Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Síťová bezpečnost - Standardy

Bc. Miroslav Tax

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Miroslav Tax

obor Systémové inženýrství

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Síťová bezpečnost – Standardy**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Bezpečnostní standardy - teorie a vývoj
4. Srovnání a použití bezpečnostních standardů
5. Závěr
6. Seznam použitých zdrojů
7. Přílohy

Rozsah hlavní textové části: 60 - 80 stran

Doporučené zdroje:

Thomas M. Thomas: Zabezpečení počítačových sítí,CP Books a.s. ,Brno 2005, ISBN 80-251-0417-6

Libor Dostálek a kolektiv: Velký průvodce protokoly TCP/IP bezpečnost,CP Books a.s.,Brno 2003, ISBN 80-7226-849-X

Tomáš Doseděl: Počítačová bezpečnost a ochrana dat,CP Books a.s.,Brno 2004, ISBN 80-251-0106-1

Stephen Northcutt a kolektiv: Bezpečnost počítačových sítí,CP Books a.s., Brno 2005, ISBN 80-251-0697-7

Vedoucí diplomové práce: **Ing. Martin Papík**

Termín odevzdání diplomové práce: duben 2011

L.S.

.....	.....
Vedoucí katedry	Děkan

V Praze dne: 3. 2. 2010

---

lováno děkanátem PEF pod č.j.: KII-067-10D

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Síťová bezpečnost - Standardy" 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 8.4.2011 _____

Poděkování

Rád bych touto cestou poděkoval ing. Martinu Papíkovi, Ph.D., za odborné vedení mé práce, cenné náměty a podnětné připomínky, které mi poskytoval v celém průběhu zpracovávání této diplomové práce.

Síťová bezpečnost - Standardy

Network security - Standards

Souhrn

V této diplomové práci je přiblížena problematika síťové bezpečnosti, a zároveň je poukazováno na existenci základních principů z oblasti bezpečnosti počítačových sítí. Dále je zde ukázána problematika dokumentu bezpečnostní politiky, včetně přiblížení jeho obsahové stránky. Značná část této práce se zabývá i mezinárodními kriterii pro hodnocení bezpečnosti informační techniky. Je zde nastíněn historický vývoj a základní principy těchto kriterií, včetně ukázání implementace v rámci české státní normy.

V další části této práce byla zkoumána znalost a využívání vybraných standardů z oblasti bezpečnosti výpočetní techniky a použití dokumentu bezpečnostní politiky v rámci organizací. Poslední část práce se věnuje praktické ukázce bezpečnostního průzkumu sítě LAN s využitím síťového skeneru Nessus. Následně jsou popsány zjištěné nedostatky v rámci zabezpečení této sítě a navrženy opatření pro jejich eliminaci.

Klíčová slova: Počítačové sítě, Informační bezpečnost, Síťová bezpečnost, Bezpečnostní politika, Standardy informační techniky, Kriteria hodnocení informační bezpečnosti, Síťový skener Nessus.

Síťová bezpečnost - Standardy

Network security – Standards

Summary

In this thesis is presented problems of network security, and is referred to the existence of the fundamental principles of security computer networks. Furthermore, there is a shown a document of security policies, including presentation of his content. Much of this thesis deals with the international criteria for evaluating security of information technology. It also outlines the historical development and basic principles of these criteria, including showing the implementation of the Czech national standards.

In the next part of this thesis were examined knowledge and use of selected standards in the field of computer security and use document of security policies within organizations. The last part is the practical demonstration LAN security survey with using the network scanner Nessus. Later are described the shortcomings in the security of the network and proposed measures for their elimination.

Keywords: Computer networks, Information Security, Network security, Security policy, Information Technology Standards, Information Security Evaluation Criteria, Network scanner Nessus.

Obsah

1. Úvod

Síťová bezpečnost je v současné době specifická problematika, která se už dostala do popředí zájmu všech velkých, středních i menších organizací. Velký důraz se na ní začíná klást ale i z řad obyčejných uživatelů či jednotlivců. Vzhledem k velmi rychlému tempu rozvoje, které počítačové sítě zaznamenali zejména na konci 20. století, je důvod zřejmý. Organizace i jednotlivci začali využívat velké spektrum služeb založených právě na technologii počítačových sítí, a začali se tak zákonitě zajímat i o problematiku bezpečnosti. Spolu se vznikem a dynamickým rozvojem Internetu, kdy se začali ve větším rozsahu využívat i velmi choulostivé služby z hlediska síťové bezpečnosti, se začali klást na zabezpečení relativně vysoké, ale adekvátní požadavky. Příkladem těchto služeb může být internetové bankovnictví, pořádání on-line aukcí, či provozování internetového obchodu nebo i využívání datových schránek. Výčet těchto služeb ale zdaleka není konečný, a téměř neustále se rozrůstá. Jak je tedy vidět, potřeba síťové bezpečnosti roste, a s ní se následně pojí i rostoucí potřeba standardizace v rámci dané problematiky.

Téměř každá lidská činnost, která je vykonávána ve větším rozsahu, by měla mít daný soubor pravidel. Tento soubor pravidel by měl být v jednotné podobě, a zároveň by měl být i v adekvátním rozsahu. Právě pro tyto účely, tedy pro sepsání a sjednocení přístupu k dané problematice, se využívá již zmíněné standardizace. V oblasti bezpečnosti informační techniky se jedná o velmi důležitou iniciativu standardizačních organizací. Pomocí standardizace je například uživatelovi prezentována úroveň bezpečnosti daného informačního systému či libovolného produktu, nebo mu je poskytnuta garance adekvátního přístupu k řešení problematiky v rámci vývojových nebo dodavatelských společností. Uživatel, respektive daná organizace, tak získává záruku určité garance kvality a s tím spojenou i úroveň bezpečnosti. Mezi další nesporné výhody standardizace v rámci bezpečnosti informační techniky, spadá také definování vlastních a objektivních ukazatelů či kriterií, které jsou využívány právě pro potřeby hodnocení úrovně bezpečnosti. Tyto kriteria mají široký rozsah aplikace, napříč téměř celou problematikou informačních technologií, jak z pohledu softwaru, tak i z hlediska hardwarového vybavení.

2. Cíl práce a metodika

2.1 Cíl práce

Snahou a zároveň prvním cílem této diplomové práce, je seznámit čtenáře s problematikou síťové bezpečnosti a základními principy zabezpečení počítačových sítí. Následně ho i seznámit s mezinárodními kriterii pro hodnocení bezpečnosti prvků informační techniky a poukázat na význam dokumentu bezpečnostní politiky, který představuje základní prvek informační bezpečnosti v rámci kterékoliv organizace.

Druhým cílem této diplomové práce je provedení průzkumu stavu informační bezpečnosti a dalších souvisejících znalostí. Především se budeme snažit zjistit a posoudit využívání dokumentu bezpečnostní politiky a standardů informační techniky v praxi. K tomuto účelu byla zvolena metoda kvantitavního výzkumu a bude tedy provedeno dotazníkové šetření.

Poslední cíl této práce spočívá v demonstraci a ukázce základního auditu či průzkumu stavu síťové bezpečnosti již konkrétní počítačové sítě menšího rozsahu. Tento průzkum má poukázat na možná bezpečnostní rizika, kterým tyto sítě musí čelit a případně i doporučit opatření pro jejich možnou eliminaci.

2.2 Metodika

První stanovený cíl této diplomové práce spočívá v prezentaci již existujících odborných znalostí, a jeho splnění se tedy předpokládá v rámci části literární rešerše.

Pro potřeby dosažení druhého cíle byl sestaven dotazník, který je obsažen v rámci přílohy této práce. Pro jeho potřeby byly identifikovány dvě cílové skupiny respondentů. První skupina představovala respondenty z řad IT odborníků, a druhá skupina zahrnovala respondenty již bez nutných odborných znalostí z oblasti informační techniky či počítačových sítí. Pro oslovení obou těchto skupin bylo využito dvou prostředků. První prostředkem byla emailová korespondence, pomocí níž bylo osloveno padesát náhodně vybraných organizací v rámci odvětví informačních technologií či informačních systému. Tento prostředek měl za cíl získat především respondenty z řad IT odborníků. Druhým využitým prostředkem bylo

zveřejnění přiloženého dotazníku na internetových stránkách. Tento prostředek měl za cíl oslovit spíše respondenty bez odborných znalostí. Získané odpovědi v rámci obou prostředků byly následně shromážděny a vyhodnoceny v programu MS Excel. V rámci dotazníku bylo položeno několik segmentačních otázek, na základě kterých byly jednotlivé skupiny respondentů odděleny, přičemž v rámci obou skupin byly sledovány jiné otázky, respektive odpovědi na tyto otázky. Takto získaná data byla následně vyhodnocena a prezentována pomocí grafů.

Třetí cíl této práce spočíval v provedení základního síťového auditu. Pro tento účel byl vybrán softwarový nástroj v podobě síťového skeneru Nessus. Tento skener umožňuje v rámci počítačové sítě provést jednotlivé bezpečnostní testy v rámci obsažených modulů a následně tak identifikovat případná slabá místa. Jelikož je možné tento software zdarma stáhnout z internetových stránek tenable.com a uvést do provozu i na počítači který je již součástí testované a posuzované sítě při zachování dobré vypovídající hodnoty testů, nebylo nutné zapojovat do cílové sítě žádný další počítač. Testování tedy proběhlo přímo s využitím jednoho počítače, který již byl součástí posuzované sítě.

3. Bezpečnostní standardy – teorie a vývoj

V následujících kapitolách budou přiblíženy základy počítačových sítí, konkrétně jejich obecná struktura, včetně referenčního modelu OSI/ISO. Z tohoto modelu vychází základní nástroj pro síťovou komunikaci dnešní doby, a to standard v podobě rodiny protokolů TCP/IP. Dále pak budou uvedeny základní bezpečnostní principy, které jsou využívané v rámci síťové bezpečnosti, a poměrně velký prostor zde bude věnován i dokumentu bezpečností politiky. Tento dokument je považován za jeden ze základních stavebních prvků informační bezpečnosti v rámci jakékoliv organizace. Poslední část této kapitoly je věnována standardům týkajících se mezinárodních kriterií hodnocení úrovně bezpečnosti informačních systémů, zejména jejich historickému vývoji a obsahu, včetně vysvětlení vlivu jejich existence na mezinárodní normu ISO/IEC 15408.

3.1 Počítačové sítě

Počítačové sítě jsou velmi důležitým nástrojem, bez kterého je velmi obtížné si představit dnešní moderní společnost v takové podobě, ve které jí známe. Se vznikem a především s rozšířením počítačových sítí na konci minulého století, se podstatným způsobem změnil pohled na svět. Usnadnila se komunikace, ale také i sdílení prostředků a dat na velké vzdálenosti, čehož následně začaly využívat jednotlivé prvky počítačových a komunikačních sítí. Následně tak došlo k obrovskému rozvoji těchto sítí jako celku.

Pod pojmem počítačová síť se v základním pojetí rozumí spojení dvou či více počítačů takovým způsobem, který jim umožňuje sdílet své prostředky. Síť je možné chápat také jako spojení určitého hardwaru, softwaru a kabelů (vodičů), které společně umožňují vzájemnou komunikaci různých počítačových zařízení. Hlavním cílem každé počítačové sítě, je tedy umožnit vzájemnou komunikaci jednotlivých prvků, které jsou v dané síti obsaženy [5,1].

Nejdříve se využívaly sítě pouze malého rozsahu, až následně se společně s rozvojem informační technologie stávaly realitou stále větší a větší sítě. Velikost sítě, včetně počtu počítačů, byla právě omezována dostupnou technologií. Dnes už je možné dosáhnout podstatně větších sítí. Pro potřeby rozdělování základních typů sítí vzhledem k jejich rozsahu vzniklo následující dělení [5,17]:

- **LAN** (*Local Area Network*) – Sítě nejmenšího rozsahu, jejíž počítače od sebe nejsou příliš vzdáleny. Často využívané v rámci jednoho podlaží budovy, či menší firmy. Velmi často jsou využity také v rámci jednotlivých domácností, které obsahují více počítačů či síťových prvků. Většinou mají tyto sítě soukromý charakter.

- **MAN** (*Metropolitan Area Network*) – Sítě středního rozsahu, které jsou využívaný pro komunikaci mezi vzdálenými pracovišti. Umožňují rozšíření působnosti lokálních sítí a zvýšení počtu připojených stanic. Tento typ sítí muže být jak soukromého, tak i veřejného charakteru.

- **WAN** (*Wide Area Network*) – Nejrozsáhlejší počítačové sítě, které vynikají geografickým dosahem v rámci různých měst, států či i kontinentů. Tyto sítě jsou ve většině případů veřejného charakteru. V současné době je nejznámějším typem sítě WAN globální síť Internet.

Pokud se má tato diplomová práce zabývat bezpečnostní počítačových sítí, je nutné se zmínit o již uvedené síti Internet. Tato síť je v dnešní době globálního charakteru, a obsahuje vzájemně propojené počítače napříč všemi kontinenty. Tyto počítače jsou fyzicky propojené pomocí síťových kabelů a mnoha dalších technických prostředků a nástrojů, které v rámci komunikace využívají stanovená pravidla. Tyto pravidla jsou definovány v rámci standardu TCP/IP, kterému jsou věnovány následující podkapitoly.

Základní navržené principy fungování byly ale poměrně jednoduché. Vlastní síť byla v každém okamžiku během navrhování považována za nespolehlivou, a proto musela být navržena takovým způsobem, aby svou nespolehlivost dokázala překonat. Tento předpoklad má opodstatnění v tehdejších požadavcích na armádní bezpečnost, v rámci které měla být původně síť používána. Pokud by došlo k napadení území USA, bylo předpokládáno, že dojde i k napadení komunikace a komunikačních tras mezi jednotlivými státy, městy a vojenskými základnami. Komunikační síť by mohla být libovolně chráněna a zajištěna, ale v případě napadení center komunikace atomovými zbraněmi, které se rovněž předpokládalo, by došlo k jejímu téměř totálnímu zničení. Proto byl vysloven požadavek na takovou síť, které by této hrozbě dokázala úspěšně čelit. V rámci tedy těchto požadavku, začali být všechny uzly

v rámci budované sítě považovány za rovnocenné. Každý uzel už navíc obsahoval i vlastní autoritu pro vytváření, předávání a i přijímání datových paketů. Data zde tedy měla vycházet z libovolného zdrojového místa, a každý vyslaný paket měl být dále už nezávisle směrován. Měl si tedy razit svoji vlastní cestu sítí, nezávisle na paketech ostatních. Konkrétní cesta, po které bude paket sítí procházet, již nebyla v této koncepci důležitá. Důležitý zde byl pouze výsledek, zda daný paket dorazil či nikoliv. Data uskupovaná v paketech měla být tedy v rámci této sítě směrována přes jednotlivé uzly do té doby, dokud nedorazí na místo určení. Takovýto způsob datové komunikace sice není příliš efektivní, ale zato je extremně robustní. I v případě vyřazení poměrně velké části takovéto sítě mohla datová komunikace pokračovat. Ovšem za předpokladu že existovala minimálně jedna funkční trasa k danému cíli [1].

