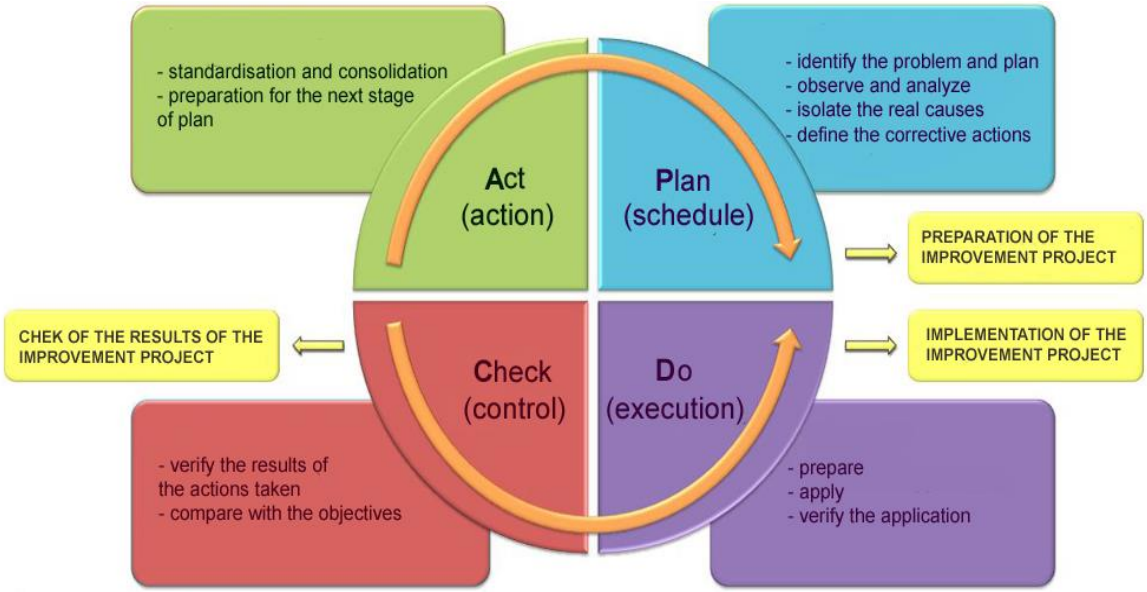
1) **Plan** - Prověřit současny stav a posoudit případné problémy či omezení procesů. Navrhnout možná řešení a naplánovat provedení nejvhodnějšího řešení.

2) **Do** - Samotná implementace vybraných řešení.

3) **Check -** Zkontrolovat a následně zhodnotit výsledky testu. Na základě toho posoudit, zda bylo plánovaných výsledků dosaženo.

4) **Act -** Provedení nápravných opatření a preventivních činností.

*[**3**, s.20]*



Obrázek 10 – PDCA model bezpečnosti – „http://www.iwolm.com/wp-content/uploads/2012/01/PDCA_en.jpg“

3.5.4 ISMS

ISMS (Information Security Management System) neboli systém řízení bezpečnosti informací je dobře dokumentovaný systém, založený na konceptu PDCA, který chrání všechna definovaná informační aktiva za předpokladu řízení rizika bezpečnosti informací. Dalším předpokladem je monitorování stavu bezpečnosti a neustálé zlepšování bezpečnosti informací. S pojmem se prvně shledáváme v normě ISO/IEC 17799, ale nově revidovaná verze je součástí již přestavené řady norem ISO 27000.

*[**3**, s.95]*

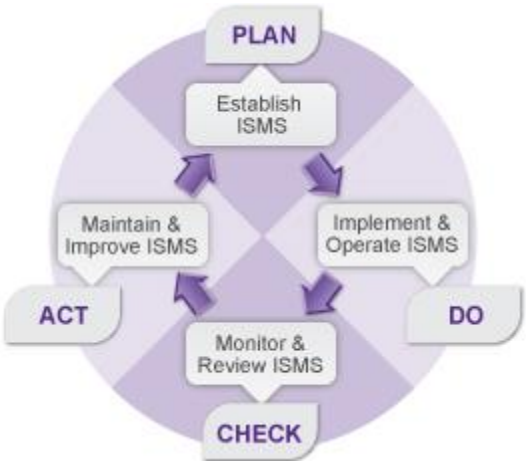
Pokud na ISMS nahlížíme z pohledu PDCA, tak se hlavní fáze transformují na:

1) **Ustanovení ISMS** – upřesnění rozsahu a hranice, kterých se řízení bezpečnosti týká. A na základě zhodnocení rizik vybrat vhodná bezpečnostní opatření.

2) **Zavádění a provoz ISMS** – efektivní a systematické prosazení vybraných bezpečnostních opatření.

3) **Monitorování a přezkoumání ISMS –** zajištění zpětné vazby a hodnocení úspěšných a neúspěšných stránek řízení ISMS.

4) **Údržba a zlepšování ISMS** – realizace možností zlepšování systému řízení bezpečnosti informací soustavným zlepšováním vlastností a odstraňováním nedostatků.



Obrázek 11 – zavedení ISMS podle ISO 27001 – „http://gaelrisk.com/siteimages/27001/plan_do_check_act_280.jpg“

Systém ISMS začínají hojně využívat i organizace, jimž to nenařizuje zákon nebo nutnost dodržovat normu, u kterých jsou informace a informační technologie klíčovou součástí, nebo které spravují citlivá data svých klientů a musí zajistit jejich bezpečnost. (což v souvislosti se zmíněným Kybernetickým zákonem dostává nový rozměr i v ČR)

Jako hlavní přínosy bych pak viděl:

1) Řízené odstranění nebo snížení rizik v oblasti informačních systémů

2) Trvalé monitorování a zlepšování systému řízení bezpečnosti informací (ISMS)

3.5.5 Bezpečnostní politika

Bezpečnostní politika organizace tvoří jeden ze základních pilířů, na kterém stojí systém řízení informační bezpečnosti. Její definice je jedním z potřebných kroků. Pokud nejsou oficiálním způsobem jednoznačně definovány některé základní parametry, jako jsou např. povinnosti a odpovědnosti klíčových rolí a zaměstnanců organizace, může být následně celý systém budován chaoticky, neefektivně a neúčelně. A pouze na pevných a stabilních základech může být vystavěn pevný a stabilní systém řízení…

*[Lit **11**]*

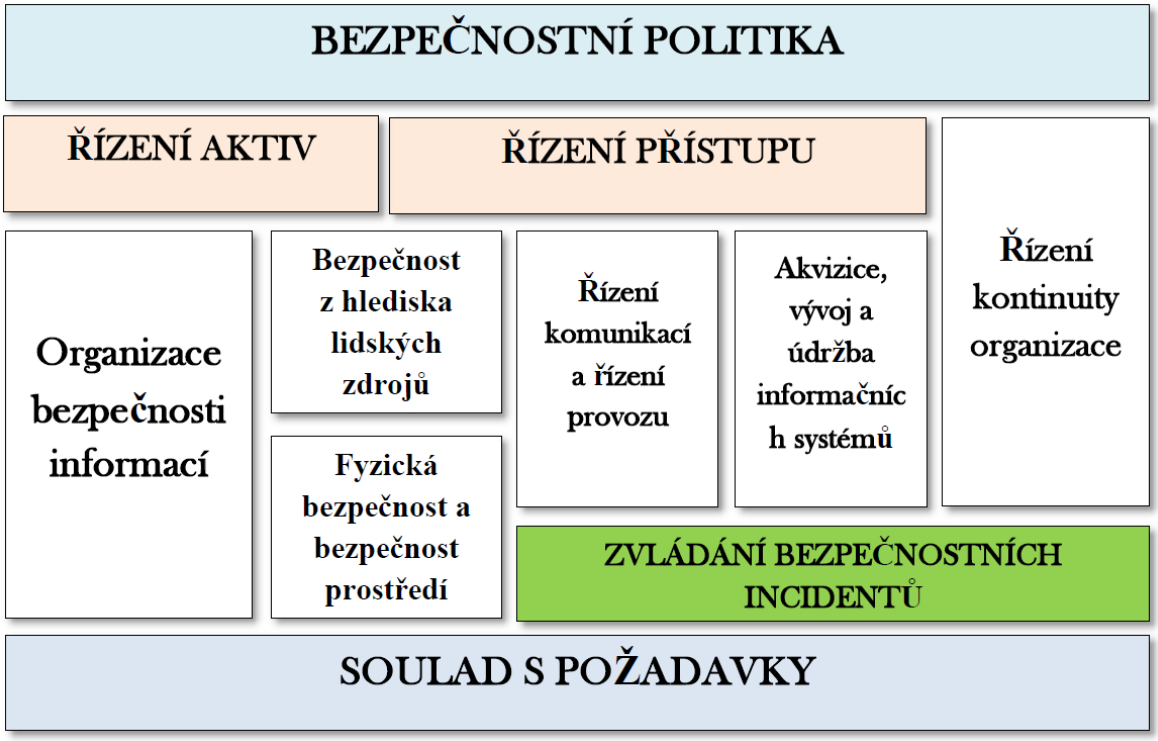
Základním úkolem bezpečnostní politiky je definovat základní bezpečnostní požadavky a nařízení, jejichž cílem je zajistit ochranu a bezpečnost informací. Bezpečnostní politika vymezuje taktéž rámec informační bezpečnosti organizace a je závazná jak pro interní subjekty, tak pro externí subjekty (spolupracující firmy atd.). Tento rámec musí být v souladu nejen s politikou bezpečnosti ale i pracovněprávní a legislativní, což může znamenat právní konzultace ohledně nasazení rozsáhlých systémů kontroly a shromažďování osobních dat jeho uživatelů. Cílem této politiky tedy není jen ochrana před hrozbami, ale také pozvednutí výkonnosti firmy.

Je podkladem pro budování nižších a specifických stupňů bezpečnostní dokumentace. Tvorba by měla probíhat podle procesu typu PDCA a sestávat z následujících kroků

- analýza rizik (viz další podkapitola)
- vypracování (dopracování) bezpečnostní politiky a následná implementace
- test funkčnosti implementace bezpečnostní politiky
- posouzení účinnosti a adekvátnosti bezpečnostní politiky

*[**3**, s.133]*

Pohled na bezpečnostní politiku podle **normy ISO/IEC 27001** ukazuje následující obrázek:



Obrázek 12 – bezpečnostní politika podle ISO 27001 – „http://www.krausova.eu/userfiles/image/ISMS_Oblasti.png“

3.5.5.1 Analýza a řízení rizik

Základem ISMS (potažmo modelu PDCA) jakožto i dobré bezpečnostní politiky je analýza rizik a podle ní přizpůsobené řízení rizik. Proces analýzy rizik slouží pro vytvoření ucelené představy o možných rizicích, která mohou na náš podnik působit. Přistupovat k analýze rizik lze několika způsoby:

1) **neformální analýza rizik** -není založena na formální metodologii, je založena na zkušenostech jednotlivců tvořících analýzu rizik.