3.1.1 Referenční model OSI/ISO

Pro dostatečný přehled, který je nutný pro zajištění dobré míry zabezpečení, je většinou nutné znát princip fungování. Základy funkčnosti pro naši problematiku, tedy pro počítačové sítě, spočívají v protokolech. Protokol je v obecné rovině množina pravidel určujících syntaxi, na základě které se přiřazují významy pro jednotlivé zprávy v systému. Základním protokolem pro síťovou komunikaci je v současné době protokol TCP/IP. Tento protokol, respektive rodina protokolů, částečně vychází z referenčního modelu OSI/ISO. Tento model vypracovala organizace ISO a v roce 1984 byl přijat jako mezinárodní standart. Samotný model OSI/ISO nebyl žádný protokol pro praktické použití, ale spíše poskytoval pouze základní informace a principy funkčnosti pro další rozvoj. Vzhledem ke složitosti problematiky, je v tomto modelu síťová komunikace rozdělena do jednotlivých vrstev. Tyto vrstvy znázorňují strukturu přenosu dat. Každá vrstva zde využívá služby vrstvy nižší úrovně a zároveň poskytuje své služby vrstvě vyšší. Tento referenční model obsahuje všeobecné principy funkčnosti sedmivrstvé síťové architektury. Neobsahuje tedy ani žádné konkrétní protokoly [3].

Referenční model OSI/OSI tedy obsahuje následující sedm vrstev:

1. ***Fyzická vrstva***
2. ***Spojová vrstva***
3. ***Síťová vrstva***
4. ***Transportní vrstva***
5. ***Relační vrstva***
6. ***Prezentační vrstva***
7. ***Aplikační vrstva***

Fyzická vrstva (*physical layer*) je 1. vrstva modelu OSI/ISO. Jedná se o základní vrstvu, která podporuje a zabezpečuje fyzicky probíhající síťovou komunikaci. Udržuje a aktivuje fyzické spoje. Obsahuje také různá specifická nastavení portů či kabelů a definuje různé technické specifika dalších přídavných zařízení.

Spojová vrstva (*data link layer*) zajišťuje spojení mezi dvěma body. Stará se o parametry, jejich nastavení a o dodržování vymezeného rámce. Detekuje a opravuje chyby na fyzické vrstvě a zajišťuje rozdělování fyzických adres.

Síťová vrstva (*network layer*) poskytuje spojení mezi vzdálenými systémy. Rovněž se stará o vzájemnou komunikaci odlišných technologií. Dohlíží na síťový provoz a zajišťuje správné směrování paketů na cílový bod v síti.

Transportní vrstva (*transport layer*) zajišťuje spolehlivost a požadovanou kvalitu datového přenosu. Poskytuje dva základní typy služeb. Jedná se o spojově (protokol TCP) nebo nespojově orientované služby (protokol UDP).

> ***TCP*** - Protokol, která navazuje spojení pouze s cílovým prvkem komunikace. Data zasílána pomocí tohoto protokolu jsou odesílány pouze cílovému prvku. Jedná se zejména o přenosy souborů, služby www stránek a email.
> ***UDP*** – Protokol, který nenavazuje spojení pouze s jediným prvkem v síti jako v případě protokolu TCP, ale odesílá data všem dostupným prvkům. Jedná se o protokol využívaná pro služby streamováného videa, internetové televize či rádia.

Relační vrstva (*session layer*) realizuje přenos dat mezi jednotlivými relačními vrstvami systémů a zajišťuje jejich synchronizaci. Umožňuje ukončení nebo opětovné navázání spojení. V rámci této vrstvy pracují protokoly NetBIOS, Appletalk, RPC či SSL.

Prezentační vrstva (*presentation layer*) je předposlední vrstvou modelu OSI/ISO. Tato vrstva je odpovědná za transformaci dat do takové podoby, které je vyžadována pro potřeby správné funkčnosti různých aplikací. Tato vrstva také zajišťuje kontrolu struktury, nikoliv ale už významu dat. Příkladem protokolu fungujícího na této vrstvě může být protokol SMB.

Aplikační vrstva (*application layer*) je poslední, tedy sedmou vrstvou referenčního modelu OSI/ISO . Na rozdíl od prezentační vrstvy zde dochází ke kontrole význam dat. Princip této vrstvy spočívá v umožnění výměny dat směrující ke komunikačnímu systému. V této vrstvě pracují například protokoly FTP, DNS, DHCP, POP3 či Telnet.

3.1.2 Rodina protokolů TCP/IP

Jak již bylo uvedeno, rodina protokolů TCP/IP vychází právě z již uvedeného referenčního modelu organizace ISO. Právě tyto protokoly jsou totiž základním stavebním prvkem a souhrnem pravidel pro komunikaci v rámci počítačových sítí. Samotný název TCP/IP se skládá ze dvou nejvíce využívaných protokolů [3].

1. **TCP** - (*Transmission control protocol*) představuje spojově orientovaný protokol pro přenos informací a dat. Pomocí toho protokolu mohou aplikace mezi sebou vytvářet spojení, přes která mohou následně proudit data. Tento protokol také zajišťuje spolehlivost přenesených dat tím, že udělá kontrolní součet, který přidá do přenášeného paketu. U příjemce se tento kontrolní součet v rámci paketu najde a zkontroluje, zda tato informace odpovídá skutečnosti.

2. **IP** – (*Internet protocol*) prezentuje protokol používaný pro přenos dat mezi různými počítačovými sítěmi. Tvoří také základ dnešního Internetu. Nejčastěji se zatím stále využívá protokolu s označením IPv4. Postupně ale začínají docházet adresy. Tato skutečnost je způsobená velkým rozšířením Internetu, se kterým autoři původní

koncepce nepočítali. V současné době se už začíná rozšiřovat verze IPv6, která má obsahovat až stovky sextiliónu možných adres. (sextilion = 10^{36})

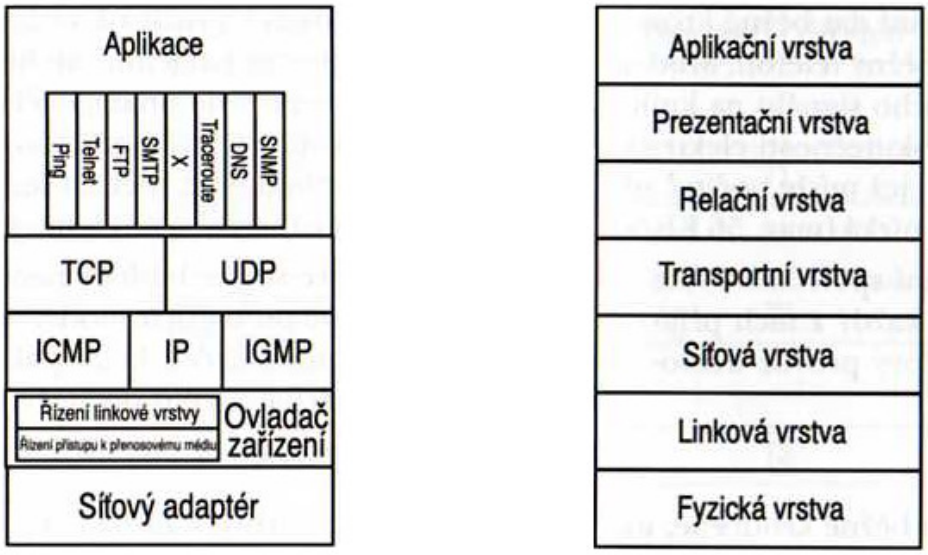
Základní architektura rodiny protokolu TCP/IP tedy spočívá pouze ve čtyřech vrstvách. Jedná se o vrstvu síťového rozhraní, síťovou vrstvu, transportní vrstvu a vrstvu aplikační.

Vrstva síťového rozhraní poskytuje fyzický přístup k datům. Je odlišná skoro v každé síti. Velmi totiž záleží na stavbě dané sítě, použitých komponentech a konkrétní implementaci.

Síťová vrstva zajišťuje hlavně síťovou adresaci a směrování dat. Na základě fyzického umístění směrovačů a rozbočovacích prvků, určuje podobu celkového síťového provozu.

Transportní vrstva je přítomná pouze v koncových prvcích sítě. Umožňuje adaptovat chování sítě pro potřeby samotné aplikace. Podobně jako v referenčním modelu OSI/ISO, poskytuje tato vrstva spojované (TCP) či nespojované služby (UDP).

Aplikační vrstva je poslední vrstvou, jak v modelu TCP/IP tak i v rámci modelu OSI/ISO. Pracuje se zde s daty, která prošla předešlými vrstvami. Aplikačních protokolů pracujících an této vrstvě je poměrně velký počet, jedná se např.: SSH, DNS, LDAP,SNMP,NTP, NetBIOS či rodina protokolů PKIX a mnohé další.



Obr. 1 – *Sada protokolů TCP/IP (obrázek vlevo) hrubě odpovídající definovaným vrstvám v síťovém modelu OSI (vpravo)* [3].

Znát jednotlivé vrstvy a funkce protokolů by měl každý, kdo se s otázkou zabezpečení počítačových sítí zabývá vážněji. Protože zastavit případný průnik někdy můžeme jen tehdy, když porozumíme slabinám v TCP/IP či v protokolech vyšší úrovně, které útočník zneužil.

TCP/IP protokol tedy samozřejmě není dokonalý. Jako dva základní a hlavní nedostatky lze uvést adresaci a zabezpečení. Původní účel těchto protokolů se podstatně změnil a právě z tohoto důvodu se objevují jisté slabiny. Nikdo neočekával, že v době kdy se protokol vyvíjel pouze pro propojení univerzit či pro potřeby armády, dosáhne celosvětového rozšíření. Původně bylo zamýšleno použití 32bitů pro adresu zařízení, což představovalo ohromující rezervu adres. Tato rezerva měla vystačit pro přibližně čtyři miliardy počítačů. V současné době ale nemá vlastní adresu zdaleka jen osobní počítač, ale i tiskárny, faxová zařízení, skenery, terminálové servery, fotoaparáty a dokonce i kávovary či ledničky. Vyčerpání původních 32 bitů pro adresaci ale umožnilo i blokové přiřazování adres. Nastala zde totiž situace, kdy nedochází k využívání všech adres, které jsou již přiděleny [3].

Druhá slabina, navzdory původnímu zamýšlenému použití v armádě, je slabé zabezpečení. Tvůrci zkrátka nevěnovali dostatek pozornosti zabezpečení protokolu proti špehování, zcizování spojení, útokům během autentizace a mnohým dalším rizikům. V době návrhu protokolů TCP/IP ještě ale zdaleka neexistovali takováto rizika. Navrhoval se jen malý komunikační systém, pouze pro pár vědeckých pracovníků, kteří si měli vzájemně vyměňovat data. Takže nikdo nevěnoval problematice zabezpečení větší míru pozornosti, kterou by si při navrhování tato rodina protokolů jistě zasloužila. Nikdo nevěděl, že se jednou budou používat pro elektronické obchody, elektronické bankovnictví a pro přenos utajovaných informací.

Proč ale v používání zvítězili právě protokoly TCP/IP? Proč se na celém světě tedy používá i navzdory slabinám které má? Mezi tyto důvody lze zařadit tyto [3]:

- **TCP/IP je založený na paketech**. Přes jedno síťové spojení může posílat data více počítačů či komunikujících prvků. Jedná se o sítě, které jsou založené na paketech a jsou rovněž levnější a snadněji se implementují. Normálně se nezaručuje dostupnost požadované kapacity přenosu a ani čekací doba. Ale zejména síla trhu rozhodla, že nižší náklady jsou důležitější než zaručený výkon.

- **TCP/IP umožňuje decentralizované řízení.** Poskytovatelé připojení dostanou k dispozici daný blok adres, který mohou průběžně dynamicky přidělovat v závislosti na klientovi a jeho připojení. Dále také samozřejmě mohou poskytovat daný počet adres nižších řádů. Př.: doména www.czu.cz je dále dělena na pef.czu.cz, tf.czu.cz, sic.czu.cz apod.

- **Zařízení, která spolu komunikují, jsou na stejné úrovni** (*peers*). V odlišnosti od jiných sítí, které rozdělují počítače na klientské a servery (např. *NetWare*) považuje TCP/IP každý počítač na síti za počítač na stejné úrovni. To tedy znamená, že je především více pružný a méně náchylný vůči selhání jiných počítačů.

- **TCP/IP je směrovatelný.** Směrovaný protokol umožňuje a usnadňuje přenášení dat mezi dvěma či více prvky v síti přes více propojení. Pomocí směrovačů se data zasílají na přesně určenou adresu. Naopak v protokolech, které nelze směrovat se muselo spoléhat na brány.

- **TCP/IP je nezávislý na přenosovém médiu.** Tento protokol funguje jak na Ethernetu,Token Ring, ARCNet, FDDI, USB tak i na jiných mechanismech které umožňují vzájemnou komunikaci na základě výměny signálu. Je dokonce pojat tak, že by mohl fungovat, i kdyby se místo dodavatelů jednotlivých paketů použili ptáci.

- **TCP/IP je otevřený standart.** Veškerá dokumentace je volně dostupná komukoliv. Žádná obchodní tajemství ani smlouvy neurčují, kdo může či nesmí protokoly implementovat.

- **TCP/IP nic nestojí**. Což souvisí s faktem, že se jedná o otevřený standard. Vyvinuly ho univerzity za podpory ministerstva obrany v USA. Implementace tohoto protokolu je zcela bezplatná a nikdo v podstatě rodinu protokolů TCP/IP nevlastní.