2) **základní analýza rizik** - postupuje se podle všeobecného standardu, vyžaduje minimum zdrojů organizace.

3) **detailní analýza rizik –** používá standardní strukturované metody, je ovšem časově nejnáročnější.

4) kombinovaná analýza rizik - kombinované použití již představených metod podle potřeby.

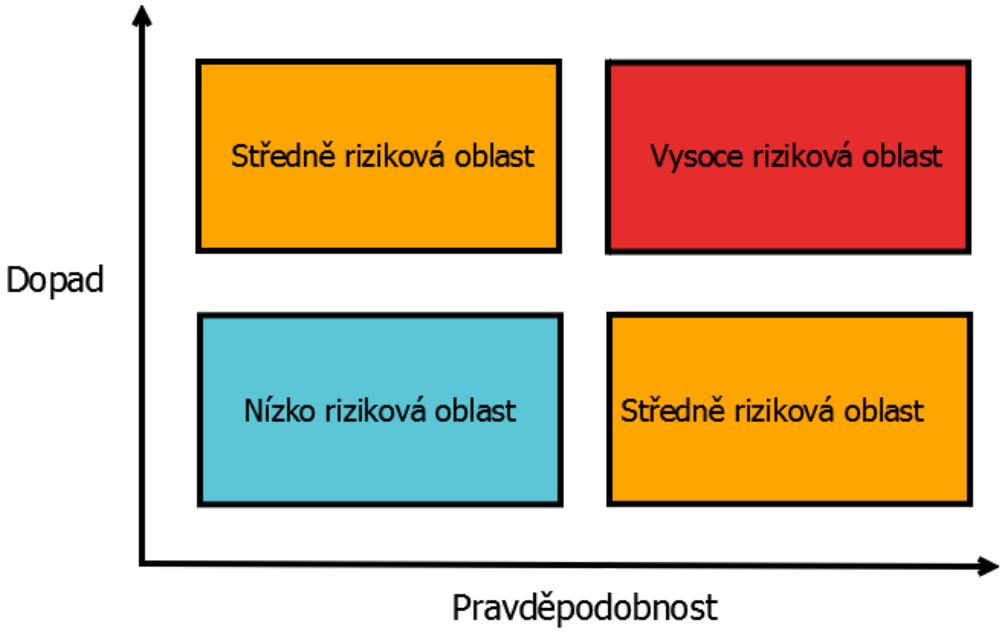
*[**1**, s.134]*

V analýze rizik se používají tyto pojmy:

- **Aktivum** – souhrn hmotných a nehmotných vlastnictví podniku, které by mělo být chráněno.
- **Hrozba** – událost, která potencionálně může zapříčinit narušení důvěrnosti, integrity, případně dostupnosti aktiv.
- **Zranitelnost** – specifikací zranitelného místa aktiv, která může být zneužita hrozbou.
- **Riziko** – kvantifikace pravděpodobnosti, že hrozba využije zranitelnosti.
- **Důsledek** – odhadované vyčíslení potencionálně napáchaných škod.
- **Opatření** – definování preventivních opatření, která snižují zranitelnost a chrání před hrozbami.

*[**3**, s.61-64]*

Významnost rizik pak ukazuje následující graf:



Obrázek 13 – významnost rizik 1 – „Lit 1 s.136“

*[**1**, s.136]*

Hlavním kritériem analýzy rizik je bezpečnostní politika podniku následována legislativním prostředím a normami. Velkou váhu poté má i zkušenost a způsobilost pracovníků krizového řízení. Výstupem je potom tzv. registr rizik (nebo taky katalog ohrožení), který funguje jako základní informace vstupující do procesu plánování opatření.

Registr rizik, jednoduše a bezpečně zpřístupní informace pracovníkům společnosti. Lze se tak snadno dostat rovnou k použití nových postupů řízení bezpečnosti v reakci na nová ohrožení. Základem je, že na různé hrozby lze uplatnit stejné opatření a tím dojde k zjednodušení celého systému řízení rizik, zpřehlednění a je docíleno i vysoké efektivity.

Schematické vyjádření procesu řízení rizik ukazuje další obrázek:

Obrázek 14 – registr rizik– „http://www.ictsecurity.cz/images/09/anect091125.png“

3.6 Penetrační testy

Penetrační testy jsou metody, jak odhalit slabá místa v počítačovém a síťovém zabezpečení, potažmo v bezpečnostní politice organizace. Prováděno je to cílenou simulací útoku proti IT infrastruktuře testované organizace. Cílem je odhalit nedostatky v konfiguraci a nedostatečná protiopatření, případně známé neošetřené hardwarové či softwarové chyby. Tento typ softwarového auditu většinou vykonává externí subjekt, který přebírá roli útočníka. Jsou dva základní typy penetračního testování, a to interní a externí. Interní je prováděno uvnitř sítě a externí zpravidla z internetu.

*[Lit **13**]*

*[Lit **14**]*

Výsledky penetračních testů shromážděných do souhrnné analýzy jsou následně předány odpovědným osobám (může to být vedoucí IT, bezpečnostní expert nebo přímo management společnosti). Součástí zprávy pak může být i reálné zhodnocení jednotlivých hrozeb, jejich případné dopady a návrh protiopatření.

Tyto testy dále prověřují schopnosti ochranných prvků systému, a to v rovině odhalení a náležité reakce. Nástroji těchto testů jsou například specializované distribuce operačních systémů (nejčastěji Linux – například Kali Linux), softwarové frameworky, které sdružují mnoho funkcí do jednoho celku (příkladem je W3AF). Poslední skupinou jsou jednotlivé programy, buď vlastní tvorby, volně dostupné, nebo je obsahuje přímo operační systém (jednoduché útoky ping, telnet, apod).

Dalším zajímavým dělením penetračních testů je podle znalostí útočníka o cílovém systému.

- **Black box –** v tomto případě nemá útočník žádnou znalost cílového systému a útočí „naslepo“.
- **Gray-box –** útočník má základní znalost systémů, která může odpovídat informacím od běžného uživatele.
- **White-box –** nejhorší scénář z pohledu bezpečnosti, ale také nejlepší otestování, kdy útočník zná detailní strukturu IT a má k dispozici vnitřní dokumentaci. Tento případ může nastat při úniku informací od IT administrátorů, případně managementu. V tomto typu testů může jít i o analýzu zdrojového kódu a hledání chyb na této nejnižší programové úrovni.

Běžný útočníkův postup proti napadenému systému ukazuje následující tabulka:

Krok	Popis	Příklady
Průzkum	Aktivní nebo pasivní sběr informací o síti.	Odposlech síťového provozu, průzkum HTML kódu webových stránek firmy, sociální útoky.
Skenování	Nalezení systému a služeb, které na nich běží.	Hromadný ping, skenování portů.
Získání přístupu	Zneužití nějaké známé bezpečnostní díry k získání přístupu do systému.	Zneužití přetečení bufferu nebo uhodnutí hesla hrubou silou.
Udržení přístupu	Nahrání softwaru, který se postará o útočníkův budoucí přístup k počítači.	Instalace zadních vrátek.
Zametání stop	Zamaskování činnosti, kterou útočník v systému provádí.	Smazání nebo úprava dat v systémovém protokolu a aplikačních protokolech.

*[Lit **12**]*

4 Představení společnosti a testovaného zařízení

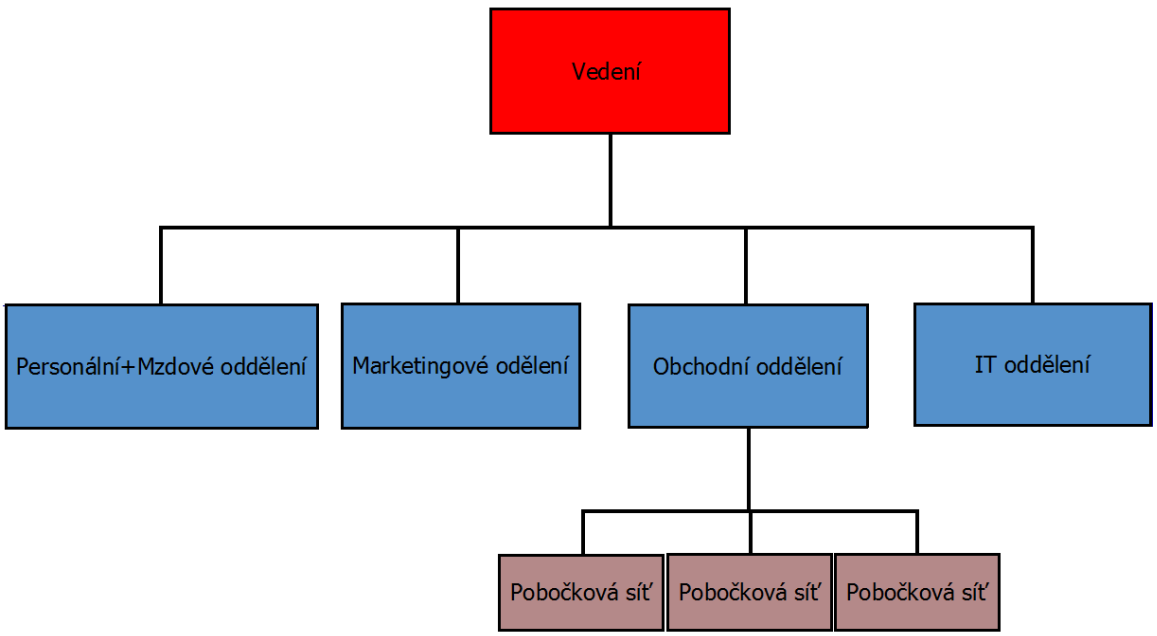
Úvodem této kapitoly bych rád poznamenal, že sehnání společnosti, kde bych mohl provést testy a jakýmkoliv způsobem zveřejnit její výsledky, bylo velice obtížné. Od odpovědi, že nepřipadá v úvahu (už jen jako porušení směrnic), jsem dostal i zarážející odpověď typu, máme hrubou představu o našem zabezpečení a víme, že má určité trhliny, a proto nechceme, aby to někdo zkoumal. Podle mého názoru je problémem způsob myšlení typický pro velkou část menších až středních podniků, které sice mají představu, v čem spočívají jejich slabiny, ale nijak je neřeší.

U testů z firmy, kde jsem uspěl a podařilo se mi naklonit vedoucího IT oddělení, aby mi testování umožnil, je z důvodu vysoké citlivosti zde uváděných údajů vymazáno

mnoho identifikačních vodítek a firmu nebudu jmenovat, což je doporučeno vedoucím mé diplomové práce a za zároveň i podmíněno ze strany firmy. Z toho důvodu budou některé informace podány například v rámci rozmezí nebo zaokrouhlené.