- **TCP/IP je robustní.** Protokoly dokážou do jisté míry detekovat a následně i opravovat vlastní chyby. Zejména se tak elegantně vzpamatovávají z dočasně přerušených komunikačních spojení. Umějí i obcházet nefunkční či poškozené části Internetu.

- **TCP/IP je pružný.** Struktura TCP/IP spočívá v základních protokolech a dalších protokolech, které jsou umístěny nad nimi. Tyto vyšší protokoly umožňují poskytovat propracovanější a náročnější služby. Ne vždy je ale nutná přítomnost celé rodiny protokolů. Zejména prvky jako směrovače a rozbočovače musejí obsahovat pouze ty prvky, které jsou nezbytné pro jejich funkci. Jakýkoliv nadbytečný protokol, či služba představuje na těchto prvcích potenciální nebezpečí.

- **TCP/IP je pragmatický.** Postupně jak se rozvíjeli možnosti využiti, tak realizátoři přidávali další protokoly. Tento postup nebyl aplikován třeba při vzniku referenčního modelu OSI/ISO, který se navrhoval „z ničeho". Nakonec byl zbytečně složitý a obsahoval křehké standarty, které se neuměly rychle adaptovat novým požadavkům.

3.2 Základní bezpečnostní principy

Síťová bezpečnost je velmi rozsáhlá problematika, která zahrnuje široké spektrum technologií a zásad. Právě proto se již v dnešní době nepoužívá pouze jedna určitá metoda či zásada zabezpečení, ale využívají se především jejich vzájemné kombinace. V moderní době je nutné pokrýt daleko více možností použití výpočetní techniky než v minulosti. Jinak již není možné zajistit dostatečný stupeň ochrany a zajistit tak i bezproblémový chod dané organizace či společnosti. Mezi základní principy tedy patří:

3.2.1 Princip autentizace, autorizace a účtování (AAA)

V anglickém jazyce je tento princip znám pod pojmem „triple A". Přičemž jednotlivá písmena vycházejí z výrazu authentication, autorization a accounting. Někdy se tento princip označuje jako pouze jedna z metod autentizace k síti, v důsledku zavádění tohoto principu do praxe a do možností konfigurace různého hardwaru. Tento princip v pravém významu ale vychází z již zmíněných tří základních bodů [5,6]:

1. ***Autentizace*** (*authentication*)
2. ***Autorizace*** (*autorization*)
3. ***Účtování*** (*accounting, auditing*)

Každý z těchto bodů představuje komponentu, která hraje v bezpečnosti sítě velmi důležitou roli. Splněním požadavků, které kladou jednotlivé body, podstatným způsobem zlepšíme zabezpečení počítačové sítě.

Autentizace

Proces autentizace nám ověřuje především uživatelovu identitu a zajišťuje skutečnost, že uživatel je skutečně tím, za koho se vydává. Identita je zde důležitá zejména pro pozdější procesy autorizace a účtování, kde bychom bez identity neměli komu provedené sledované operace přiřadit.

Autentizace nám tedy umožňuje i snadné zpětné dohledání aktivity uživatele, což je v dnešní době už samozřejmostí. Například ale ještě v poměrně nedávné době hojně využívaná aplikace TELNET, toto při vzdáleném přístupu neumožňovala. Uživatel se zde přihlašoval jen pomocí hesla, bez zadávání identity uživatele. Neoprávněnému uživateli tak stačilo uhádnout pouze heslo, nehledě na skutečnost, že měl k dispozici téměř neomezené množství času a měl přístup k našemu systému. Přitom zpětné dohledání změn nebo uprav dat na základě indenty, zde nebylo možné právě kvůli faktu, že pro přístup nebylo zapotřebí žádné uživatelské jméno. Pokud se tedy někomu povedlo zjistit heslo, mohl napáchat opravdu velké a především těžko vypátratelné škody našem sytému.

S autentizací respektující princip AAA je této skutečnosti zamezeno, jelikož každý uživatel musí zadat vlastní přiřazené uživatelské jméno a heslo. Je zde tedy i možnost dohledat provedené změny v našem systému.

Autorizace

Proces autorizace úzce souvisí s procesem autentizace. Pouze na základě úspěšné autentizace následuje další fáze zahrnující autorizaci uživatele. Zde musíme rozhodnout, k jakým systémovým zdrojům bude mít daný uživatel přístup a které může případně měnit nebo i smazat. Je zde také samozřejmě nutné odlišit běžná uživatelská práva od práv administračních.

Autorizace ale nedefinuje jen přístupové práva, ale stanovuje i typ povolených komunikačních aktivit a protokolů, které jsou povolené. Proces autorizace je většinou

zajišťovaný pomocí přístupových seznamů, známe také pod zkratkou ACL. Tuto roli ale mohou rovněž plnit i zásady odvíjející se z bezpečnostní politiky organizace.

Účtování

Tento proces je poslední prvek bezpečnostního principu AAA. Jeho využívání má smysl pouze v případě, že byla úspěšně provedena jak autentizace, tak i autorizace.
V opačném případě je přínos z účtování nulový.

Během tohoto procesu jsou shromaždovány informace, zahrnující jak identity uživatelů, tak i jimi provedené akce v dotyčném systému. Tyto nashromážděné informace mohou samozřejmě sloužit také jako důkaz o neprávoplatných akcích a být i podkladem pro soudní řízení. Pokud nám ale někdo podvrhne falešnou identitu a náš systém jí akceptuje, tak sice víme, jaké operace se prováděly, ale nikoliv už kdo je provedl.

Princip AAA nám tedy dává do rukou poměrně mocný nástroj ochrany našeho systému, ale určitě nestačí spoléhat se pouze na něj. Existuje velké množství možností jak princip AAA přelstít či obejít. Minimálně ale tvoří překážku, kterou je třeba překonat a poskytuje nám určitou míru zabezpečení proti neoprávněnému zásahu do našeho systému.

3.2.2 Princip důvěrnosti, integrity a dostupnosti (CIA)

Tento princip vychází podobně jako princip AAA z anglické terminologie. Zkratka CIA je vytvořena ze slov confidentality, availability a integrity. Přičemž se jedná o utajení informací, respektive udržení důvěrnosti (Confidentality), zajištění dostupnost (Availability) a nakonec i zajištění integrity (Integrity) [11].

V souvislosti s tímto principem se také velmi často uvádí potřeba provedení analýzy rizik. Cílem této analýzy je identifikace klíčových dat, které organizace zpracovává a následně i určení hrozeb, které nějakým způsobem ohrožují důvěrnost, integritu a dostupnost těchto dat. Vše samozřejmě s ohledem na finanční a další konkrétní možnosti či omezení dané organizace.

Bohužel v dnešní době je téměř nemožné, aby si každý jednotlivý subjekt prováděl analýzu rizik ve vztahu k informační bezpečnosti sám. Malé subjekty narážejí na nedostatek financí a nedostatek zkušeností, případně této problematice nevěnují dostatek pozornosti. Naopak u větších subjektů je už situace lepší a pro potřeby analýzy rizik vyčleňují vlastní zaměstnance, nebo si najímají minimálně externí firmu.

Obr. 2 – *grafické znázornění principu CIA*[11]

Princip CIA je tedy poměrně komplexní nástroj pro zajištění datové, respektive informační bezpečnosti. Velmi často se lze ale setkat pouze s jeho dílčím použitím v praxi. Pokud například budeme dbát pouze na integritu a dostupnost, a bez ohledu na důvěrnost, dostaneme se do situace, kde jsou naše data sice dostupná a je možné s nimi pracovat v nezměněné podobě, ale zároveň jsou přístupné i dalším neoprávněným osobám bez autorizace.

Podobná situace je i ve zbylých dvou dílčích kombinacích. V případě podcenění integrity máme sice data dostupná pouze pro zaměstnance, které jsme si stanovily, ale nemáme zajištěn fakt, že s daty nebylo nepřípustně manipulováno a že jsou v původní podobě. Nejsme tedy schopni opět zajistit stoprocentní informační bezpečnost, a vystavujeme se mnohým rizikům plynoucí z tohoto nedostatku.

Obdobně v případě opomenutí otázky dostupnosti dochází k jevu, kdy máme sice zajištěnou vnitřní stálost dat a odolnost proti nežádoucí modifikaci dat spolu s důvěrností informací, ale data nejsou přístupné pro zaměstnance, kteří s nimi potřebují pracovat. Ačkoliv

máme tedy informace poměrně dobře zajištěny, jsou nám k ničemu, když nejsou v daný okamžik k dispozici. Tento případ je poměrně vzácný v praxi, ale například se vyskytuje u firem, které naopak přecenily otázku informační bezpečnosti. Organizace zahltila svoje výpočetní prostředky bezpečnostními softwary, a v důsledku vyčerpání výpočetní kapacity došlo k nedostupnosti klíčových dat.

Vždy je tedy nutné učinit rozumný kompromis, a stanovit míru zabezpečení na základě analýzy rizik, a zejména na základě potřeb organizace. Jiné potřeby v rámci informační bezpečnosti má živnostník a jiné bankovní institut či armádní složka.

V současné době je už také nutné vzít v úvahu legislativní opatření. Nejvyšší pokuta, kterou může úřad pro ochranu osobních údajů udělit, činí 5.000.000 Kč v případě právnické osoby, a v případě fyzické osoby je tato maximální hranice stanovena na 1.000.000 Kč. Sice se zatím tyto finanční postihy uplatňují poměrně zřídka v našich poměrech, ale při závažném porušení ochrany osobních údajů se využívají. Tento fakt je ale pouze dalším důvodem pro praktickou aplikaci principu CIA v celém jeho rozsahu. Dalším důvodem pro praktické využívání tohoto principu v celém jeho rozsahu, je konkurenceschopnost. Pokud například nebudeme dbát na integritu našich klíčových dat, a dojde k jejich změně, činíme ze sebe či z celé společnosti velmi snadno zmanipulovatelný objekt. Princip CIA má tedy určitě své opodstatnění v zabezpečení komunikace, respektive v zabezpečení přenášených informací.

3.2.3 Princip minimálních oprávnění (least privilege)

V anglické literatuře bývá tato zásada označována jako „*principle of least privilege*“. Tento princip vyjadřuje požadavek, aby všichni uživatelé našeho systému měli v každém okamžiku pouze minimální možné oprávnění pro nakládání s daty [18].

Musíme ale vzít potaz pracovní pozici a náplň činnosti daného zaměstnance, a zajistit mu práva nezbytná pro její vykonávání. Opět je tedy na místě jistý kompromis, kdy udělujeme práva pouze pro takové informace a zdroje, které jsou nezbytné pro vykonávání práce, a ostatní práva se snažíme blokovat, z důvodu eliminace možného rizika neoprávněného přístupu ke zdrojům či informacím.

3.3 Bezpečnostní politika

Informace uložené v elektronické podobě přináší vedle řady výhod i řadu možných hrozeb. Z tohoto důvodu by měla být bezpečnostní politika jedním ze základních dokumentů každé společnosti. V současné době přistupují k tomuto problému některé organizace komplexněji, jiné ale spíše nahodile. Všechny organizace by se ale měli snažit o systematické řešení, a snažit se tak docílit požadovaného stavu. A právě prvním krokem v této změně je vypracování celkové bezpečnostní politiky organizace.

Dokument bezpečnostní politiky by měl v obecné rovině vycházet především z celkové koncepce dané organizace, a základem této koncepce by zase měla být provedená analýza rizik. Není to sice nezbytnou podmínkou, může se vycházet i z jiných zdrojů, ale tyto zdroje berou v potaz většinou jen určitou část problematiky a neumožňují takový komplexní nadhled nad problematikou jako již zmíněná analýza rizik. Pokud jsou jedním z těchto zdrojů i empirické poznatky, k čemuž v praxi také poměrně často dochází, dochází zpravidla i k subjektivnímu ohodnocení bezpečnosti a tím k neobjektivnímu hodnocení možných rizik. Pokud ale bezpečnostní politika nebude vycházet z uvedené analýzy rizik, nemusí tím nutně utrpět její kvalita. Kvalitní dokument bezpečnostní politiky se dá vytvořit i z jiných zdrojů, ale je nutné věnovat zvýšenou pozornost právě objektivitě a rozsahu hodnocení možných rizik. Velmi často se ale analýza rizik využívá, a proto je dobré se s ní seznámit.[10,4]

3.3.1 Analýza rizik

Analýza rizik je vynikající nástroj pro sestavení bezpečnostní politiky. Zjednodušeně se jedná o přehled zjištěných hrozeb, kterým je společnost vystavena. Udává také pravděpodobnost, kdy daná hrozba zneužije zranitelnosti našeho systému, a rovněž by měla zahrnovat i hledisko možných dopadů na společnost. V rámci analýzy rizik se používají následující pojmy, které je důležité znát: [7]

- **Aktivum** (Asset) – představuje zjednodušeně vše, co má pro společnost nějakou hodnotu, a mělo by být nějakým adekvátním způsobem i zabezpečeno a chráněno.

- **Hrozba (**Threat) – potenciálně nebezpečná událost, která muže způsobit ztrátu či narušení důvěrnosti, integrity nebo dostupnosti dat v našem informačním systému.

- **Zranitelnost** (Vulnerability) – prezentuje slabinu v našem zabezpečení systému, ať už na úrovni fyzické, logické nebo administrativní bezpečnosti. Tato zranitelnost může být potenciálně využita hrozbou, a ohrozit tak naše aktiva.

- **Riziko** (Risk) – pravděpodobnost, udávající šanci zneužití zranitelnosti některou hrozbou. Případně je riziko také definované jako pravděpodobnost, při které dojde k narušení důvěrnosti, integrity nebo dostupnosti.

- **Opatření** (Countermeasure) – bezpečnostní opatření, které směruje ke snížení úrovně zranitelnosti v našem systému. Toto opatření je prováděno opět na fyzické, logické, nebo administrativní úrovni bezpečnosti.

- **Ohrožení** (Exposure) – vyslovení skutečnosti, která udává existenci potenciálně zneužitelné zranitelnosti systému.

- **Narušení** (Breach) – situace či stav, kdy už došlo ke zneužití zranitelnosti systému, a došlo k narušení důvěrnosti, integrity nebo dostupnosti v důsledku překonání bezpečnostních opatření.

Pojmy ohrožení a narušení zde definované jsou už méně známé, nicméně je vhodné o nich a jejich významu vědět. Hrozby tedy zneužívají zranitelnost, která vede k ohrožení, což je riziko, které lze snížit pomocí opatření chránící aktiva. Vzájemné vztahy mezi jednotlivými pojmy lze znázornit pomocí následujícího obrázku:

Obr. 3 – *Základní funkce a vztahy mezi definovanými pojmy v rámci analýzy rizik* [7]

Vlastní proces analýzy rizik se skládá z několika fází. Jedná se o identifikaci a kvantifikaci aktiv, hrozeb, zranitelnosti a výsledného rizika. Přístupů a metodik k provedení analýzy je více, ale pro demonstraci zde uvedeme normu ISO/IEC 13335, ve které jsou definovány a vysvětleny čtyři základní přístupy k analýze rizik:

- **Základní přístup** – zde se žádná vlastní analýza rizik neprovádí. Jsou pouze vybrány některé základní sady opatření, které jsou následně zavedeny.

- **Neformální přístup** – již obsahuje provedení analýzy rizik, ale ta se provádí pouze na základě zkušeností odborných pracovníků a vyhodnocení potenciálně možných scénářů. Jedná se časově nenáročnou a hlavně orientační analýzu.

- **Formální přístup** – zde se provádí již detailní analýza. V jejímž rámci se provádí hodnocení aktiv, hrozeb a zranitelnosti, přičemž vše za použití matematického aparátu.

- **Kombinovaný přístup** – využívá výhody neformálního i formálního přístupu. Zde se tedy provádí nejdříve orientační analýza rizik, kde se identifikují kritická aktiva nebo procesy pro společnost, a na základě orientační analýzy se následně provede i analýza detailní.

Analýza rizik, nezávisle na přístupu, by měla obsahovat čtyři základní fáze, které jsou nezbytné pro její správnou funkci a rozsah. První fáze je analýza aktiv, kde se identifikují pro organizaci důležitá aktiva a určuje se jejich hodnota. Vytváří se zde tzv. registr aktiv. Druhá fáze nese označení analýza hrozeb. Zde se opět identifikují možné hrozby, a rovněž se i určitým způsobem kvantifikují. Během této fáze vycházíme buď ze seznamu obecných, nebo specifických hrozeb. Následně na identifikaci hrozeb navazuje třetí fáze, kde se zabýváme analýzou zranitelnosti. V tomto kroku musíme identifikovat a ohodnotit všechna slabá místa našeho systému, ale nezávisle na identifikovaných hrozbách. V okamžiku kdy je známá hodnota aktiv, společně se slabými místy, pravděpodobností hrozeb a mírou zranitelnosti přechází analýzy do poslední fáze. Zde se zejména stanovuje výše rizika a škody. V závislosti zda jsme prováděli kvantitativná či kvalitativní analýzu, dochází v této fázi k vyjádření výší rizika v peněžních jednotkách, či ve stupních.

Normy ani standardy ale prakticky už vůbec neřeší otázku, kdo by měl analýzu rizik provádět. V praxi se přitom jedná o poměrně zásadní rozhodnutí, které velmi znatelným způsobem může ovlivnit vlastní funkci a účinnost analýzy rizik. Existují dvě základní formy provedení analýzy rizik právě na základě subjektu, který jí vykonává. Jedná se o formu interní analýzy rizik, která je prováděna vlastními zaměstnanci dané organizace, nebo formou externí analýzy, prováděné zaměstnanci cizí poradenské či konzultantské firmy.[2]

#	Interní analýza rizik	Externí analýza rizik
1.	znalost prostředí a procesů	zkušenosti z jiných společností
2.	zachování důvěrnosti	porušení důvěrnosti
3.	nutno koupit nebo vyvinout meto-diku	není nutné kupovat nebo vyvíjet metodiku
4.	nutno koupit nebo vyvinout nástroj	není nutné kupovat nebo vyvíjet nástroj
5.	nutno mít nebo vyškolit vlastní odborníky	není nutné mít vlastní odborníky
6.	všichni rozumí výstupům projektu	výstup projektu je nesrozumitelný
7.	neschopnost vést interview	schopnost vést interview
8.	nižší míra objektivity	vyšší míra objektivity
9.	nižší cena	vyšší cena
10.	více zatěžuje společnost	méně zatěžuje společnost

Obr. 4 - Porovnání interní a externí formy analýzy rizik [2].

Shrneme-li analýzu rizik, můžeme konstatovat, že popisuje jak všechny možnosti, které mohou nastat, tak i z jakých důvodu nastaly. Zahrnuje ale i popis kde přesně taková situace může nastat a koho se bude týkat. Jak je tedy vidět, dobře zpracována analýza rizik je velmi užitečný dokument bezpečnosti informačních technologií, a skvěle se hodí i pro potřeby nastavování rámců bezpečnostní politiky.

3.3.2 Obsah dokumentu

Bezpečnostní politika je termín pro označení souboru přijatých zásad, postupů, plánů a metod směrující k zabezpečení daného systému či prvku. Jejím charakterem by také měla odpovídat na pět základních otázek:

- Co přesně chce organizace chránit?
- Jakým způsobem to chce chránit?
- Proč to chce chránit?
- Jak bude ověřovat, že je to chráněno?

- Co bude dělat v případě selhání ochrany?

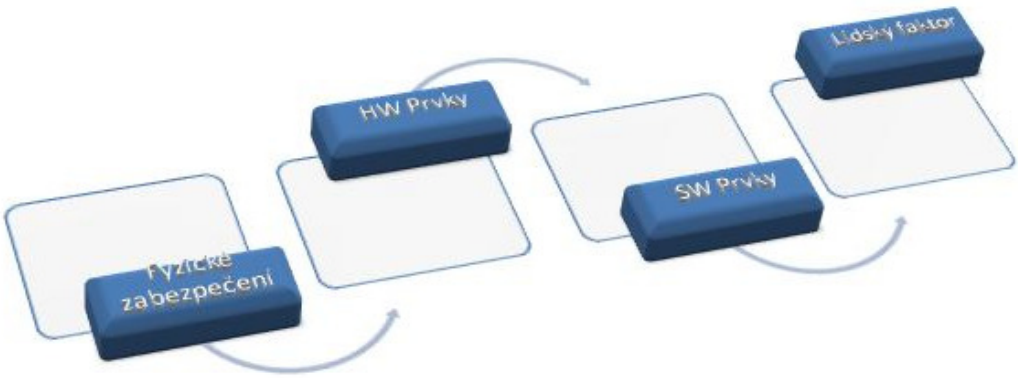
Bezpečnostní politika musí ale také splňovat tři základní principy, jinak se ztrácí její veškerý smysl. Musí být v písemné podobě, musí být závazná pro všechny zaměstnance a musí být známá. Tato skutečnost se označuje jako tři pilíře bezpečnostní politiky [10].

V případě že není tento dokument sepsán v písemné podobě, zákonitě dochází k podcenění významu a především k mnoha nejasnostem. Proto by každá organizace, která nechce podceňovat problematiku zabezpečení, měla mít bezpečnostní politiku v písemné formě. V případě kdy bezpečnostní politika není závazná pro všechny zaměstnance nebo není dokonce vůbec známa její existence, dochází k podobnému důsledku. Stačí jeden nezodpovědný zaměstnanec či člověk na pracovišti, který není seznámen s dokumentem bezpečnostní politiky, a smysl tohoto dokumentu z pohledu zabezpečení prudce klesá, respektive se úplně vytrácí. Proto se v praxi velmi často uplatňují sankce za porušování této politiky, které jsou zakotveny přímo v pracovní smlouvě spolu s povinností zaměstnance se s tímto dokumentem ihned po přijetí do pracovního poměru seznámit.

Cílem bezpečnostní politiky musí být detailní popis zabezpečení komplexního celku, včetně vzájemných interakcí jednotlivých částí. Proto je doporučeno rozdělit koncepci zabezpečení na čtyři základní úrovně [16]:

1. Fyzické zabezpečení jednotlivých prvků IT infrastruktury
2. Hardwarové prvky zabezpečení provozu
3. Softwarové prostředky ochrany provozu
4. Ochrana před selháním lidského faktoru

Každá jednotlivá úroveň představuje dimenzi komplexního zabezpečení a její nezbytnou součást. Není možné nějakou dimenzi vynechat, a očekávat že náš systém bude dobře zabezpečen. Pokud vynecháme nějakou dimenzi, naše zabezpečení se pravděpodobně zhroutí, přičemž je to jen otázka času. Je tedy nutné dbát jak na všechny čtyři úrovně, respektive dimenze zabezpečení, ale i na jejich vzájemné interakce a vztahy.



Obr. 5 – *schéma zabezpečení IT systému* [16]

Právě pro účely zajištění odpovídající úrovně zabezpečení již zmíněných dimenzí, bylo potřeba vytvořit ucelený dokument, který bude danou problematiku popisovat. Tento účel by měl bezezbytku v každé organizaci plnit dokument bezpečností politiky. Dále by ale bezpečnostní politika, kromě pohledu na všechny čtyři dimenze zabezpečení, měla zahrnovat minimálně i tyto následující body [15]:

- Stanovení účelu dokumentu bezpečnostní politiky, prohlášení o závaznosti pro pracovníky a deklarace plné podpory ze strany vedení organizace.
- Definici požadované úrovně bezpečnosti
- Definici úrovní zabezpečení a míry odolnosti proti jednotlivým typům útoků.
- Definici bezpečnostního managementu organizace
- Základní bezpečnostní opatření v oblasti administrativní, personální, fyzické a systémové v obecné formě.
- Normy chování zaměstnanců
- Havarijní plány a postupy
- Deklaraci souladu řešení bezpečnosti s platnou legislativou

Po zkompletování uvedených bodů, jsou zpravidla jednotlivé části předloženy k připomínkám a k případnému dodělání. Teprve po samotném odsouhlasení všech kapitol a částí je vypracován výsledný dokument celé bezpečnostní politiky. Ten je následně předložen vrcholovému vedení organizace k vyslovení souhlasu, a následně i k uvedení v platnost.

3.3.3 Obecné typy politiky

Existuje několik variant obecného typu bezpečnostní politiky informačního systému. Vždy je ale nutné mít na paměti, že finální dokument bezpečnostní politiky informačního systému by měl vycházet jak z komplexní bezpečnostní politiky organizace, tak i z provedené analýzy rizik, ale samozřejmě i z konkrétního prostředí v rámci působení dané organizace. V obecném pojetí tedy rozpoznáváme podle poskytované úrovně zabezpečení čtyři modely bezpečnostní politiky informačního systému [8].

- **Promiskuitní model** se dá zjednodušeně považovat za nejméně přísnou bezpečnostní politiku. V zásadě každému povoluje vykonávat jakoukoliv činnost, tedy i takovou, kterou by provádět neměl z hlediska bezpečnosti. Tento model zaručuje velmi nízkou úroveň bezpečnosti, případně dokonce vůbec žádnou. Praktickým důvodem pro použití tohoto modelu je jeho nízká finanční náročnost.

- **Liberální model** je typ bezpečnostní politiky, který umožňuje opět každému provádět jakoukoliv činnost, ovšem s výjimkou explicitně nadefinovaných zakázaných věcí. Úroveň zabezpečení je zde tedy i lepší než u předchozího promiskuitního modelu, ale stále při zachování poměrně nízké ekonomické náročnosti. Liberální model bezpečnostní politiky se uplatňuje zpravidla u takových informačních systémů, ve kterých se případné hrozby považují za málo či průměrně závažné. Klasickým základním stavebním prvkem této politiky je zásada volitelného a řízeného přístupu, založeného na jednoznačné identitě subjektu.

- **Racionální model** bývá také někdy označován jako model opatrné bezpečnostní politiky. U tohoto modelu je filosofie vzhledem k předchozím modelům opačná. Je zde zakázáno vše, kromě explicitně nadefinované a povolené činnosti. Zavedení tohoto modelu je už ekonomicky podstatně náročnější, ale poskytuje také daleko vyšší úroveň zabezpečení. Model požaduje rovněž provedení klasifikace objektů v informačním systému podle jejich schopností a citlivosti. Základem je zde princip povinného řízení přístupu, který je založen na přidělených uživatelských rolích, ve kterých subjekty vystupují. Tento model ale našel i uplatnění při zavádění firewallů, kdy se na začátku používání, nejlépe ale ihned po instalaci firewallu, zakáže veškerá aktivita, a následně se povolují pouze identifikované a žádoucí procesy.

- **Paranoidní model** bezpečnostní politiky zakazuje dělat vše, co by mohlo být potenciálně nebezpečné. Tedy i to, co nemusí být explicitně zakázáno. Tento model zaručuje nejvyšší úroveň zabezpečení, a vede k maximální izolaci informačního systému od okolního prostředí při zachování poměrně nízké úrovně nákladů. Takováto politika je aplikována v oblastech, ve kterých se zpracovávají vysoce důvěrné informace. Na základě přesně definovaných vstupů a výstupu do systému, je dosažena i vyšší výkonnost, jelikož všechny ostatní aktivity jsou eliminovány a automaticky bezpečnostní politikou zakázaný.

Samotné zavedení bezpečnostní politiky do praxe se už následně může jevit jako snadný úkol. Je nutné ale mít na paměti, že praktické zavedení tohoto dokumentu do každodenního provozu, vždy přináší určité restrikce a klade na zaměstnance nové požadavky. Zejména v takovém prostředí, kde jsme nuceni vybudovat bezpečnostní politiku od samého začátku, nejsou uživatelé na tyto restrikce a požadavky zvyklí, a nemusejí je přijímat jednoduše.