4.1 Profil společnosti

V této části diplomní práce pojednává o společnosti z finančního nebankovního sektoru. Firma se zabývá převážně poskytováním krátkodobých hotovostních půjček fyzickým osobám do výše cca 100 tisíc Kč. Na našem trhu funguje již řadu let a expanduje i do okolních zemí. Sídlo společnosti se nachází v Praze, kde se zároveň nachází i většina IT zázemí, dále je společnost dělena na pobočky podle krajů ČR. Mezi dceřinými firmami a mateřskou firmou není vybudována žádná společná IT infrastruktura ani jednotný systém. Ač se používá stejný, na míru vyrobený interní software, tak mezi různými státy je oddělen a neexistuje žádná centrální databáze. Stálých zaměstnanců má v současnosti firma přibližně dvě stovky, z čehož naprostá většina připadá na pobočkovou síť, a k tomu je zde zhruba tisíc obchodních zástupců pracujících na živnostenský list. Obrat společnosti je v řádu stovek miliónů Kč ročně. Strukturu společnosti můžeme vidět na následujícím schématu:



Obrázek 15 – struktura společnosti– „autor“

4.2 Zadání analýz a testů

Ve spolupráci s vedoucím IT oddělení jsem vytvořil určitý rámec, podle kterého budou audit a testy postupovat, a specifikoval to, co by to celkově mělo řešit, byť v teoretické rovině. Následující tabulka obsahuje dohodnuté body:

Bod č.	Co se má dělat:	Co bude výstup:
1.	Základní přehled stavu IT, struktury sítě a stavu HW a SW.	Komentovaný přehled.
2.	Zhodnocení rizik a bezpečnosti.	Analýza rizik, SWOT analýza bezpečnosti.
3.	Testování systému - penetrační testy.	Doporučení ke zjednání nápravy.
4.	Navrhnout změny v kontextu zjištění předchozích bodů.	Komentovaný návrh změn bezpečnostní politiky.

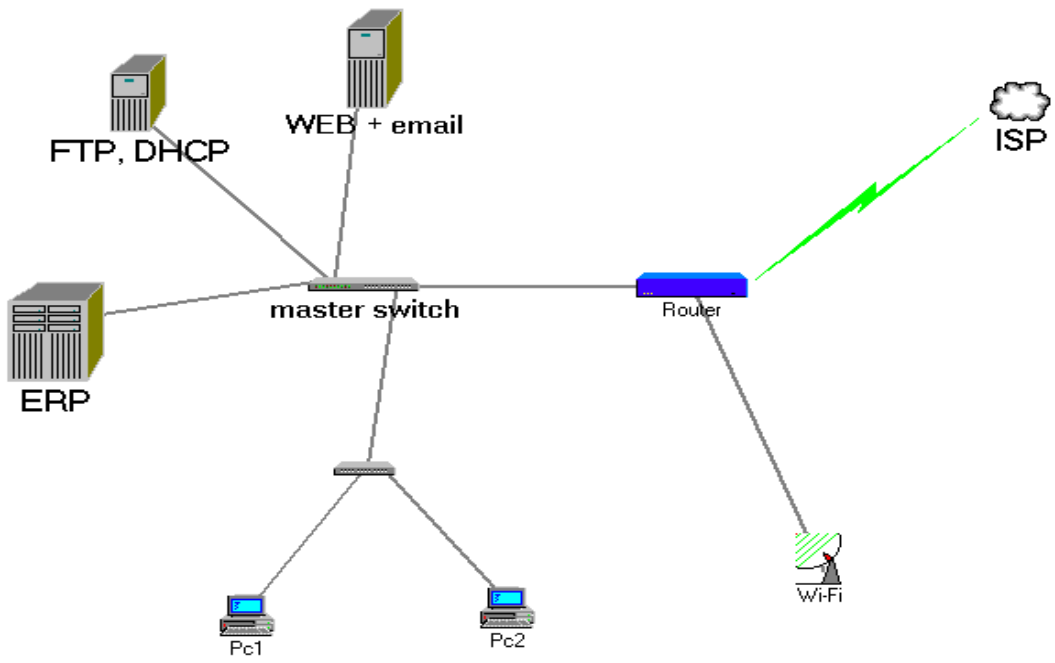
4.3 IT infrastruktura

IT struktura podniku je taková, že v sídle společnosti je jedna místnost, sloužící jako datacentrum (serverovna), kde se nachází naprostá většina IT zázemí. Nachází se zde webový a emailový server na jednom fyzickém serveru HP ProLiant s dvěma dvou-jádrovými procesory Intel Xeon a 16GB paměti RAM z roku 2010. Dále je zde clusterový server pro ERP (Enterprise Resource Planning) systém společnosti s aktivním load balancingem, zajišťujícím rozložení zátěže mezi dva identické servery HP Proliant řady SL. Každý s dvěma osmi-jádrovými procesory Intel Xeon E5 a 32GB paměti RAM, tento systém byl pořízen do firmy v roce 2013. Jako datové úložiště zvolili NAS server Dell PowerEdge řady 2xxx z roku 2008 obsahující čtyři 2TB disky zapojené do RAID 1, k dispozici je tedy pro data 2x 2TB tedy 4TB prostoru. Doplněno je to o server Dell řady 800

pro převážně potřeby vnitřní sítě, pracuje primárně jako DHCP server, ale VPN server a neveřejný FTP server.

Z vnější sítě je přístupný pouze webový a emailový server, případně po připojení přes VPN i FTP server a ERP systém. Připojení do internetu je realizováno skrz starší router Cisco řady 800 s integrovaným firewallem. V sídle společnosti se dále nachází množství osobních PC připojených do hlavní sítě a zasedací místnost s Wi-Fi připojením do internetu. Toto připojení je pomocí oddělené podsítě oprávněno přistupovat pouze k internetu. Na každé pobočce se nachází alespoň jeden stolní počítač s přístupem do ERP systému společnosti připojující se pomocí VPN do hlavní sítě.

Schéma sítě v sídle firmy znázorněno diagramem:



Obrázek 16 – infrastruktura IT – „autor“

4.3.1 Síť LAN/WLAN/WAN

4.3.1.1 LAN

Lan síť jako taková je vybudována profesionálně, strukturovaná kabeláž je skvěle vyvázána, přístup do rozvodné skříně má jen několik málo administrátorů. Aktivní prvky jsou dostatečně dimenzovány, zde je technicky vše v pořádku. Bohužel ale chybí důkladná dokumentace sítě.

4.3.1.2 Bezdrátová síť

Jak již bylo napsáno, v sídle firmy se nachází wifi, primárně pro zasedací místnost a pro probíhající schůzky, ale pokryt je zároveň zbytek pracovních prostor, a to nejspíš i okolních kanceláří nepatřících pod tuto firmu. Síť je chráněna technologií WPA (Wi-Fi Protected Access), která je v současnosti ve spojení s algoritmem AES považována za nejbezpečnější. Za další ochranu sítě lze považovat fakt, že se sdílený klíč bezdrátové sítě každý týden mění a dále je v síti přidělována serverem DHCP jiná sada IP adres s jinou maskou sítě.

Jak je již z diagramu sítě vidět, wifi síť se nachází za firewallem a představuje tedy sama o sobě ohromné riziko, jelikož se dneska nedá na 100% označit žádná wifi síť jako neprolomitelná, což se pokusím dokázat i v tomto případě v následující kapitole.

4.3.1.3 WAN – přístup do internetu

Připojení do internetu je realizováno přes pevný kabel společným vedením pro celou budovu. Zde určité riziko představuje společné vedení pro více firem v jedné budově, ale jako větší problém vidím neexistenci jakékoli náhradní formy připojení do internetu. V případě výpadku poskytovatele (ISP) dojde ke značným problémům obzvlášť na pobočkách, které potřebují často přistupovat do podnikového ERP systému.

4.3.2 Softwarová vybavenost

Z pohledu softwarové vybavenosti jsou na tom uživatelská PC dobře, standardně se zde používá legální systém Windows 7, aktualizace se instalují pravidelně podle plánu,

firemní politikou je defaultně zakázán software, který není na seznamu povoleného software. Jakožto kancelářský balík se potom používá kancelářský software Libre Office, který je šiřitelný pod licencí GNU LGPL, takže odpadá nutnost zakupovat licence.

Servery jsou bez výjimky vybaveny odlišnými edicemi linuxového operačního systému. Běží zde služby jako MsSQL, DHCP daemon, webový Apache nebo Samba pro sdílení dat se systémem Windows.

Možné problémy zde plynou z použití různých verzí linuxu v jednom případě již s propadlou podporou od vývojářů. Další problémy můžou plynout z nedostatků nastavení, které je zřejmé už jen u PC s Windows 7, o čemž pojednává další podkapitola.

4.3.2.1 Uživatelské účty

Operační systém standardním uživatelům poskytuje dostatečná práva typu „ Power user“, ale tito uživatelé nemají plný administrátorský přístup. Dále uživatelé nepodléhají omezení z pohledu manipulace s daty na lokálním PC. Co se týče přístupu na sdílené síťové složky, tak jsou alespoň rozdělena práva pro různé skupiny uživatel, takže zde si uživatelé navzájem do složek nemůžou. Z uvedených faktů tedy vyplývá, že každý uživatel může volně stahovat a instalovat software, který nevyžaduje přímo administrátorská práva.

Pro tento krok jsem zvolil testování pomocí nástroje Microsoft Baseline Security Analyzer 2.3, kde byl zjištěn jeden vážný nedostatek, a tím je nastavení systému s neomezenou platností uživatelského hesla – což by se v mnohých společnostech dalo považovat za porušení bezpečnostní politiky, ale o tom až dále.

Část výstupu z tohoto programu zde uvádím pomocí tohoto obrázku:

Obrázek 17 – screen MS BSA – „autor“

Na PC je potom administrátorský účet se stejným heslem pro všechny PC. V tomto bodě je tedy další evidentní slabina zabezpečení – stačí zjistit heslo na jednom PC a administrátorský účet je rázem dostupný všude. A zjistit všechna lokální hesla na systému Windows je pomocí programu Ophcrack opravdu velmi jednoduché (vlastně stačí jen nabootovat přes DVD mechaniku nebo USB Flash disk) a většinou to zabere maximálně pár desítek minut, podmínkou ovšem je přístup k těmto PC. Výjimku tvoří velmi dlouhá a silná hesla.