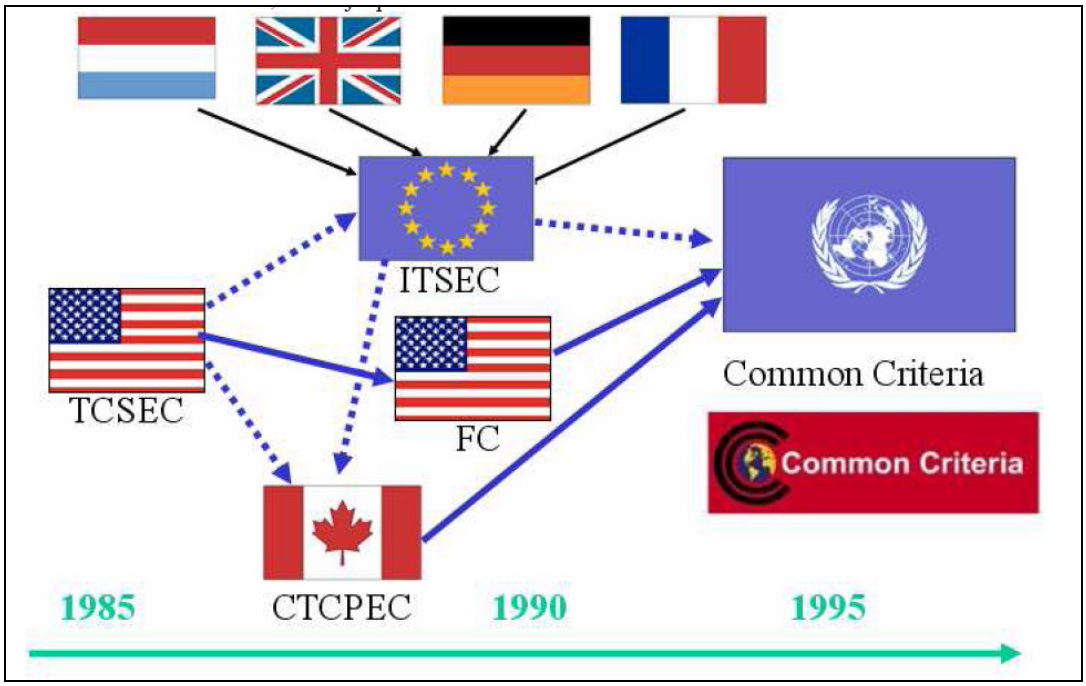
Informace uložené v elektronické podobě přináší vedle řady výhod i řadu možných hrozeb, jak již bylo řečeno na začátku kapitoly. Účelem dokumentu bezpečnostní politiky je tedy zabránit možným hrozbám, ať už pomocí fyzického zabezpečení informační techniky, hardwarové a softwarové dimenzi, či pomocí lidského faktoru. Kombinace účinnosti těchto dimenzí v zabezpečení, nám udává z pohledu bezpečnostní politiky úroveň bezpečnosti a důvěryhodnosti našeho informačního systému. Vypracování dokumentu bezpečnostní politiky nám tedy umožňuje všechny dimenze přiblížit, a zavést pro ně takové opatření, aby nedocházelo k ohrožení našich informací v rámci informační technologie.

3.4 Standardy a kritéria hodnocení informační bezpečnosti

Historickým základem pro problematiku informační bezpečnosti jsou považována kriteria Trusted Computer System Evalution Criteria (TCSEC). Tyto kriteria vznikla ve Spojených Státech Amerických, zhruba v polovině devadesátých let 20. století. Někdy jsou tyto kritéria označována jen zkratkou TCSEC či "Orange Book“, podle barvy obálky ve které byla původně zveřejněna. Tato kriteria byla využívána pro hodnocení informačních systému,

mimo jiné i pro informační systémy Ministerstva obrany USA. Jednalo se tedy o vysoce citlivé informace, na které byly kladeny, ve smyslu bezpečnosti, velmi vysoké nároky [13].

Dále následoval vznik různých národních variant standardů pro zabezpečení informačních systémů. Na území Kanady to byla kriteria CTCPEC (Canadian Trusted Computer Product Eval. Criteria). Následně i na Evropském kontinentě vznikla obdobná kritéria ITSEC (Information Technology Security Criteria). Poměrně důležitým milníkem v této problematice je rok 2000, kdy se 6 států dohodlo na ustanovení jednotného standardu ISO/IEC 15408, který je známější spíše pod názvem Common Criteria.



Obr. 6 - *Vývoj kritérií hodnocení informační bezpečnosti* [13]

3.4.1 TCSEC (Trusted Computer System Evaluation Criteria)

Prvním průkopníkem v problematice zabezpečení informačních systémů bylo tedy USA. Standard TCSEC vznikl jako první ucelený dokument týkající se této problematiky. Místo vzniku těchto standardů na území USA ale samozřejmě nebylo náhodné. Bylo určeno především technologickou úrovní v rámci informační techniky na území USA. Jako příklad vysoké úrovně informačních technologií v době vzniku TCSEC kritérií ve Spojených Státech Amerických, lze uvést vznik v současnosti největší celosvětové sítě – Internetu.

Vznik internetu je pevně spojen s agenturou ARPA, která 29. října 1969 zprovoznila síť ARPANET se 4 uzly. Tyto uzly představovaly jednotlivé univerzitní počítače v různých částech USA. Jedna z klíčových vlastností spočívala a stále spočívá v decentralizaci sítě. Tato vlastnost znamenala zvýšení zabezpečení a především možnost další datové komunikace v případě zničeni jakékoliv dílčí části sítě. Data zde putují v síti po paketech, tedy po částech, které jsou směrovány přes jednotlivé uzly, a to umožňuje pakety v případě potřeby přesměrovat jinou cestou, která rovněž vede ke stanovenému cíli. Tato a další technologické výhody určily dnešní velikost Internetu. Dnes se jedná o celosvětovou síť, která má podle odhadů více jak 2 miliardy uživatelů, a je nezbytnou součástí světa v dnešní podobě.

Americká kritéria TCSEC představují pro hodnocení prostředku bezpečnosti počítačových systému velmi cenný nástroj. Jejich vzniku ale předcházela řada dokumentů, nařízení a již existujících doporučení. Už v roce 1967 Defense Science Board [1] vykazovalo snahu o sjednocení celé bezpečností problematiky napříč počítačovým průmyslem. Výsledkem práce tohoto výboru byli i dvě direktivy ministerstva obrany v USA, které byly vydány v roce 1972 a 1973. Obsahovaly doporučení a požadavky na zabezpečení, včetně jejich administrativního zajištění [13].

1] Defense Scicence Board (DSB) *je civilní výbor z předních vědeckých odborníků pro obranu, které jmenuje americké ministerstvo obrany. Tento výbor byl založen v roce 1956 na doporučení Hoover Komise .*

Dále se ministerstvo obrany USA od roku 1977 zaměřilo samostatně na problematiku počítačového zabezpečení. Společně s touto aktivitou byla zahájena i práce na definici problematiky souvisejících s návrhem, implementací a kontrolou systémů, které vyžadovali určitý stupeň zabezpečení, pod vedením National Bureau of Standards [2].

Na základě obou zmíněných aktivit a činností započala svojí iniciativu i společnosti Mitre Corporation. Tato společnost funguje do současné doby, a má registrováno více jak šest desítek patentů, a obdržela velmi mnoho ocenění. V jisté míře navazuje na snahu ministerstva obrany USA a vědeckého výboru pro obranu, ale její hlavní snažení směřovalo do problematiky hodnocení stupně zabezpečení libovolného informačního systému. V roce 1981 bylo v rámci ministerstva obrany USA založeno Computer Security Center, ale už jen pouze za účelem rozšíření nově vzniklých norem a doporučení do všech systému které na základě své povahy vyžadovali dle ministerstva určitý stupeň zabezpečení. Výstupem této aktivity ale byli i kriteria, které napomáhal uživatelům zhodnotit stupeň ochrany daného systému.

Tato přibližně dvacetiletá snaha a úsilí o standardizaci problematiky zabezpečení informačních systému, vyústila v normu Trusted Computer System Criteria (TCSEC). Tato norma, respektive kriteria pro hodnocení zabezpečení počítačových systémů, vstoupila v platnost v roce 1983. Vzhledem k tomuto datu, je jasné, že v dnešní době nového tisíciletí je tato norma již nedostatečná. Informační technika prodělala od té doby neuvěřitelný rozvoj a rozmach, a tato norma již plně neuspokojuje požadavky na ní kladené. Postupně se od tohoto standardu tedy přechází na novější. Základní principy ale většinou zůstaly zachovány i v současné době, a z tohoto důvodu je dobré se s kriterii hodnocení informační bezpečnosti TCSEC minimálně seznámit.

---

[2] National Bureau of Standards *je dnes známý spíše jako Národní institut pro standardy a technologie (National Institute of Standards and Technology, neboli NIST).*

Standard TCSEC rozděluje systémy do čtyř základních skupin, na základě jejich úrovně zabezpečení. Jedná se o skupiny A – D, přičemž se tyto skupiny dále dělí do tříd nižších, které jsou značeny číselně. Každá třída pokrývá čtyři aspekty, na základě kterých jsou systémy hodnoceny. Jedná se tyto kritéria:

- ***Bezpečnostní politika***
- ***Účtovatelnost***
- ***Míra záruky***
- ***Dokumentace***

Logika značení skupin na základě těchto aspektů tedy spočívá ve vzestupném řazení, podle abecedy a podle nejlepší úrovně zabezpečení. Nejlepší úroveň zabezpečení tedy poskytuje skupina A, nejhorší zabezpečení má naopak systém označený písmenem D. Další řazení tříd v rámci jednotlivých skupin pomocí číslic má ale logiku opačnou. Čím vyšší číselné označení v rámci třídy, tím daný systém poskytuje vyšší úroveň zabezpečení [14].

- **Skupina A: Verifikovaná ochrana**
  Označení libovolného informačního systému písmenem A prezentuje fakt, že implementované bezpečnostní funkce skutečně fungují, a splňují požadavky, které jsou na ně kladené. V neposlední řadě toto označení skupiny zaručuje i skutečnost, že dané bezpečnostní funkce jsou ověřeny, respektive verifikovány.

  Třída A1 : Verifikovaný projekt – Funkční obdoba systému se systémem třídy B3, ovšem s výjimkou verifikace správně implementovaných funkcí, která se zde provádí navíc. Ověřujeme zde fakt, zda systém dělá přesně to, a pouze to, co po něm požadujeme a co je uvedeno v projektové dokumentaci. Tato skutečnost je důležitá pro systémy s vysokými požadavky na úroveň zabezpečení. Může se jednat například o systémy, které využívají bankovní instituty.

- **Skupina B: Direktivní ochrana**
  Prezentuje takové systémy, ve kterých je hlavním požadavkem uplatnění povinných pravidel pro řízení přístupu. Přičemž tento systém musí vycházet ze stanoveného bezpečnostního modelu. Skupina B se dále rozdělena do 3 tříd (B1, B2, B3)

Třída B1: Ochrana bezpečnosti návěstím – Systémy označené B1 jsou obdobou systému třídy C2, ale jelikož se jedná o vyšší skupinu, obsahuje navíc model bezpečnostní politiky, který může být i v neformální podobě. Tato třída (B1) obsahuje také další bezpečnostní prvek, který se označuje pojmem návěstí dat. Tento prvek obsahuje informace o režimu utajení dat, ke kterým je připojen, a na základě tohoto režimu jsou i řízeny přístupy k jednotlivým objektům.

Třída B2 : Strukturovaná ochrana – V této třídě se mění zejména podmínka existence dokumentu obsahující bezpečnostní politiku. Už zde musí být ve formální podobě, na rozdíl od třídy B1. Vyžaduje se také řízení přístupu na základě návěstí dat stejně jako u třídy B1, ale zde je nutné takto řídit přístup ke všem objektům. Je zde požadována také analýza skrytých kanálů a realizace zabezpečené cesty při proceduře login.

Třída B3 : Bezpečnostní zóny – Tato třída hodnocení zabezpečení informačního systému omezuje přístup jakéhokoliv subjektu k objektům danému systému pouze prostřednictvím jediného zařízení, které je zde nazváno jako referenční monitor. Od systému jsou zde i požadovány procedury bezpečného zotavení. Třída B3 je vysoce odolná proti proniknutí neoprávněného subjektu.

- **Skupina C: Výběrová ochrana**

  Skupina C prezentuje systémy, které do sebe začleňují prověřovací schopnosti pomocí výběrové ochrany. Tato skupina obsahuje dvě třídy:

  Třída C1: Zabezpečení ochrany výběrem – Prezentuje systémy, které adekvátním způsobem oddělují uživatele a data. Tato skutečnost v sobě zahrnuje řízení přístupových omezení takovým způsobem, aby uživatel mohl chránit svoje soukromá data před náhodným čtením či manipulací jiným uživatelem.

  Třída C2: Ochrana řízeným přístupem – Zpřísňuje zabezpečení systému především v požadavku na autentifikaci uživatele. Zejména klade důraz na autenfikaci

na úrovni celého systému, nikoliv pouze na úrovni jednotlivých programů. Na základě autenfikace mohou tyto systémy vést i logování, a umožňují tedy zpětné dohledání významných událostí.

- **Skupina D: Minimální ochrana**
  Skupina D prezentuje systémy, poskytující minimální ochranu a které nevyhověly požadavkům žádné vyšší skupiny. Jedná se tedy z pohledu zabezpečení o nejméně zajištěné systémy.

Uvedené rozdělení v rámci kriterií TCSEC je uvedeno v tzv. „Orange Book“. Tato kniha tvoří základ standardu TCSEC, a je to jeden z prvních dokumentů pro hodnocení zabezpečených systémů. Tvoří tak tedy základ pro tuto problematiku. Tato publikace byla vytvořena v rámci „Duhové série“ návazných norem, kde orange book tvoří základní stavební prvek této série.

Rozdělení systémů do 7 uvedených tříd podle jejich bezpečnosti se ale týká celé duhové série, respektive tedy všech zhruba 25ti publikací, nikoliv pouze knihy orange book. Všechny publikace z této série na toto rozdělení přímo navazují, či je upravují zpřesňováním a vysvětlováním bezpečnostních požadavků. Jedná se například o následující publikace série:

Trusted Database Interpretation – tato publikace definuje standardy bezpečnosti pro databázové aplikace a programy.

Trusted Network Interpretation (Red Book) – červená kniha, popisuje zejména problematiku důvěryhodnost počítačových sítí

Password Management Guideline (Green Book) – zelená kniha, směrnice pro správu hesel

TCSEC in Specific Environments (Yellow Book) – žlutá kniha která obsahuje směrnice pro aplikaci standardu TCSEC ve specifických prostředích a podmínkách.

Standard TCSEC pro hodnocení úrovně zabezpečení vznikl již roku 1983, a ačkoliv již tedy není zdaleka aktuální a neodpovídá neustále se rozvíjejícím informačním technologiím,

obsahuje cenné principy, které jsou v platnosti i v dnešní době. Jeho základní principy následně přebírají i další standardy a kritéria hodnocení. Jedním z takovýchto standardů jsou i kriteria CTCPEC či ITSEC, které ale čerpají především ze zkušeností několika zakladatelských států v Evropě.