4.3.2.2 Antivirové a anti-malwarové (anti-spywarové) řešení

V celém podniku jsou zakoupeny licence pro centrální antivirové řešení, kterým je NOD32. Na Windows ve verzi Endpoint Security – tedy zároveň jako anti-malware. Na linuxových serverech zase běží Endpoint Antivirus, kde nad mailovým serverem je naistalován ještě NOD32 Mail Security. Všechny instalace jsou nastaveny tak, aby automaticky stahovaly potřebné aktualizace programů i databáze virových signatur. Potencionální slabinu zde tvoří volná přístupnost uživatelů k nastavení antivirového programu, kdy v nejhorším případě mohou celou ochranu i vypnout.

4.3.2.3 Zálohování

Zálohování je upraveno vnitřními směrnicemi, které udávají jak často a jakým způsobem zálohovat. V současnosti je ochrana dat proti selhání jednotlivých disků nebo stanic na přijatelné úrovní. Kromě redundance dat na samotném datovém úložišti NAS je tu pak vyhrazen zálohovací disk, kam se zálohuje každou noc databáze ERP systému a sdílená firemní data. Měsíčně se potom zálohuje mailová databáze a obsah webových stránek (ten se příliš často nemění). Toto probíhá automaticky a o výsledcích zálohy jsou zasílány informační emaily do sdíleného mailového boxu. V případě výpadku zálohování přijde výstražný mail všem pracovníkům IT oddělení. Kromě toho jednou za měsíc jsou veškeré nové zálohy vypáleny na Blu-ray disky a archivovány. Dále jsou připraveny postupy pro obnovu jednotlivých serverů včetně předpřipravených skriptů pro jejich nastavení.

Zálohování je tedy řešeno systémově, ale není promyšleno do důsledků, které požadují dnešní normy pro manažery, jako například **ČSN BS 25999-1:2006**. Není vypracován celkový havarijní plán a data nejsou nijak chráněna proti pravděpodobným katastrofám, jako je požár, který zničí nejen archivované zálohy, ale i veškeré pevné disky s daty.

4.3.2.4 Logování

Všechny dostupně aplikace mají zapnutou přiměřenou vyšší úroveň logování, takže v případě problémů lze leccos dohledat. Nicméně se zde nenachází žádný systém, který by tyto logy zpracovával, natož vyhodnocoval, a tím předcházel riziku rozsáhlého bezpečnostního incidentu.

4.4 Bezpečnostní politika

Jako naprosto nevyhovující se mi jeví koncepce bezpečnostní politiky, jelikož de facto žádná neexistuje, jsou zde různé směrnice, nebo doporučení zaměstnancům, které se věnují některým oblastem, ale mnohé oblasti jsou naprosto nepodchyceny – existují maximálně jako informace předávané ústně. Dále zde není žádné řízení bezpečnosti, koncepce rozvoje (bezpečnosti) IT, natož nějaká spolupráce s vedením společnosti.

V tomto bodě vidím absolutně největší problém, který vlastně zároveň ovlivňuje i většinu popsaných zjištěných nedostatků.

4.4.1 Fyzické zabezpečení

Prostory v sídle firmy jsou vybaveny přístupovým systémem na čipové karty HID i Class. Bez čipové karty se do prostor dá dostat jen přes recepci nebo násilným vniknutím.

Celý systém pro řízení přístupu je značně zastaralý program na zakázku, který ale při současném využití plně dostačuje. Přístup do technické místnosti mají všichni IT zaměstnanci taktéž pomocí systému pro řízení přístupu. Kromě přístupu pomocí karet mají členové vedení a vedoucí jednotlivých oddělení k dispozici univerzální klíč, který lze použít v případě výpadku systému.

Potencionální hrozbou je zde zneužití přístupové karty a s tím související neexistence logů o přístupu do technické místnosti – tedy nelze dohledat, kdo tam kdy byl. Současný software tuto možnost ani nenabízí.

4.4.2 Správa a politika hesel

Správa hesel podléhá internímu dokumentu, který stanovuje minimální délku hesel na 8 znaků a další aspekty, jako např. které skupiny znaků ho mají tvořit atd. Ačkoliv tento dokument lze považovat za dostatečný, není nijak stanovena kontrola dodržování, tedy v praxi to znamená, že to uživatelé obcházejí. Je zde tedy velký prostor pro volnost a vše závisí na zodpovědnosti každého uživatele.

4.4.3 Zajištění dat proti zneužití

Ochrana dat před únikem je zde realizována v minimální míře. V případě práce s ERP systémem je nakonfigurován uspořádaný systém práv uživatelů, stanovující do jakých částí a tabulek systému mají přístup, což je podchyceno a graficky znázorněno v jednom z interních dokumentů. Dále určitou ochranu tvoří rozdělení přístupových práv ke sdíleným složkám, ale ochrana dat, která jsou uživatelům přímo přístupná, není žádná.

Firemní data mohou naprosto nepozorovaně opustit firmu a dle informací od vedoucího IT je to také častý případ, jelikož o data mají zájem konkurenční společnosti a od zaměstnanců je vykupují. Zde opět existuje velice vážný problém firemní bezpečnosti.

4.4.4 Vzdálený přístup

Firma využívá několika možností, jak se připojit k jednotlivým systémům podnikové infrastruktury. Prvním z nich je FTP server, který běží na standardním portu 21 a pro přihlášení je třeba jméno i heslo. Sice je zabezpečení očividně dost slabé, ale FTP se nepoužívá ke stahování citlivých firemních dat, ale spíš obecných dokumentů, šablon apod.

Dále je dostupná webová verze firemního mailu, zabezpečená pomocí HTTPS a ověřeného SSL certifikátu, vše je dostupné i přes zašifrovanou verzi protokolu POP3.

Další vzdálený přístup do firmy mají pobočkové počítače, které se připojují přímo na databázi ERP systému. Přesný způsob komunikace mi nebyl objasněn, ale jedná se o šifrovanou komunikaci přímo prostřednictvím internetu – tedy přes otevřené porty na firemním firewallu. K autentifikaci používají pobočkové PC instalovaný certifikát, generovaný z obslužných programů ERP systému. Zhodnotit bezpečnost tohoto řešení si tedy netroufám, ale minimálně vidím problém s neustále otevřeným portem pro tato příchozí spojení.

4.4.5 Kontroly (audit)

Každá informační infrastruktura potřebuje pravidelnou a nezávislou kontrolu svého zabezpečení, a proto byla vznesena otázka na existenci těchto kontrol nebo lépe auditů. Zde je opět neutěšený stav, jelikož kontroly se provádí náhodně a zřídka, spíše v souvislosti v nějakým problémem. Audit, natož pak externí audit bezpečnosti IT, se nikdy nerealizoval a tato práce je tedy ojedinělým krokem tímto směrem.

5 Testy a vyhodnocení

Soubor testů byl navržen podle možností cílového podniku a také přípustnosti ze strany vedení IT oddělení. Proto byly provedeny vybrané testy vnější a vnitřní bezpečnosti, webové ochrany, síťové ochrany a nakonec provedena analýza rizik.

5.1 Důvod testování

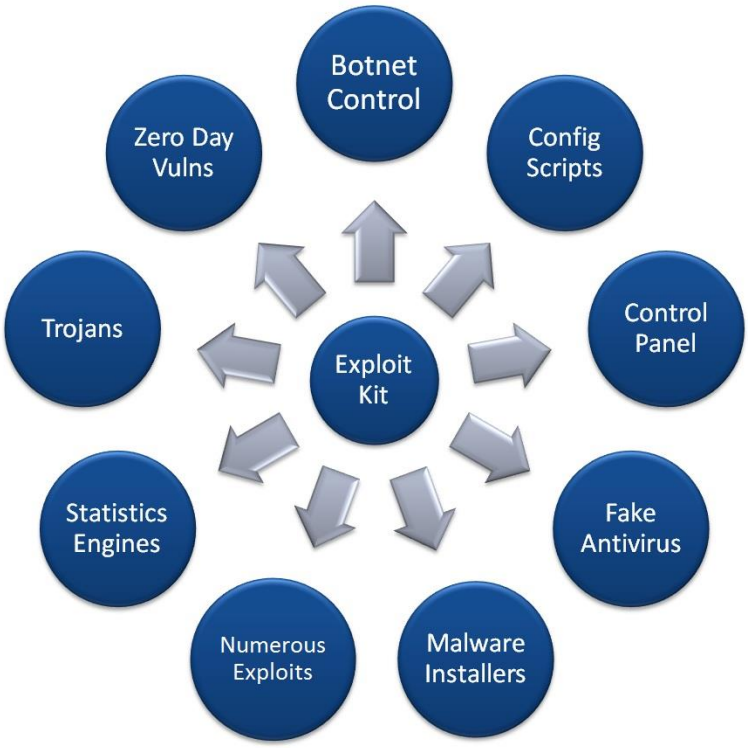
Důvodů k testování systému již bylo představeno několik, ale nyní uvedu konkrétní skupinu ohrožení pro jakýkoliv software, která je velmi aktuální.

5.1.1 Exploit

Exploit je v informatice speciální program, kus kódu nebo jen sekvence příkazů, který využívá bezpečnostních chyb v programech a dokáže způsobit nestandardní činnost napadeného software, čímž umožní útočníkovi získat nějaký prospěch. Mezi obvyklé cílové funkce se potom řadí:

- Ovládnutí PC
- Instalace malware
- Instalace spyware

Další možnosti ukazuje následující obrázek:



Obrázek 18 – exploit kit – „http://blogs.cisco.com/wp-content/uploads/exploit-kits.jpg“

Útočník ke splnění cíle využívá celou řadu metod, z nichž jako nejzákladnější bych zařadil tyto:

1) **Přetečení zásobníku (Buffer overflow)** tvoří až 80% veškerých zranitelností programů. Jedná se o situaci, kdy se program pokusí do zásobníku uložit víc dat, než se tam vejde, což způsobí pád softwaru, případně spuštění útočníkova kódu.

2) **SQL injection** je zase oblíbená technika pro napadání databází podsunutím kódu přes neošetřený vstup (SQL dotaz).

3) **Trojský kůň** je samostatný program, který nese skryté nežádoucí funkce, o kterých uživatel neví a nesouhlasí s nimi.

4) **Virus** je program, který se šíří bez vědomí uživatelů a podle typů pak plní další pro uživatele nežádoucí funkce.

5) **Cross-site scripting (XSS)** je metoda narušení webových stránek, díky podsunutí útočníkových skriptů s cílem změnit vzhled nebo získat data o návštěvnících.

*[Lit **12**]*

5.1.1.1 Zero day exploit

Zero day attack (či útok nultého dne) značí v informatice typ útoku nebo vzniklé hrozby (exploitu), snažící se v PC využít zranitelnosti software, která ještě není známá a tím pádem na ni neexistuje. Nula v tomto případě neznačí číslo, ale skutečnost, že je uživatel ohrožen až do vydání opravy a nachází se proto stále v základním (nultém) postavení = zero day.