3.4.2 CTCPEC (Canadian Trusted Computer Product Evaluation)

Kanadská verze kritérií pro hodnocení bezpečnosti informačních systémů se pokusila sestavit použitelnější kategorizaci v této problematice. Pro orientaci a inspiraci využila i již existující kriterii TCSEC která v době vzniku kanadské verze již poměrně spolehlivě fungovala. První verze kriterií CTCPEC byla vydaná v roce 1989. Současná aktuální verze poskytuje velice kladně hodnocené měřítka pro hodnocení bezpečnosti. Podobně jako u pozdějších kriterií ITSEC, jsou kanadská kriteria rozdělena na dvě základní části. Jedná se o část funkčnosti, zde nazvanou jako bezpečnostní služby, a záruku zabezpečení [13,9,8].

Část věnována funkčnosti využívá rozdělení do skupin, kde je pro každou funkci stanoveno několik úrovní. Toto rozdělení vychází z podobného základu jako princip CIA, tedy z důvěrnosti (Confidentality), integrity (Integrity), dostupnosti (Avaibility), a nově ještě přidává část odpovědnost [13,9], případně je tato část v některých zdrojích označenou i pod názvem účtovatelnost [8].

- **Funkce zajištující důvěrnost** jsou určeny pro zamezení přístupu a poskytnutí dat neoprávněným subjektům. Jinými slovy to jsou tedy takové funkce, které zajišťují, že informace budou poskytnuty pouze takovým uživatelům, které jsme oprávnili. Celkem se jedná o čtyři bezpečnostní funkce:

    - **Skryté kanály** (Obsahující úrovně CC-0 až CC-3) představují bezpečnostní funkci zabývající se identifikací datových toků a eliminací takových toků, které jsou v rozporu s bezpečnostní politikou. Tato funkce se vyskytuje pouze u systému s povinným řízením přístupu.

- **Nepovinné řízení důvěrnosti** (úrovně CD-0 až CD-4) je bezpečnostní funkce obsahující mechanismy nepovinného řízení přístupu k datům. Přičemž se může jednat například o seznamy přístupových práv či přístupové matice. Všechny tyto funkce ale musejí jednoznačně přispívat k zajištění důvěrnosti dat.

- **Povinné řízení důvěrnosti** (CM-0 až CM-4) prezentuje funkci starající se o povinné řízení přístupu k informacím. Přičemž se může jednat například o mechanismy využívající stupně klasifikace spravovaných objektů na základě jejich významu a snaze utajení

- **Opětovné použití objektů** (CR-0 až CR-1) představuje funkci, která zajišťuje, že žádný objekt nebo proces, který je přidělený uživateli, neobsahuje informace od předchozího vlastníka objektu.

- **Funkce zajištující integritu** jsou určeny pro potlačování možností neoprávněné modifikace dat, respektive slouží pro stanovení omezení týkající se provádění modifikace a manipulace s daty. Tato část obsahuje sedm bezpečnostních funkcí.

  - **Doménová integrita** (IB-0 až IB-2) je funkce, která přesně definuje důvěryhodnou výpočetní bázi (Trusted Computing Base) v rámci informačního systému. Zejména stanovuje její schopnost ochrany před útokem a správu chráněných objektů.

  - **Nepovinné řízení integrity** (ID-0 až ID-4) prezentuje bezpečnostní funkce, které obsahují mechanismus nepovinného řízení přístupu k informacím a přispívající k zajištění integrity dat. Jedná se například o přístupové seznamy, matice, nebo i o komplexní seznamy přístupových práv podobně jako u nepovinného řízení důvěrnosti.

  - **Povinné řízení integrity** (IM-0 až IM-4) zahrnuje mechanismy povinného řízení přístupu k informacím sloužící pro zajištění datové integrity. Podobně jako u povinného řízení důvěrnosti se jedná například o funkci klasifikace a členění spravovaných objektů na základě jejich povahy

- **Fyzická integrita** (IP-0 až IP-4) definuje fyzický ochranný perimeter informačního system či jeho části, a poskytuje služby vedoucí k ochraně komponent ležící uvnitř vytyčeného perimetru na základě.

- **Návrat** (IR-0 až IR-2) prezentuje schopnost informačního systému, či jeho části, vrátit se k předchozímu správně fungujícímu stavu. Tato schopnost je důležitá zejména při chybových či katastrofálních situacích kdy není možná oprava.

- **Oddělení rolí** (IS-0 až IS-3) je bezpečnostní funkce, zajištující rozdělování pravomocí a odpovědnosti v rámci definovaných uživatelských rolí. Omezují se tím možné potenciální škody způsobené nežádoucím chováním uživatele či správce informačního systému. Omezuje rovněž i škody v případě odcizení identity.

- **Autonomní testování** (IT-0 až IT-3) prezentuje bezpečnostní mechanismy různých funkcí sloužící k testování. Testováním se zjišťuje, zda se hardware i software v našem systému nachází ve správném a zabezpečeném stavu, a zda nehrozí bezpečnostní riziko.

- **Funkce zajištující dostupnost** mají za cíl zajistit přístup k informacím či službám informačního systému, na základě uživatelských oprávnění, a zabránit i případnému neoprávněnému odepření. Jedná se o čtyři následující funkce.

  - **Přidělování prostředků** (AC-0 až AC-3) prezentuje bezpečnostní funkci, která kontroluje přidělování systémových zdrojů mezi jednotlivé uživatele a zajišťuje i jejich využívání.

  - **Tolerance k chybám** (AF-0 až AF-23) představuje vlastnost systému, vyjadřující jeho schopnost přizpůsobení se chybovým stavům. Respektive

schopnost výměny vadných částí či komponent systému, bez nutnosti přerušení poskytovaných služeb.

- **Robustnost** (AR-0 až AR-3) prezentuje schopnost systému zajišťovat dostupnost informací a služeb i po výpadky některých dílčích komponent systému.

- **Zotavení** (AY-0 až AY-3) je další z bezpečnostních služeb zajištující dostupnost informací a služeb, a prezentuje vlastnost systému vrátit se do důvěryhodného stavu po výpadku způsobeného poruchou nebo chybou.

- **Funkce zajištující účtovatelnost** zahrnují zodpovědnost uživatelů za jimi vykonané akce, které v systému provádějí, a zároveň umožňují jejich zpětné dohledání. Tato část obsahuje tří následující funkce.

  - **Audit** (WA-0 až WA-5) zajišťuje detekci a zaznamenávání důležitých událostí z hlediska bezpečnosti, včetně jejich pozdější analýzy. Hlavním principem je mechanismus zajištující protokolování vykonaných událostí, a uchovávání jejich záznamu.

  - **Identifikace a autentizace** (WI-0 až WI-3) prezentuje schopnost systému důvěryhodně ověřit uživatelovu identitu, na jejímž základě mu jsou následně přiděleny pravomoce a odpovědnost.

  - **Důvěryhodná cesta** (WT-0 až WT-3) poskytuje uživatelovi možnost přímé a bezpečné komunikační trasy s centralizovaným informačním systémem.

Tímto způsobem zde definované bezpečnostní služby mohou sloužit jako protiopatření k zajištění bezpečnosti. Tato skutečnost přímého adresování služeb jako protiopatření k možným hrozbám, je typickým dominantním rysem kanadských kriterií.

Další důležitou částí dokumentu CTCPEC je vedle bezpečnostních funkcí i záruka zabezpečení. Tato záruka je dána kvalitou už konkrétního návrhu, vývojovým a provozním prostředím, rozsahem dokumentace a testováním. Jednotlivé úrovně záruky jsou značeny od skupiny T-1 až do T-6. Skupina T-1 je oklasifikována jako nevyhovující, a skupina T-6 jako nejlepší dosažitelná třída míry záruky zabezpečení daného informačního systému (obsahující přesný formální model návrhu systému a jasný popis implementace včetně návazností a zvoleného designu).

Téměř souběžně jako vznikla kanadská kriteria CTCPEC, začala vznikat i obdobná evropská iniciativa spojena s kritériemi ITSEC. Zatímco kanadská verze vznikla v roce 1989, vznik první verze evropských kritérií následoval o rok později (jako doporučení byla ale schválena až v roce 1995). Dá se tedy říci, že tyto standardy vznikaly téměř současně, a řešily stejnou problematiku lišící se jen geografickou polohou. Často se také uvádí skutečnost, že vzhledem k podobné době vzniku se autoři obou standardu v jistých oblastech vzájemně inspirovali. V daleko větší míře se ale autoři jistě inspirovali již fungujícími kritériemi TCSEC, která vznikla jako první na území USA již v roce 1983 a představovala bohatý zdroj informací a zkušeností.

3.4.3 ITSEC (Information Technology Evaluation Criteria)

Zkušenosti fungování evropského společenství před dobou vzniku normy ITSEC ukázali problémy, způsobené nejednotným přístupem k problematice zabezpečení informačních systémů jednotlivých zemí Evropského společenství. Tyto problémy vykazovaly především nadnárodní společnosti, působící ve více zemích Evropy. Tehdejší situace je nutila respektovat poměrně velké množství vzájemně se lišících standardů a norem. Základní prvky hodnocení bezpečnosti byly ale ve všech zemích stejné. Proto logicky následovala iniciativa, které měla vytvořit nový standard, který by byl platný pro celé Evropské společenství.

Výsledkem této iniciativy byla norma ITSEC, neboli kriteria hodnocení informační technologie (Information Technology Evaluation Criteria). Tato kriteria byla vytvořena v roce 1990 a ihned předána k případným připomínkám a diskusi. Tato první podoba standardu byla v podstatě sjednocená verze národních kriterií, přijatých zatím pouze ve Francii, Německu,

Velké Británii a Nizozemsku. Po menších úpravách byla tato kriteria již v červnu roku 1991 vydána Úřadem pro oficiální publikace Evropského Společenství, ale pouze jako prozatímní materiál k ověření. V podobě doporučení byla schválena a vydána až v dubnu roku 1995.

V souvislosti se standardem ITSEC je ale nutné také zmínit prováděcí manuál, vydaný opět Úřadem pro oficiální publikace Evropského společenství v roce 1993. Tato publikace je vypracována jako nadstavba nad kriterii ITSEC verze 1.2. Vyšla po názvem Information Technology Security Evaluation Manual, neboli pod zkratkou ITSEM. Jejím cílem bylo usnadnit proces hodnocení daného systému či subjektu, samozřejmě plně v souladu s kriterii ITSEC. Tento prováděcí manuál obsahuje zejména vhodnou metodologii pro hodnocení zabezpečení informačních systémů, a navazuje tak na stanovené kritéria ITSEC, na jejichž základě se toto hodnocení provádí.

Standard ITSEC pod pojmem informační technologie nechápe ale pouze fyzický hardware. Tento pojem je zde chápán jako konkrétní instalace technologie, za určitým účelem, ale bez bližších znalostí provozního prostředí. Jinými slovy pod pojmem informační technologie je zde chápán hardware i software, nezávisle na místě jeho konkrétní implementace. O jeho provozním prostředí lze tedy vyslovit pouze obecné předpoklady.

Podobně jako TCSEC obsahuje také standard ITSEC jednotlivé třídy. Tyto třídy vycházejí přímo z kriterií specifikovaných v German National Criteria (Německá národní kritéria – ZSIEC). Svým obsahem a podobou se ale blíží i požadavkům na jednotlivé třídy v rámci TCSEC. Před provedením samotného hodnocení a přiřazení třídy je nutné nejdříve zjistit předmět hodnocení. Pro tyto potřeby zjištění předmětu hodnocení existuje zavedený postup v rámci standardu ITSEC:

- Zadavatel specifikuje operační prostředí systému
- Hodnotitelé se seznamují s prostředím, ve kterém má být systém implementován. (Především z důvodu poznání potenciálního nebezpečí a rizika, která musí být ošetřena.)
- Stanovení bezpečnostního cíle systému, zejména na základě legislativy a dalších platných předpisů či norem.

- Zadavatel specifikuje úroveň nebo referenční model, podle kterého chce systém hodnotit

Všechny důležité aspekty systému, které jsou předmětem hodnocení, specifikuje bezpečnostní cíl. Tento cíl, respektive dokument, popisuje bezpečnostní funkce a předpokládané hrozby. Musí také obsahovat detailní informace o použitých mechanismech, včetně dílčích bezpečnostních cílů. Bezpečnostní cíl tedy musí obsahovat následující prvky:

- Definici dílčích bezpečnostních cílů, v souladu s bezpečnostní politikou.
- Definici provozního prostředí
- Popsané a specifikované bezpečnostní funkce
- Požadované bezpečnostní mechanismy a stanovení minimální účinnosti
- Požadovanou třídu, která zaručuje danou míru bezpečnosti

Všechny třídy bezpečnosti definují i podklady, které musí hodnocený hodnotiteli poskytnout. Předpokládá se zde úzká spolupráce mezi těmito dvěma subjekty. Přičemž výsledkem hodnotícího procesu je výrok, zda daný předmět hodnocení splňuje nebo nesplňuje svůj definovaný bezpečnostní cíl.

Poměrně velký výhoda standardu ITSEC spočívá v oddělení požadavku na míru zaručitelnosti bezpečnosti a na bezpečnostní funkčnost. Do jisté míry jsou tedy kriteria ITSEC dvojrozměrná, což znamená, že u každého objektu lze odděleně hodnotit jak funkčnost, tak i míru zaručení bezpečnosti. Tato vlastnost je považována za jednu z největších výhod kriterií ITSEC, zejména v porovnání s jednorozměrnými TCSEC. Ve standardu TCSEC je totiž definována pouze jedna hierarchie tříd, která obsahuje jak požadavky na míru zaručitelnosti bezpečnosti, tak i požadavky na funkčnost. Tato skutečnost může vadit některým uživatelům, neboť nemají možnost tyto požadavky definovat jednotlivě, ale na základě požadavku na funkčnost jsou pevně stanoveny i požadavky na míru zaručitelnosti zabezpečení. Přičemž požadavky na zaručitelnost míry zabezpečení mohou být i značně neadekvátní požadavkům uživatele na funkčnost. V případě standardu ITSEC si uživatel volí tyto prvky samostatně a odděleně nezávisle na sobě, a může si zvolit skoro libovolnou kombinaci těchto dvou požadavků.