5.1.1.2 Ochrana

Za běžnou ochranu se považuje včasná instalace aktualizací od tvůrce napadnutelného software. Existuje několik technik k omezení zranitelnosti paměti, jako je uváděné přetečení na zásobníku a částečné ochranné mechanismy fungují i ve všech současných operačních systémech, jako Windows , Mac OS , Linux nebo Unix. Nicméně důležitou technikou pro předcházení hrozeb, jako je zero day exploit, je **whitelisting**. Whitelisting funguje na principu známých a spolehlivých aplikací (vytvořeného seznamu), a tak žádné neznámé aplikaci není povolen přístup.

5.2 Testy odepření služeb

5.2.1 Denial of Service (DoS)

DoS jsou útoky s cílem odepření fungování napadené služby. Jde o techniku přehlcení cílové služby nebo síťové infrastruktury, která zprostředkovává přenos dat mezi službou a jejím uživatelem. Často se také používá po jiných útocích, jako prostředek pro zahlazení stop.

5.2.1.1 DoS - ping útok z příkazové řádky

Jako první byl proveden naprosto jednoduchý útok pomocí příkazové řádky a příkazu ping. Spuštění probíhalo formou snadno šiřitelné dávky, která odeslala 100 ping požadavků na cílový webový server.

ping.bat

@echo off

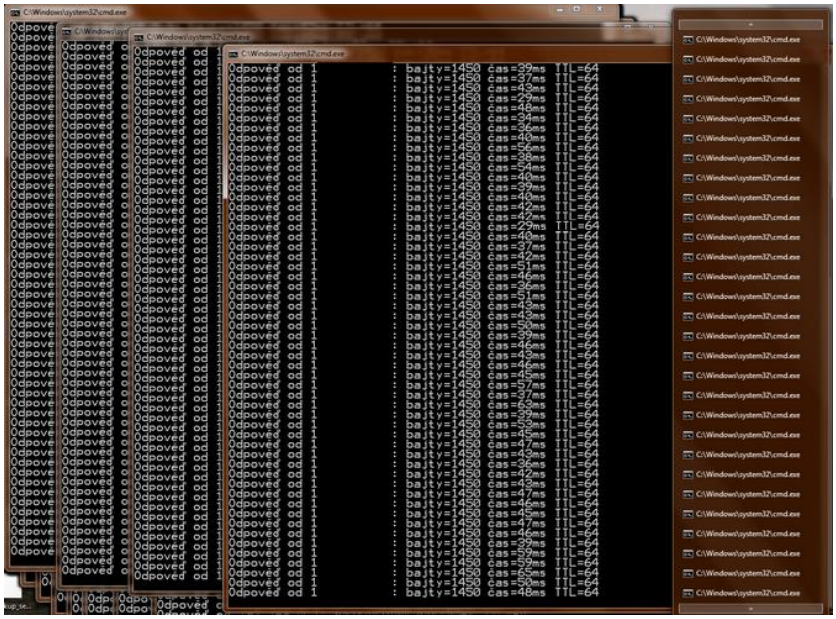
cls

echo 100x ping DDoS davka

for /L %%j in (1,1,100) do start cmd /c ping x.x.x.x -n 1000 -l 1450

exit

Tato dávka potom byla spuštěna na deseti počítačích a počet instancí této dávky na každém z nich byl 30.



Obrázek 19 – Ping útok – „autor“

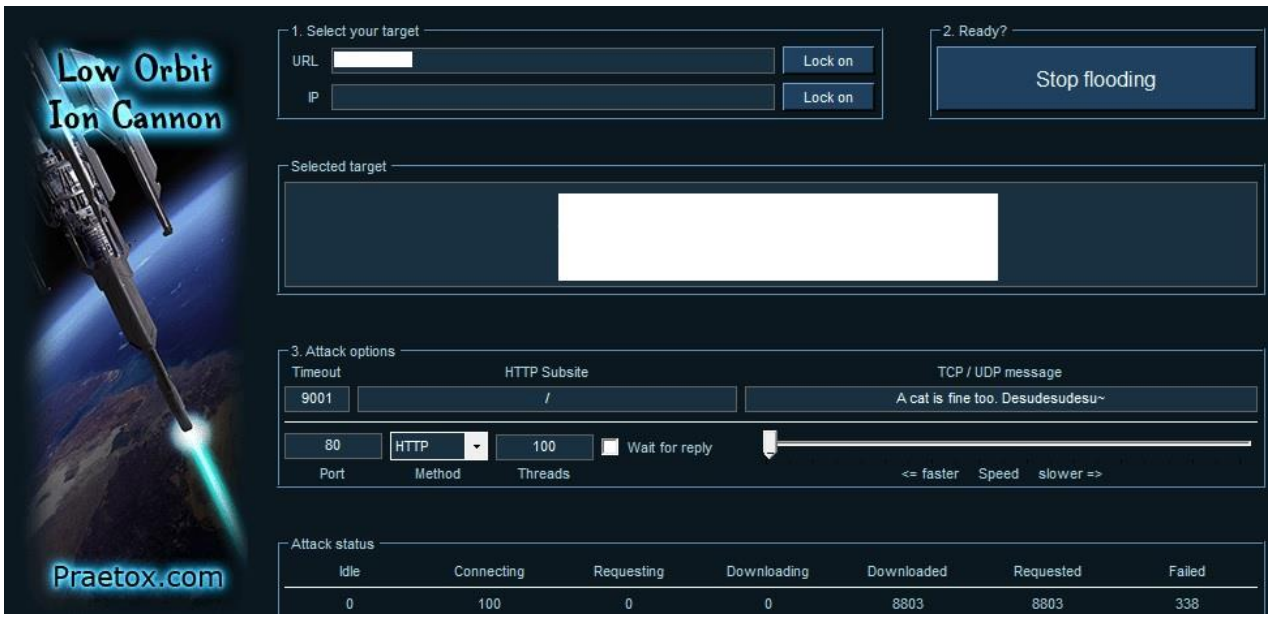
Bohužel, jak jsem tušil, toto služby webového serveru měřitelným způsobem nenarušilo

5.2.1.2 DDoS útok

Jelikož první metoda DoS nevyšla, přikročil jsem k použití programu LOIC (Low Orbit Ion Canon), který stojí za mnoha velkými a úspěšnými DDoS útoky. Jedná se o open source projekt primárně určený k síťovým stress testům. Dokáže posílat požadavky nastavitelnou rychlostí v několika stovkách vláken, a krom standartních testováni TCP portu umí zahltit i UDP porty a skrz HTTP požadavky také web server.

Při testování jsem zkoušel variabilní počet vláken a rychlost. Došel jsem k závěru, že pro „útočící“ PC je optimální nastavit zhruba 100 vláken maximální rychlostí – při vyšším počtu již měl útočící PC problémy s připojením k internetu a s metodou útočení formou HTTP požadavků.

Již při útoku z prvního PC se reakce firemního webu neuvěřitelně propadly někam do pásma 5-20 s čekání na odpovědi. Po spuštění útoku z třetího PC již došlo k cílenému efektu a firemní web byl kompletně nepřístupný.



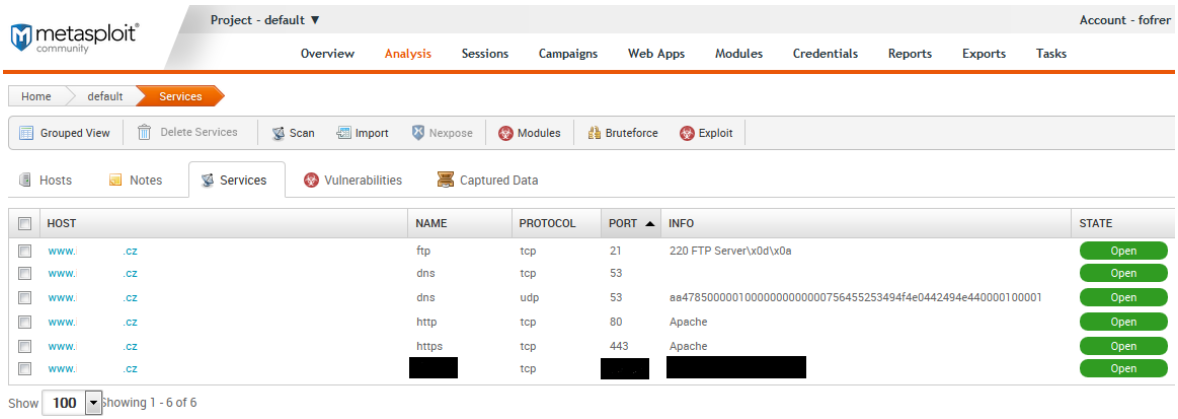
Obrázek 20 – LOIC DDoS útok – „autor“

5.3 Testy vnější a vnitřní zranitelnosti

5.3.1 Metasploit – testování zranitelností

Metasploit je softwarový bezpečnostní framework se zaměřením na penetrační testování. Obsahuje kvalitní a často aktualizovanou databázi expoitů. První verze vyšla v roce 2004 jako volně šiřitelný program, nicméně současná verze 4 už je plně komerční záležitost a volná verze je značně omezena.

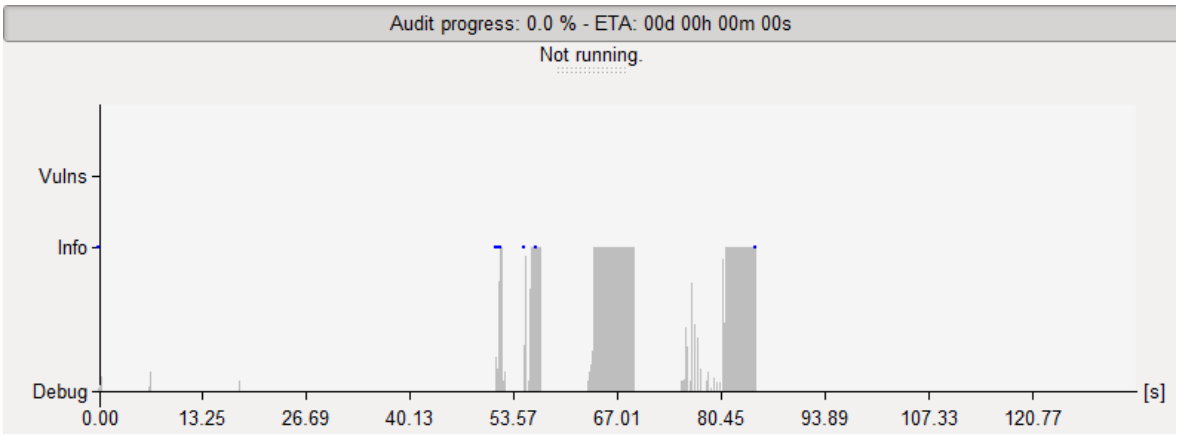
Pomocí tohoto programu (GUI verze se ovládá přes webový prohlížeč) jsem otestoval firemní síť a servery z venku i zevnitř. Nástroj kromě otevřených portů nedetekoval žádná rizika, což je dobré, nicméně kromě základního scanu v této volné verzi nic neposkytuje.