V rámci ITSEC jsou tedy definovány třídy, které prezentují konkrétně sedm možných úrovní zabezpečení. Jejich značení probíhá pomocí jednoho písmena (E) a číslice (0 - 6). Rozsah značení je tedy od úrovně nejnižší E0 do nejvyšší E6.

- **Třída E0** – Představuje nejnižší, respektive tedy nedostatečnou úroveň zabezpečení hodnoceného systému. Jedná se o třídu, která je automaticky přirazena systémům, které nesplňují žádnou z dále uvedených podmínek tříd vyšších, nebo systémům u kterých není možné hodnocení provést.

- **Třída E1** – Tato třída ukládá povinnost existence bezpečnostního cíle a minimálně neformálního popisu struktury navrženého systému. Dále musí být také pomocí testování prokázáno, že hodnocený předmět splňuje definovaný bezpečnostní cíl.

- **Třída E2** – Touto úrovní zabezpečení je ohodnocen systém, který splňuje podmínky třídy E1 a navíc obsahuje popis detailního návrhu, který může být jen v neformální podobě. Systém by měl také poskytovat konfigurační nástroje, a hodnotiteli se musí dodat důkazy o testování.

- **Třída E3** – Prezentuje skutečnost, že kromě již výše uvedených podmínek nižších tříd musí být navíc provedeno i testování bezpečnostních mechanismů. Další podmínka spočívá v dostupnosti detailního návrhu a zdrojových textů programu poskytujících bezpečnostní funkce.

- **Třída E4** – Pro ohodnocení systému touto úrovní zabezpečení musí už existovat formální model bezpečnostní politiky systému. Je zde ale i povinnost mít minimálně semiformální provedení návrhu architektury a provedení analýzy zranitelnosti na této úrovni.

- **Třída E5** – Zde je navíc povinnost, kde detailní návrh systému musí úzce odpovídat finální implementaci na úrovni zdrojových textů programu. Na této úrovni se musí provést i další analýzy zranitelnosti.

- **Třída E6** – Systémy této třídy musí obsahovat formální popis návrhu bezpečnostní architektury a funkcí zajišťující bezpečnost. Tento popis musí být zároveň plně v souladu s formálním modelem bezpečnostní politiky. Pro udělení této třídy musí být ještě jednoznačně prokázána souvislost výkonových programů s jejich zdrojovými formami.

Kriteria TCSEC i ITSEC se tedy dělí na sedm tříd, a existuje mezi nimi jistá podobnost. Ačkoliv jsou tyto třídy značeny rozdílně, mají podobné vlastnosti. V případě ITSEC je nejnižší třída zabezpečení E0, a u kriterií TCSEC je na nejnižší úrovni zase třída D.

ITSEC	TCSEC
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-A1, E6	A1

Obr. 7 – analogie mezi třídami standardů ITSEC a TCSEC [14]

Kriteria ITSEC ale nebyla přijímána pouze v pozitivním směru. Poměrně často byla i kritizována a bylo poukazováno i na různé nedostatky či nepřesnosti. Jako první lze zmínit hned připomínku, že nejde tak zcela o kriteria v pravém smyslu a dokument neodpovídá zcela svému názvu. Sice dokument ITSEC obsahuje dohodnutá kritéria, v části ve které jsou definovány třídy míry zaručitelnosti, ale ty jsou obsaženy pouze v poměrně malé části tohoto standardu. V dalších částech, zejména v části týkající se bezpečnostní funkčností, obsahuje dokument spíše návod jak vypracovat kriteria vlastní, a nedává tak dostatečný důraz na již stanovená kriteria na základě mezinárodní dohody.

Druhý bod, který je také poměrně často kritizován, je skutečnost, že dokument ITSEC nezahrnuje informační systémy s distribuovanou správou**.** Tedy se vůbec nezabírá problematikou vzájemně propojených informačních systémů s několika správci.
Jedná se sice o poměrně obtížně popsatelnou a novou problematiku, ale bylo by vhodné, aby se jí dokument zabýval, pokud na něj má být pohlíženo jako na komplexní dokument pro hodnocení zabezpečení informačních systémů.

Následně je také poukazováno na definovaný pojem integrita v dokumentu ITSEC. Ten je zde definován jako „ prevence proti neautorizované modifikaci informace“, což je sice definice, která se objevuje i v jiných zdrojích, a z prvního pohledu se zdá správná, ale není určitě nejlepší. Její poměrně nešťastná definice se projevuje zejména u distribuovaných informačních systémů. U těchto systémů většinou nelze zabránit neautorizované modifikaci dat bez použití velmi nákladných a prakticky nerealizovatelných fyzických bezpečnostních opatření. Jediné co se zde dá udělat pro zajištění integrity je neautorizovanou modifikaci dat detekovat, a následně celé datový přenos opakovat. Pokud případně dále, i při každém pokusu o přenos dat dojde k neoprávněné modifikaci informace, je porušena dostupnost, nikoliv integrita. Z tohoto důvodu, kdy chceme zahrnout i distribuované informační systémy, bývá uváděna vhodnější definice, která definuje integritu jako prevenci proti neodhalené a neautorizované modifikaci informace. Lehkou změnou definice integrity by se tedy dosáhlo jednoznačnějšího rozlišení mezi pojmy integrita a dostupnost. Při zavedené této změny je možné navíc dosáhnout shody pojmu s dobře definovanými pojmy z problematiky dokazování programů. Integrita by zde odpovídala pojmu částečná správnost, a dostupnost spolu s integritou by zase už odpovídala pojmu úplná správnost (partial a total correctness).

Další z problematických částí je část obsahující generická záhlaví pro bezpečnostní funkce. Tyto záhlaví zde totiž nejsou obsažena všechna a nejsou ani vytvořena systematicky. Chybějí zde zejména některé duální bezpečnostní funkce. K funkcím identifikace a autentizace zde schází funkce anonymita a pseudonymita, a dále ještě k funkci audit zde chybí jeho duální funkce nemožnost sledování. Poté i zařazení funkce výměna dat mezi ostatní bezpečnostní funkce je poměrně nešťastné. Tato funkce je totiž na zcela jiné úrovni. Navíc k ní opět chybí i odpovídající duální funkce ukládání dat. Shrneme-li tyto poznatky, docházíme k poznatku, že klasifikace bezpečnostních funkcí by měla být doplněna s ohledem na fakt, aby umožňovala hodnocení takových informačních systému, které vyžadují nebo poskytují anonymitu, pseudonymitu či nemožnost sledování.

Posledním bodem kritiky je deset příkladů tříd funkčnosti, které jsou uvedené jako příloha dokumentu ITSEC. Pro uživatele to není dostatečný materiál. Uživatelé sice mají možnost definovat si své vlastní třídy funkčnosti, ale pouze velmi malé procento je schopno tento proces provést. Uvedených deset příkladů zde ještě navíc může budit i dojem, že se jedná o kompletní a ucelenou sadu tříd, které pokrývá celou problematiku. To ale není pravda, jedná se opravdu pouze o příklady.

ITSEC standard pro hodnocení informační bezpečnosti se v aktualizované podobě používal od roku 1991 postupně na celém území Evropské unie. V současnosti ale význam ITSEC již pomalu upadá. Postupně jsou tato kritéria nahrazována novějším standardem, a to sice normou CC (Common Criteria). Vzniku CC kriterií ale předcházeli ještě dvě podobné iniciativy. Za kanadský územní celek to byla již zmíněná CTCPEC kriteria, a za území spojených států amerických vedle také již uvedených TCSEC ještě kriteria označována pod zkratkou FC.

3.4.4 FC (Federal Criteria)

Federal Criteria jsou další kriteria určená pro hodnocení bezpečnosti informačních systémů, vzniklá na území USA. Na jejich vzniku se podíleli zejména organizace NSA (National Security Agency) a NIST (National Institute of Standards and Technology). Kriteria FC vznikla jako náhrada za standard TCSEC, a jejich první vydání bylo uskutečněno v roce 1992. Nikdy se však nedočkala většího uplatnění, protože celosvětově uznávaným standardem se následně stala společná kriteria CC (Common Criteria). Společná Kriteria ale mnohé nápady z kritérií FC převzala, zejména je nutné zmínit zavedené profilu ochrany označovaného zkratkou PP (Protection Profile).

Samotná FC kriteria jsou rozdělena na dvě základní části. Jedná se o část vlastní kriteria, a část druhou, která je pojmenovaná jako bezpečnostní profil.

- **První oddíl - vlastní kritéria.** Tento oddíl rozlišuje sedm možných úrovní záruk zabezpečení informačního systému. Jedná se o podobně značené úrovně jako v případě kriterií CTCPEC, která rozlišovala úrovně T-1 až T-6. V případě FC

standardu se ale stupnice ještě o jeden stupeň zvětšila, a obsahuje tedy úrovně od nejnižší T-1 až do úrovně poskytující nejvyšší záruku T-7. Tato část, ve které jsou popsána vlastní kriteria, obsahuje i následující požadavky:

- **Požadavky na funkčnost složky** – Tyto požadavky jsou v tomto dokumentu členěny podle jednotlivých bezpečnostních funkcí.
- **Požadavky na vývoj systému** – Zahrnují požadavky na vývojový proces, dokumentaci, vývojové prostředí a také na provozní podporu daného informačního systému.
- **Požadavky na hodnotitelské záruky** – Obsahují prvky testování systému, a zahrnují i hodnotitelské posudky a analýzy.

- **Druhý oddíl – bezpečnostní profily.** Tato část poskytuje komplexní vyjádření obecných bezpečnostních vlastností, včetně přiblížení základních rysů připravených bezpečnostních profilů bezpečnosti. Bezpečnostní profily se zde dělí na profily pro komerční použití a na profily pro systémy víceúrovňové bezpečnosti. Zahrnují popis účelu, podmínek použití a požadavků na bezpečnostní funkce.

3.4.5 CC (Common Criteria)

Tato norma představuje nejnovější standard pro hodnocení úrovně zabezpečení informačních systémů. Jejich vznik představoval snahu o vytvoření jednotného standardu pro hodnocení bezpečnosti informačních systémů s co největším možným rozšířením. Jak již bylo uvedeno u předchozích kriterií, CC standard vychází z již dříve používaných kriterií TCSEC, FC, ITSEC a CTCPEC. Jeho vznik se datuje k roku 1996, kdy byla vydána první verze dokumentu známého pod názvem Common Criteria for Information Technology Security Evaluation. Tato prvotní verze vydaná v roce 1996 byla vzhledem ke své rozsáhlosti ale poměrně nepoužitelná a velmi často kritizována. Z tohoto důvodu následovalo pozdější přepracování, a v roce 1998 byla vydána verze pod číselným označením 2.0. Tato verze se o rok později dočkala i normalizování, pod označením ISO/IEC 15408-1:1999.

Jako místem vyvinutí a vzniku dokumentu Common Criteria je označované území USA. Jednalo se ale o iniciativu celé řady různých národních institucí zabývající se bezpečnostní a

standardizací, nejenom v rámci USA. Na vývoji CC se podíleli zejména následující země [12]:

- **Spojené státy americké** – v zastoupení národního standardizačního a technologického institutu NIST (National Institute of Standards and Technology) a národní bezpečnostní agentury NSA (National Security Agency).
- **Kanada** – v zastoupení organizace zodpovědné za komunikační bezpečnost CSE (Communication Security Establishment)
- **Francie** – Centrální služba pro ochranu informačních systémů SCSSI (Service Central de la Security des Systemes d'Information)
- **Německo** – Spolkový úřad pro informační bezpečnost BSI (Bundesamt für Sicherheit in der Informationstechnik)
- **Nizozemí** – Holandská národní bezpečnostní a komunikační agentura NLNCSA (Netherlands National Communications Security Agency)
- **Velká Británie** – Oddělení britského vládního komunikačního ústředí GCHQ pracující na zabezpečení komunikačních a informačních systémů CESG (Communications-Electronics Security Group)

Následně vznikla nová verze pod označením 2.3 v roce 2005. Podle mnohých se jednalo o poměrně přelomovou a velmi významnou verzi kriterii CC. Obsahovala tři části, a všechny se dočkali i vydání ve formě mezinárodní normy ISO/IEC po názvy 15408-1:2005, 15408-2:2005, 15408-3:2005. Tato verze zásadním způsobem změnila strukturu a uspořádání bezpečnostních cílů a přinesla rovněž katalog bezpečnostních funkcí spolu s katalogem požadavků na záruku.

V současné době je k dispozici nejnovější verze 3.1, která byla vydána v roce 2006 a revidována naposled v červenci 2009. Z této skutečnosti je vidět že se jedná o aktuální a stálé aktualizovaný standard pro hodnocení bezpečnosti informačních systémů. Tato dosud nejnovější verze přinesla změny především v poslední třetí části – v části požadavků na záruku bezpečnosti IS. Ke změně došlo i v oblasti bezpečnostního cíle ST (Secure Target).

Samotný dokument CC obsahuje tři části:

1. Úvod a všeobecný model
2. Bezpečnostní funkční požadavky
3. Požadavky na záruky bezpečnosti

V první části jsou definovány jednotlivé použité pojmy, a je zde vysvětlena základní filosofie CC. Také je zde představen obecný model hodnocení. Poměrně důležitou součástí je také přiblížení základních stavebních prvků, sloužící pro jednotnější vyjádření bezpečnostních požadavků. Jedná se o: [14]

- **Prvek** (element) - bezpečnostní požadavek ověřitelný při hodnocení, který je v elementární podobně a není tudíž dále dělitelný.

- **Komponenta** (component) - představuje nejmenší množinu prvků, pro účely zahrnutí do vyšších struktur CC

- **Rodina** (family) - prezentuje určité seskupení komponenet , které slouží k naplnění stejného cíle, ale lišící se přísností požadavků.

- **Třída** (class) - seskupení rodin komponent pokrývající jednotlivé dílčí cíle a tvořící konsistentní celek pro dosažení celkového cíle.

Tato první část definuje také velmi důležitý pojem profil ochrany (Protection profile, zkráceně PP). Tento pojem prezentuje množinu bezpečnostních požadavků pro účely dosažení definovaných cílů. Tyto požadavky mohou být jednak vybrány z CC, či vyjádřeny explicitně. Měly by zahrnovat i míru záruky, zde označené jako EAL (Evaluation Assurance Level). Profil ochrany se vytváří zpravidla takovým způsobem, aby bylo možné jeho opakovatelné použití.