Obrázek 21 – Metasploit výsledky – „autor“

5.3.2 W3AF – test exploitů webových aplikací

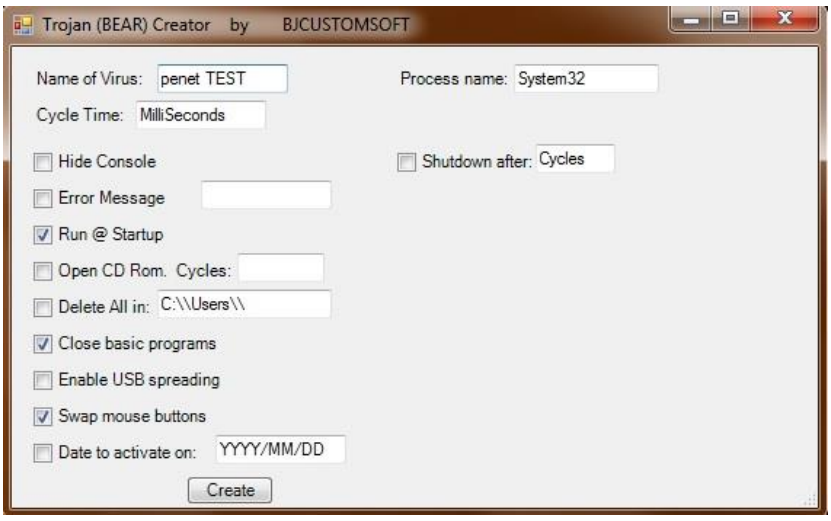
Jelikož minulý framework byl vzhledem k neplacené verzi značně zredukován, přistoupil jsem k testu ještě pomocí dalšího oblíbeného nástroje, a tím je scanovací framework W3AF, který se specializuje na weby a webové aplikace. Tento program nabízí auditorům různé techniky a jejich kombinace. Já jsem zvolil testování podle metodiky OWASP (Open Web Application Security Project – komunita bezpečnostních odborníků, se zájmem o tvorbu důvěryhodných webových aplikací), nicméně, jak je vidět z následujícího obrázku, žádné slabiny se nepodařilo najít ani v tomto případě.



Obrázek 22 – analýza W3AF – „autor“

5.3.3 Test virového zabezpečení

Dalším zvoleným testem je zkouška reakcí antivirových programů na pokus o průnik viru do vnitřní sítě. Jelikož není volně k dispozici neznámý nebezpečný kód (což je z podstaty věci logické), bylo třeba použít nějaký volně dostupný, případně ho modifikovat. Pro tento účel byl použit vir **Win32.Polip.a,** získaný ze stránky tuts4you.com. Dále byl vygenerován jednoduchý „trojský kůň“ pomocí programu Trojan Creator. („http://sourceforge.net/projects/virusgeneratort/“) V prvním případě se jednalo o zkomprimovaný soubor v příloze emailu a trojan byl zase nainstalován jako automaticky spouštěný soubor na USB flash disk a připojen do pracovního PC.



Obrázek 23 – Trojan Creator – „autor“

Výsledky tohoto testu byly podle očekávání bezvadné. Ochrana emailu závadnou přílohu ihned smazala a antivirový program na PC rychle detekoval a zablokoval automaticky spouštěný proces na pozadí i přesto, že ho neznal. Přesto tyto výsledky se nesmí ochrana souborů nijak podcenit, jelikož dle proběhlého bezpečnostního incidentu se v minulosti přes mailovou ochranu dostal vir (respektive ransomware) typu Cryptolocker a infikoval několik pracovních PC.

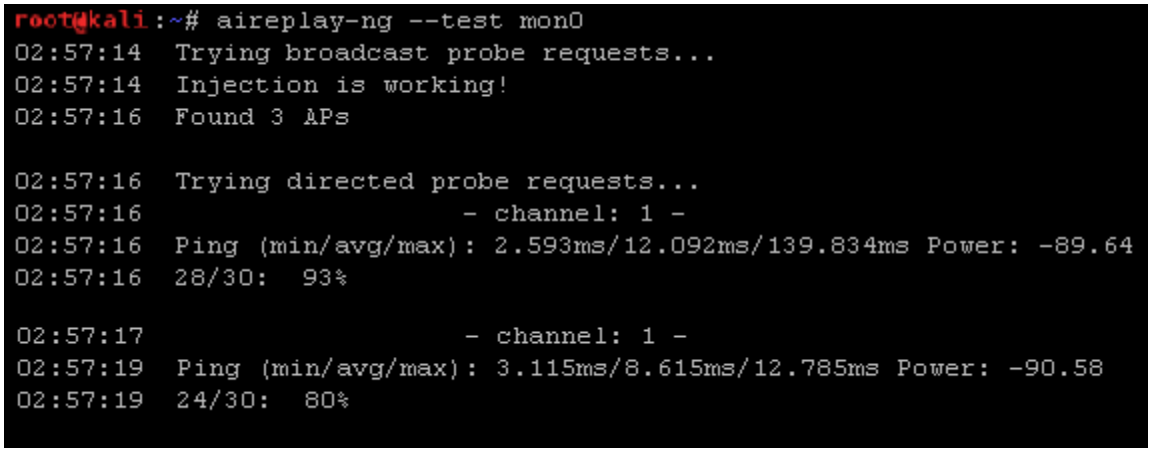
5.4 Testy síťového zabezpečení

5.4.1 Test bezdátové sítě – hackování Wifi

Jak již bylo zmíněno, v zasedací místnosti se nachází bezdrátová síť, která je pomocí jiné adresace oddělena od zbytku sítě a má primárně sloužit jen jako přístup k internetu. Pro připojení uživatel potřebuje heslo, které se každý týden mění, ale většinou je tvořeno jednoduchým slovem. Pro test penetrace zabezpečení bezdrátové sítě využijeme balíku softwaru Aircrack ve verzi 1.2, který bude ovládán z live distribuce Kali Linux (distribuce pro testery / hackery). Pro test je potřeba mít některý z podporovaných wifi chipsetů – v tomto případě Realtek RTL 8187.

5.4.1.1 Útok na WPA PSK

K připojení k síti bez znalosti hesla potřebujeme nejprve odchytit tzv. handshake – jedná se o techniku autentizace klientů k vysílači, která se vysílá při iniciaci spojení. Čekání na tuto situaci může trvat dlouho, a proto to lze urychlit použitím programu aireplay (z balíku Aircrack), krerý se snaží vybraný cíl pro vysílač deautentizovat a vyvolat novou autentizaci pomocí handshaku, čehož dosahuje pomocí speciálních síťových deauth paketů.



Obrázek 24 – Aircrack Injection – „autor“

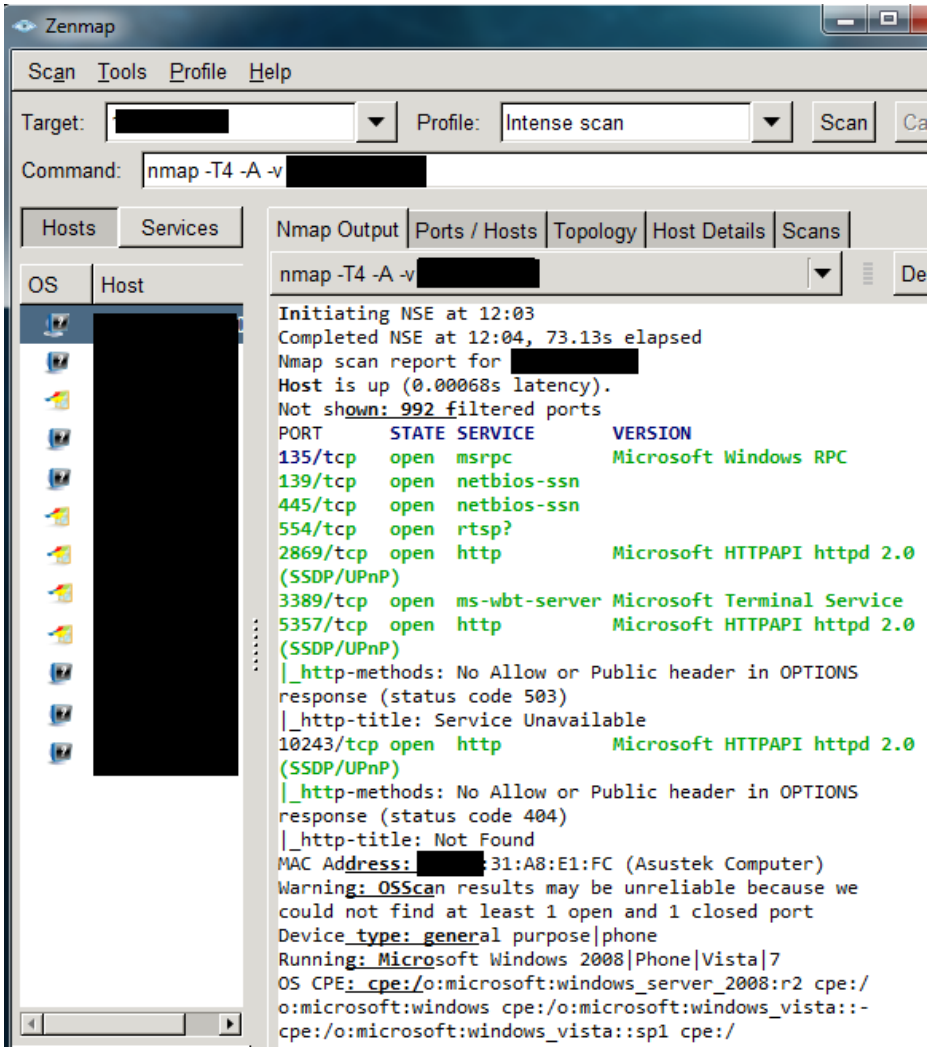
Po odchycení handshake paketů zbývá prolomení hesla a to se dělá tzv. bruteforce metodou s pomocí slovníku – porovnává se řetězec znaků s možnými kombinacemi ze slovníku. Úspěšnost tedy záleží na rozsáhlosti slovníku a čas na výkonu hardware, kde to provádíme. V případě dlouhých hesel se tedy složitost a trvání výpočtu může dostat do řádů měsíců a let. V našem případě bylo do půl hodiny nalezeno řešení (pomocí slovníku z „www.openwall.com/passwords/wordlists“), se kterým se lze připojit do sítě.

5.4.1.2 Průnik do hlavní sítě

Po úspěšném přihlášení do sítě je pomocí z DHCP serveru přidělena adresa, ze které je opravdu vnitřní síť nepřístupná, nelze se připojit k ERP, ani k sdíleným SMB složkám. Ale snadno manuálně nastavím adaptéru IP i masku odpovídající vnitřní adresaci, čímž bez problému docílíme přístupu k výše zmíněným službám. V tomto bodě jsem si jist, že o problému všichni z IT oddělení ví, ale vzhledem k ulehčení práce to neřeší.

5.4.2 Skenování sítě pomocí Nmap

Dalším důležitým nástrojem je Nmap sloužící pro rozkrývání struktury datové sítě – tedy většinou po průniku do vnitřního perimetru, jako se povedlo v předchozí kapitole. Aktuálně se používá verze 6 s grafickou nadstavbou Zenmap, která umí spojovat jednotlivé logy dohromady a graficky vykreslit strukturu sítě, síťové prvky nebo počet skoků mezi jednotlivými PC.



Obrázek 25 – Zenmap výsledky – „autor“

Pomocí tohoto software jsem tedy snadno rozkryl síťovou strukturu, včetně informací, jako je použitý operační systém, výrobce síťové karty, otevřených portů, sdílených složek apod. V tomto případě se jedná o vlastnosti operačních systémů a nikoliv slabiny.

5.4.3 Shrnutí výsledků

Po provedení testů je možné objektivně prohlásit, že je firma snadným terčem útoku hackerů a celkové zabezpečení by mělo rychle posílit, než bude pozdě. Tedy mělo by se zde problémům předcházet a ne řešit až naléhavé problémy.

V této kapitole jsem představil nástroje, pomocí nichž můžeme ověřovat vlastní zabezpečení, ale také provádět samotné útoky. Z toho plyne, že některé nástroje jsou shodné pro útočníky i auditory, rozdílem v užívání je pouze úmysl uživatele.

5.5 Analýza rizik

Na základě popsaných prvků analýzy rizik jsem vytvořil tabulku, viz níže. Hodnocení je subjektivní z pohledu autora - auditora a nemusí plně odrážet skutečnost (obzvlášť co se ohodnocení a dopadu týče), vzhledem k tomu, že se na něm nepodílel nikdo z managementu firmy. Tato analýza nemá za cíl podrobně rozebrat celkovou situaci hrozeb této firmy, ale ukázkově a zahrnout již probrané a zjištěné problémy.

Aktivum	Hodnota stupnice 1-10	Hrozba	Zranitelnost	Pravděpodobnost incidentu v procentech %	Dopad stupnice 1-10	Opatření
Klienti	7	krádež seznamu	nedostaečná bezpečnostní politika	80	4	politika ochrany dat
Klienti	7	krádež seznamu	zranitelná bezdrátová síť	15	4	úplné oddělení bezdrátové sítě od vnitřní sítě
Databáze ERP	10	neúmyslná modifikace	nedostatečný zácvik zaměstnanců	50	8	pravidelné zálohování
Databáze ERP	10	úmyslná modifikace	nedostatečné zabezpečené databáze	10	10	pravidelné zálohování
Databáze ERP	10	přerušení komunikace poboček	přerušení kabelu nebo problémy ISP	40	5	záložní internetové připojení
Server	5	selhání hardware	stárnutí HW, náchylnost na prach	10	8	plán obměny hardware, pravidelná údržba
Server	5	selhání hardware	přehřátí	20	8	pravidelná údržba klimatizace
Server	5	úmyslná sabotáž nebo krádež	snadný přístup k hardware	5	8	umístění ve střeženém prostoru

Obrázek 26 – analýza rizik– „autor“

Aktivum	Hodnota stupnice 1-10	Hrozba	Zranitelnost	Pravděpodobnost incidentu v procentech %	Dopad stupnice 1-10	Opatření
Server	5	krádež hardware	snadný přístup k hardware	5	8	umístění ve střeženém prostoru
PC	3	zneužití zaměstnanci	snadné zjištění administrátorského o účtu	60	3	zakázat bootování z DVD a USB, nastavit v BIOSu heslo
PC	3	poškození virem	volnost nakládání s antivirovým programem	50	5	zabezpečit nastavení antivirového programu heslem
PC	3	prozrazení hesla	nedostaečná bezpečnostní politika	30	3	dodržování bezpečnostní politiky hesel
Data na FTP	2	prolomení ochrany	nedostatečná ochrana FTP	70	3	změna defaultního portu, sledování incidentů
Souhrnná data	10	neoprávněné vniknutí do sítě	špatně nakonfigurovaný a výkonný firewall	40	10	výměna firewallu a detailní konfigurace
Souhrnná data	10	požár	umístění serverů, záloh a archviu na jednom místě	10	10	pravidelné zálohování dat s umístěním sídlo (offsite copy)
Webová prezentace	4	nedostupnost služby	nedostatečná ochrana před DDoS útoky	25	3	zablokování na úrovni ISP

Obrázek 27 – analýza rizik– „autor“

5.6 SWOT analýza stavu IT

V tomto kroku provedu stručnou SWOT analýzu, což je univerzální analytická technika zaměřená na zhodnocení faktorů, ovlivňujících úspěšnost záměru. Hodnotí se jak vnitřní tak vnější faktory a dělí se na silné a slabé stránky.

V tomto případě je záměrem určení stavu IT oddělení.

Silné stránky	Slabé stránky
• Finanční zdroje • Zálohovací strategie • Kvalitní ERP systém • Kvalitní antivirová ochrana	• Lidské zdroje • Bezpečnostní politika • Absence strategie rozvoje IT • Zabezpečení bezdrátové sítě
Příležitosti	**Hrozby**
• Nedostatečná komunikace s vedením • Snadný posun kvality bezpečnosti • Uvedení do souladu s normou ISO 27000 • Zavedení ISMS	• Bezpečnostní rizika • Špatně definované procesy • Ztráta finančních zdrojů v souvislosti s úniky • Softwarové chyby

6 Navrhované změny

V této kapitole bude představen základ pro rozvoj sledovaného IT oddělení. Navrhovaná řešení jsou brána s ohledem na velikost firmy, jelikož menší firma nemá takové prostředky jako velké korporace. Návrhy týkající se zjištěných nedostatků jsou rozděleny do několika kategorií podle zaměření.

6.1 WAN

Z pohledu vnější sítě a komunikace přes ni bych navrhoval implementovat OpenVPN a veškerý provoz mezi pobočkami a hlavním serverem přesunout přes tuto zabezpečenou formu komunikace. Dále je naprosto nezbytné provést revizi nastavení firewallu, v lepším případě zakoupit nový router Cisco a provést novou konfiguraci s přizváním certifikovaného odborníka na tuto problematiku. Jako obranu proti DDoS útokům bych doporučil přenést část obrany na poskytovatele internetové konektivity, což se řeší blokováním opakujících se paketů již na serverech ISP, což znamená menší zátěž pro firemní server. Alternativním řešením by bylo převést celý web do cloudu, který má značnou škálovatelnost výkonu a konektivity a běžné DDoS útoky bez problému zvládne. Dále, jelikož neexistuje žádná varianta záložního připojení, bych doporučoval vybrat z místních poskytovatelů bezdrátového nebo mobilního připojení a přes vybraného ISP zřídit záložní konektivitu do internetu.

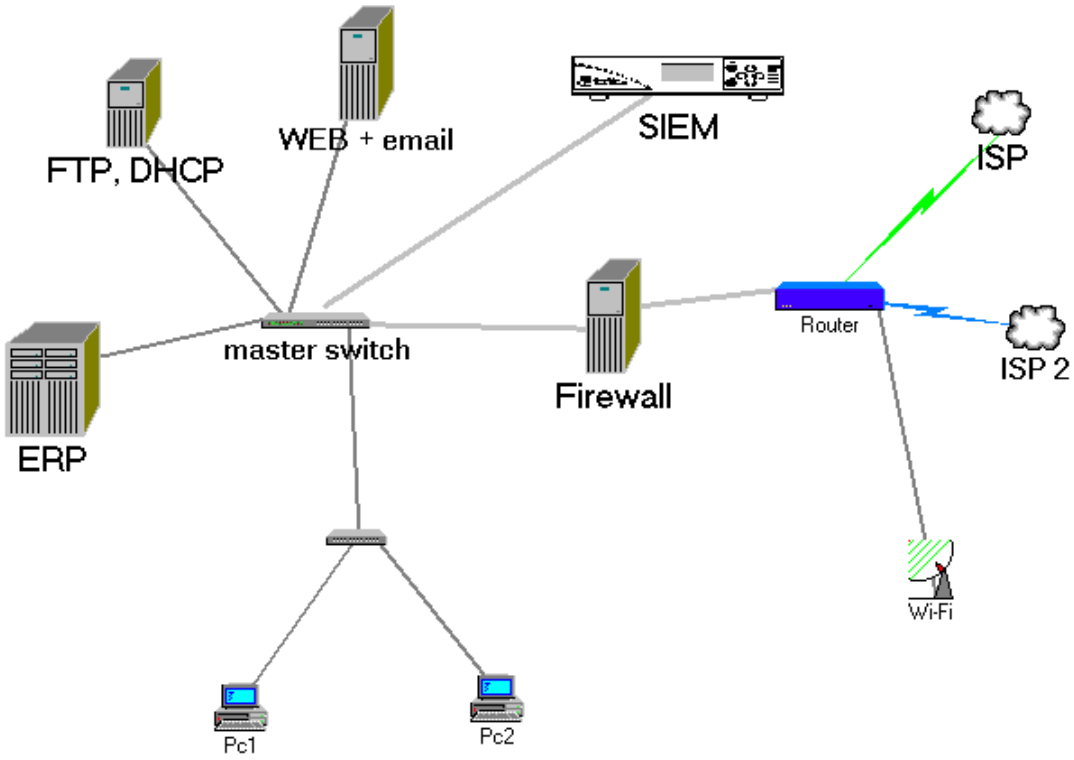
6.2 Vnitřní síť

Pro vnitřní síť bych doporučil v prvé řadě rozsegmentovat síť podle struktury firmy (nebo podle oddělení), aby si mezi odděleními navzájem neviděly na PC, a mezi jednotlivé podsítě postavit alespoň softwarový firewall. Jako stěžejní bych označil vyřešit slabiny bezdrátové wifi sítě, což může být dořešeno v zásadě dvojím způsobem

1) maximalizovat zabezpečení, použitím technik jako je WPA 2, skrytí SSID vysílače společně s MAC address filtrem a dlouhým složitým heslem

2) změnit strukturu sítě a bezdrátovou síť předřadit před firewall – naprosto bez přístupu do vnitřní sítě.

Vzhledem k charakteru využití této sítě mi přijde vhodnější řešení číslo dvě, jelikož se wifi často poskytuje hostům a prvním řešením by došlo ke značnému omezení tohoto benefitu. Navíc v případě napadení této sítě může útočník maximálně krást konektivitu do internetu. Vizualizaci, jak by to mohlo vypadat, nám zobrazuje následující obrázek:



Obrázek 28 – návrh změny infrastruktrury– „autor“

6.3 Technická místnost a její vybavení

Doporučení týkající se serverů a technické místnosti jsou brány z pohledu jak fyzické bezpečnosti tak datové a síťové bezpečnosti. Pro každou oblast uvedu u mého pohledu nejzásadnější změnu.

1) Je nutné posílit bezpečnost samotné místnosti, konkrétně nastavit systém řízení přístupů (vyměnit nebo programově rozšířit) na časové úseky, kdy je možné přistupovat do místnosti, logovat a sledovat frekvenci využití tohoto přístupu a v případě anomálií kontaktovat odpovědného pracovníka. Tento systém bych zavedl ještě v kombinaci s číselnou klávesnicí, kde by ke každé kartě musel být přiřazen správný číselný kód, čímž by se minimalizovalo riziko při ztrátě karty.

2) Je třeba dopracovat systém záloh, jejich sledování a uchovávání. Pro automatické sledování záloh bych doporučil open source software Nagios.

Zálohování jako takové bych rozšířil o typ offsite copy – tedy kopírování na vzdálené úložiště – například do cloudového úložiště.

3) Síťovou bezpečnost je třeba doplnit o nový server pro zpracovávání a hlídání vnitřní i vnější bezpečnosti typu SIEM (Security Information and Event Management) – který by ze všech serverů a sledovaných uzlů sbíral online data (logy) a okamžitě je vyhodnocoval. Je to zároveň skvělý prostředek ke kontrole dodržování bezpečnostní politiky. Doporučil bych produkt HP ArcSight, se kterým mám osobní zkušenost.

Obrázek 26 – Logo HP ArcSight– „http://www.tecnogaming.com/images/articulos/2013/07/hp-ArcSight-tecnogaming.jpg“

6.4 Uživatelská PC

V případě pracovních stanic bych doporučil jen několik časově i finančně nenáročných úprav nastavení. Jedná se o nastavení pevné doby do vypršení hesla na systémech Windows, dále navrhuji zabezpečit nastavení antivirového programu heslem. Jako další krok bych doporučil omezit bootování PC pouze ze systémového HDD, a to restriktivním nastavením BIOSu a jeho zabezpečení heslem.

Do budoucna by nebylo špatné uvažovat o kompletním šifrování HDD, což už přinese určitá omezení uživatelů. Dalším návrhem je vypnout lokální účty a nakonfigurovat síťové přihlašování – tím odpadne snadná zjistitelnost hesla (OPHcrack).

6.5 Bezpečnostní politika

Nejzásadnějším krokem k zajištění bezpečnosti by měla být tvorba celkové strategie IT oddělení, počínaje plánem rozvoje a určením výšky investic konče. Je nutné neprodleně začít pracovat na ucelené bezpečnostní politice a zapracovat ji do vnitřních směrnic. Politiku hesel zapracovat včetně způsobů kontroly a délku hesla prodloužit na minimálních 12 znaků. Celou koncepci bych doporučil pojmout ve smyslu normy ISO/IEC 27000 a po realizaci zažádat o provedení profesionálního auditu. Dále navrhuji vytvoření evidence hardwaru pro snadnější sledování záruk a stáří a řádné zdokumentování infrastruktury sítě. V novém pojetí bezpečnostní politiky je třeba se zamyslet nad aplikací některého IDS systému (intrusion detection system) pro aktivní zabezpečení sítě. Vybrané náměty bezpečnostní politiky jsem shrnul do několika bodů doporučeného postupu:

1) definovat základní procesy správy a údržby,

2) sestavit plán pravidelně údržby systému,

3) sestavit plán řešení poruchových stavu a havarijní plán,

4) stanovit jednoznačnou odpovědnost za servery, včetně kontrol systému,

5) stanovit odpovědnost za zálohování a nakládání se zálohami,

6) stanovit pravidla změn v systému a návazných aplikací.

7 Závěr

V teoretické části této diplomové práce byly objasněny techniky a metody, které vedou k systematickému vedení IT oddělení. V obecné rovině byly představeny aktuální normy a zákony, které je dobré sledovat, a podle nich přizpůsobit řízení podnikového IT. Ve zkratce byl nastíněn vznik a význam auditu a institucí, jež umožňují rozvoj tohoto odvětví. Jako další zásadní bod byla prezentována nutnost řídit bezpečnost informací a zapracovat ji do bezpečnostní politiky podniku. V teoretické rovině byly popsány metodiky provádění penetračních testů, které byly následně v praktické části použity společně s vybraným nástrojem.

Cílem praktických testů bylo dokázat možnost průniku zabezpečením organizace technikami používanými hackery k útokům na interní počítačové systémy. Bez problému bylo překonáno zabezpečení bezdrátové sítě a proveden průzkum sítě za ní. Povedlo se dokázat, že zabezpečení zvolené firmy je na velmi špatné úrovni.

Po provedení testů je možné objektivně prohlásit, že prověřovaná instituce je snadným terčem pro útok hackerů a celkové zabezpečení by mělo být zásadně posíleno, jinak bude bezpečnost systémů v permanentním ohrožení. Zároveň je nutné bezpečnostním problémům předcházet, nikoli řešit až naléhavé problémy. Provedená bezpečnostní prověrka odhalila několik zásadních nedostatků. Jako klíčový nedostatek byla označena absence promyšleného řízení IT a s tím spojená bezpečnostní politika. V závěru praktické části byl navržen plán změn s návrhem konkrétních protiopatření, včetně návrhu na přepracování systému řízení bezpečnosti do shody s normou ISO/IEC 27000 a doporučena následná certifikace. Přínosem pro testovaný podnik byl nový a nezaujatý náhled na stav bezpečnosti IT a představení nového směru, jak ji vnímat a zajišťovat. Z těchto závěrů byl vedoucí IT oddělení testovaného podniku překvapen, očekával lepší hodnocení stavu bezpečnosti, nicméně o leckteré potencionální hrozbě věděl, tedy mohl být výsledný stav o mnoho lepší.

8 Seznam použitých zdrojů

1) SVATÁ, Vlasta. Audit informačního systému. 2. vyd. Praha: Professional Publishing, 2012, 219 s. ISBN 9788074311062.

2) HARRIS, Shon. Manuál hackera. 1. vyd. Praha: Grada, 2008, 399 s. Hacking (Grada). ISBN 9788024713465.

3) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 9788086946887.

4) SENFT, Sandra. Information technology control and audit. 4th ed. Boca Raton, FL: CRC Press, 2013, 740 s. ISBN 9781439893203.

5) LOCKHART, Andrew. Bezpečnost sítí na maximum. Vyd. 1. Překlad Jiří Veselský. Brno: CP Books, 2005, 276 s. ISBN 8025108058.

6) MAISNER, Martin. Základy softwarového práva. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2011, xv, 339 s. Právní monografie. ISBN 9788073576387.

7) Kybernetickyzakon.cz. [online]. 2015. vyd. [cit. 2015-03-04]. Dostupné z: http://www.kybernetickyzakon.cz/

8) Businessinfo.cz. [online]. 2015. vyd. [cit. 2015-03-04]. Dostupné z: http://www.businessinfo.cz/cs/clanky/novy-kyberneticky-zakon-jak-se-pripravit-59504.html

9) ISO.cz. [online]. [cit. 2015-03-04]. Dostupné z: http://www.iso.cz/?page_id=46

10) RiskAnalysisConsultants. [online]. [cit. 2015-03-04]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799

11) AEC - Bezpečnostní politika organizace. [online]. [cit. 2015-03-04]. Dostupné z: http://www.aec.cz/cz/sluzby/bezpecnostni-politika-organizaceCZ/BS7799

12) Computerworld. [online]. [cit. 2015-03-04]. Dostupné z: http://computerworld.cz/securityworld/zranitelnost-desetileti-aneb-kdyz-pretece-zasobnik-46243

13) Trustica. [online]. [cit. 2015-03-04]. Dostupné z: http://www.trustica.cz/penetracni-testy/

14) ISVS. [online]. [cit. 2015-03-04]. Dostupné z: ww.isvs.cz/penetracni-testy-jak-se-provadeji-a-k-cemu-jsou-1-dil/

15) ICT security. [online]. [cit. 2015-03-04]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/bezpecnostni-audit-krok-za-krokem.html

16) System online. [online]. [cit. 2015-03-04]. Dostupné z: http://www.systemonline.cz/it-security/priority-bezpecnostni-politiky-v-malych-a-strednich-firmach.htm

9 Přílohy

9.1 Seznam použitých zkratek

AES - Advanced Encryption Standard - standart pokročilého šifrování
BIOS - Basic Input-Output Systém - firmware pro PC
DHCP - Dynamic Host Configuration Protocol – protokol pro automatické přidělování IP adres
FTP - File Transfer Protocol - protokol pro přenos souborů mezi počítači
GNU LGPL - Library General Public License - licence svobodného software, jež je možno linkovat
GUI - Graphical User Interface - grafické uživatelské rozhraní
HDD - Hard Disk Drive - pevný disk
HTTP - Hypertext Transfer Protocol - protokol určený pro výměnu hypertextových dokumentů
HTTPS - Hypertext Transfer Protocol Secure - nadstavba síťového protokolu HTTP
IP adresa - virtuální adresa, které jednoznačně identifikuje síťové rozhraní v počítačové síti
ISP - Internet service provider - poskytovatel připojení
PC - Personal Computer - osobní počítač
LAN - Local Area Network - místní síť
MAC adresa - Media Access Control – MAC adresa je jedinečný identifikátor síťového zařízení
Malware - Malicious software - program sloužící k vniknutí do PC systému

NAS - Network Attached Storage - datové úložiště na síťi
POP3 - Post Office Protocol - protokol pro stahování emailových zpráv
RAID - Redundant Array of Independent Disks - vícenásobné diskové pole
RAM - Random Access Memory
Ransomware - druh malware, požadující výkupné za zpřístupnění PC
Spyware - program odeílající data z PC bez vědomí majitele
SQL - Structured Query Language - strukturovaný dotazovací jazyk databází
SSL - Secure Sockets Layer - zabezpečená transportní síťová vrstva
USB - Universal Serial Bus - standartizovaná sběrnice pro periferie počítače
USB flash disk - malé paměťové médium do USB
VPN - Virtual Private Network - zabezpečená datová síť nad standartní síťí
WAN - Wide Area Network - geograficky rozhlehlá datová síť - nejčastěji internet
WLAN (WIFI) -Wireless LAN - bezdrátová počítačová síť