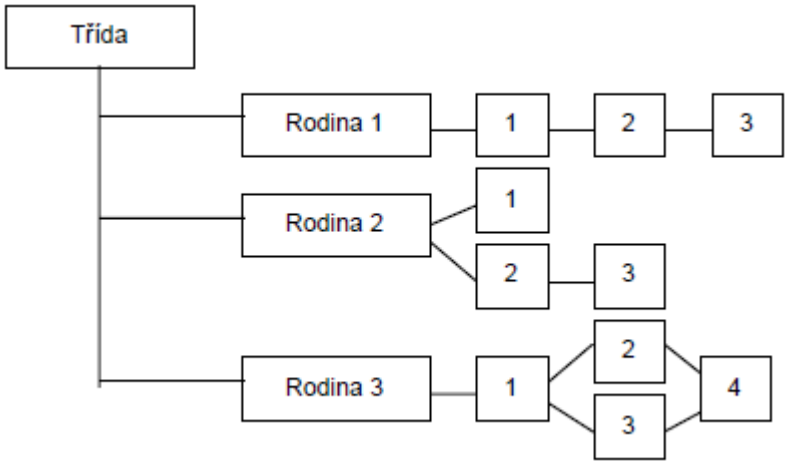
Druhým možným seskupením bezpečnostních požadavků je balík (package). Ten představuje kombinaci komponent z funkční části, nebo z oblasti záruk, které je sestavena pro opakované použití za účelem splnění definovaných bezpečnostních cílů. Charakter tohoho balíku má opět míru zaruky (EAL).Jako další důležitý pojem je nutné ještě doplnit předmět

hodnocení (Target of evaluation, zkráceně TOE). Na něj navazuje zase bezpečnostní cíl (Security target, ST), který definuje bezpečnostní požadavky, které jsou realizovány právě v rámci předmětu hodnocení.

Ve druhé části dokumentu CC jsou zahrnuty funkční komponenty. Tyto komponenty jsou používány jako standardní způsob vyjadřování funkčních požadavků, přičemž v této druhé části je obsažen jejich kompletní výčet ve formě katalogu, spolu s třídami a rodinami. Katalog obsahuje následujících jedenáct funkčních tříd: [8]

- **Třída FAU :** Bezpečnostní audit (Audit)
- **Třída FCO** : Komunikace (Communications)
- **Třída FCS :** Kryptografická podpora (Cryptographic support)
- **Třída FDP :** Ochrana uživatelských dat (User data protection)
- **Třída FIA :** Identifikace a autentizace (Identification and authentication)
- **Třída FMT :** Správa bezpečnosti (Security management)
- **Třída FPR :** Soukromí (Privacy)
- **Třída FPT :** Ochrana bezpečnostní funkcionality TOE (Protection of the TOE security functions)
- **Třída FRU :** Využívání zdrojů (Resource utilisation)
- **Třída FTA :** Přístup k TOE (TOE access)
- **Třída FTP:** Důvěryhodné cesty / kanály (Trusted path / channels)

Každá z těchto uvedených funkčních tříd obsahuje několik rodin, přičemž se každá rodina ještě skládá z jedné nebo více komponent, které jsou uspořádány dvěmi možnými způsoby (hiearchicky či nehiearchicky).



Obr. 8 - Schéma uspořádání funkčních tříd do rodin a komponentů [8]

Jako příklad lze uvést funkční třídu audit. Ta obsahuje šest rodin, které prezentují jednotlivé aspekty auditovaní. Jedná se o automatickou reakci, generování auditních dat, analýzu auditních dat, kontrola proběhnutí auditu, výběr událostí z auditu, a uchovávaní auditních záznamů. Dále se pak například rodina generování auditních dat dělí na dvě nehiearchické komponenty, První komponenta se zabývá generováním auditních záznamů a druhá přiřazením uživatele a auditované události.

Třetí část dokumentu CC se věnuje popisu komponent pro stanovení požadavků na záruku. Obsahuje jak katalog komponent záruk, tak i jejich rodin a tříd, ale i definovaná kriteria pro hodnocení profilů ochrany (Protection profile, PP) a bezpečnostní cíle (Security target, ST). V rámci CC je pro potřeby záruk definováno osm tříd:

- Správa konfigurace (Configuration management)
- Průvodní dokumentace (Guidance documents)
- Posouzení zranitelnosti (Vulnerability assessment)
- Dodání a provoz (Deliverz and Operation)
- Popora životního cyklu (Life cycle support)
- Údržba záruky (Assurance maintenance)
- Vývoj (Development)
- Testování (Tests)

Obdobně jako u předchozí části, jsou i zde třídy členěny dále do několika rodin, které obsahují minimálně jednu komponentu. Například třída vývoj obsahuje sedm rodin, které postihují různé aspekty v rámci vývoje. Následně tyto rodiny obsahují ještě další komponenty, ale všechny komponenty jsou v rámci této části CC přísně hierarchicky uspořádány. Kromě uvedených tříd jsou ale ve třetí části uvedeny ještě další dvě, obsahující požadavky na záruky pro profil ochrany (PP) a bezpečnostní cíle (ST).

Velmi důležité je ale v rámci dokumentu CC sestavení hodnotící stupnice pro úroveň zabezpečení. CC za tímto účelem poskytuje předdefinovaný balík (Assurance package). Tato stupnice je známá jako Evaluation Assurance Levels, neboli míra záruky EAL. Tato stupnice je velmi dobře sestavená a vyvážená. Samozřejmě je obecně aplikovatelná na základě svého charakteru. Veškerá hodnocení informační techniky podle CC se provádějí právě podle stupnice EAL. Jednotlivé úrovně jsou tedy značeny následovně [8,14]:

- **EAL 1** - Tato úroveň je vhodná pro systémy či prvky informační techniky, u kterých se nepředpokládá výskyt závažnějších hrozeb. Vyjadřuje se zde základní důvěra spočívající v bezchybnosti a správnosti fungování. Pro potřeby této úrovně dochází k nezávislému testování shody bezpečnostního profilu, cílu a předmětu hodnocení s neformální funkční specifikací a především s předloženou dokumentací pro koncové uživatele. V porovnání s nehodnoceným prvkem informační techniky, představuje úroveň EAL1 výrazně vyšší míru zaručitelnosti bezpečnosti. Úspěšné ohodnocení touto úrovní je ale možné i bez kooperace a pomoci vývojářů, a finanční náročnost je zde minimální.

- **EAL 2** - Zde se již předpokládá spolupráce hodnotící laboratoře s vývojáři hodnoceného produktu. Ti musí dodat funkční specifikace o návrhu bezpečnostních funkcí spolu s jejich výsledky testování. Tato úroveň poskytuje nízkou až střední úroveň ověření bezpečnosti, a je ověřována detailnějším testováním než u úrovně EAL 1, ale také i analýzou síly funkcí a analýzou zranitelnosti. Úroveň EAL 2 tedy i vyjadřuje výrazně vyšší zaručitelnost zabezpečení než úroveň předchozí. Pro potřeby předmětu hodnocení (TOE) musí dále byt vyhotoven dokument konfigurace a vypracována procedura pro bezpečnou instalaci, generaci a spouštění.

- **EAL 3** - Prezentuje úroveň, která je ještě poměrně dosažitelná v rámci zavedených vývojových praktik. Poskytuje střední úroveň bezpečnosti, která je samozřejmě také nezávisle ověřena. Ohodnocení tímto stupněm záruky je na základě důkladnějšího zkoumání a testování bezpečnostních funkcí, v porovnání s předchozí úrovní. Dále se tyto úrovně liší ještě povinností používáním řídících nástrojů, v rámci vývojového prostředí, a zajištěním správy konfigurace. Ohodnocení touto úrovní rovněž představuje důvěru v to, že produkt nebyl jakýmkoliv způsobem narušen během vývoje. Rovněž dokumentace produktu musí být adekvátním způsobem zpracována, a nesmí z její nedokonalosti či neúplnosti plynout možné ohrožení či bezpečnostní hrozba.

- **EAL 4** - Tato úroveň je nejvyšší záruka zabezpečení, kterou lze ještě dosáhnout zpětně pro již existující produkt. Rovněž je dosažitelná v rámci kvalitní komerční vývojové praxe, průkazně založené i na využití bezpečnostního inženýrství. Obecně poskytuje střední až vysokou míru záruky zabezpečení pro hodnocený produkt či informační systém. Pro potřeby zabezpečení je ale také nutné očekávat dodatečné finanční náklady na bezpečností konstruování. Oproti EAL3 je již nutné provést analýzu všech rozhraní a analýzu detailního návrhu, včetně implementace bezpečnostních funkcí. Dále je také nutné vypracovat neformální model bezpečnostní politiky a dodat minimálně část zdrojového kódu bezpečnostních funkcí. Provádí se také nezávislá analýza zranitelnosti prokazující odolnost proti útokům s nízkým potenciálem. Tato úroveň je vhodná pro produkty s očekávaným středním až velkým rizikem napadení.

- **EAL 5 –** Zde se již vyžaduje aplikace speciálních technik v rámci bezpečnostního inženýrství ve středním rozsahu. Produkty, které dosahují této úrovně, už ve většině případů mají v rámci vývoje definovaný TOE s ohledem právě na dosažení stupně EAL5. Oproti EAL 4 se zde ale neočekává nějaké výraznější zvýšení úrovně nákladů v důsledku zahrnutí speciálních bezpečnostních technik. Dále je zde oproti předchozí úrovni vyžadováno dodání kompletní implementace TOE, formální model bezpečnostní politiky, poloformální prezentace funkčních specifikací a poloformální globální návrh. Nezávislá analýza zranitelnosti, která musí být také samozřejmě provedena, musí prezentovat odolnosti proti útokům se středním potenciálem. Je zde také navíc vyžadována analýza skrytých kanálů a analýza modularity návrhu. Tato

úroveň EAL5 se aplikuje tam, kde se vyžaduje vysoká úroveň bezpečnosti, či je očekáváno velké riziko napadení systému či produktu.

- **EAL 6 –** Prezentuje úroveň, která má sloužit pro ochranu vysoce hodnotných aktiv organizace. Tímto je zároveň zdůvodněna poměrně vysoká úroveň nákladů. Oproti předchozí úrovni je vyžadován detailní návrh v poloformální podobě, více rozsáhlejší testování, prezentace implementace ve strukturované podobě a návrh TOE v modulární a zvrstvené podobě. Následně provedené analýza zranitelnosti musí prezentovat vysokou odolnost proti možnosti průniku útoku s vysokým potenciálem, a být úplná. Také provedení další analýzy skrytých kanálů musí být systematická.

- **EAL 7 –** Představuje nejvyšší možnou míru záruky zabezpečení. Používá se v rámci extrémně rizikového prostředí, nebo případně tam, kde vyšší hodnota aktiv ospravedlňuje i vysoké náklady na dosažení této úrovně. Praktická použitelnost této úrovně zabezpečení je ale v současné době omezena na produkty či informační systémy s úzce zaměřenou bezpečností funkcionalitou, kterou je možné velmi rozsáhle a formálně analyzovat. Požaduje se tedy plná formalizace, spočívající ve formálním modelu bezpečnostní politiky, formálním pojetí funkčních specifikací a formální či minimálně poloformální demonstraci korespondence. Je vyžadován i detailní návrh produktu v poloformální podobě, přičemž by měla být provedena i minimalizace jeho složitosti. Zároveň musí být také dosaženo kompletního a nezávislého potvrzení výsledků všech předložených testů.

Na hodnocení produktu mají zájem tři základní skupiny. Jsou to zákazníci, vývojáři a hodnotitelé, přičemž dokument CC je přizpůsoben takovým způsobem, aby uspokojil potřeby všech tří skupin. Všechny skupiny jsou chápány jako primární uživatelé kriterií CC.

- **Zákazníci** používají kriteria CC zejména při výběru požadavků na bezpečnost, kterými vyjadřují své potřeby. Zároveň jsou tato kriteria sestavena tak, aby zajistila splnění jejich potřeb, což je zároveň i prvotním záměrem procesu hodnocení. Výsledné ohodnocení konkrétního produktu mohou zákazníci použít k rozhodnutí, zda produkt splňuje či nesplňuje jejich požadavky, ale je použitelné i pro vzájemné porovnávání různých produktů. Zákazníkovi požadavky většinou

plynou z provedené analýzy rizik, či politických rozhodnutí. Common Criteria také poskytují skupinám zákazníků se shodnými zájmy implementačně nezávislé struktury – profily ochrany (PP), ve kterých mohou vyjádřit své speciální požadavky na zabezpečení.

- **Vývojáři** využívají Common Criteria jako pomocný nástroj pro přípravu hodnocení vyvíjeného produktu, ale také i jako prostředek pro identifikaci adekvátních požadavku na bezpečnost. Vývojář může prostřednictvím nástrojů zavedených v CC připravit důkazový materiál pro podložení tvrzení, že vyvinutý produkt vyhovuje stanovenými bezpečnostními funkcemi a zárukou bezpečnosti identifikovaným požadavkům. Pro účely právě těchto požadavků zavádí dokument CC nezávislou strukturu, označovanou jako bezpečnostní cíl (ST). Požadavky více zákazníků s podobným zaměřením zase podporují definované struktury profilů ochrany (PP).

- **Hodnotitelé** mají možnost používaní dokumentu CC pro posuzování, zda produkty či informační systémy odpovídají svým bezpečnostním požadavkům. Dokument CC rovněž popisuje činnosti, které hodnotitel musí provést v zájmu zachování dobré úrovně hodnotícího procesu. Nestanovuje ale přesné postupy při takovém hodnocení, a pro tyto účely vznikla samotná norma pod názvem *„Common Methodology for Information Technology Security Evaluation“*, označována zkratkou *CEM*.

Kromě výše uvedených tří zájmových skupin, jsou CC užitečná i pro manažery zabývající se oblastí informačních technologií či informačních systémů, nebo jsou dále vhodná i pro pracovníky, kteří jsou zodpovědní za informační bezpečnost, či vypracování bezpečnostní politiky organizace. Samozřejmě jsou vhodným prostředkem i pro auditory bezpečnosti IT a akreditační úředníky.

4. Srovnání a použití bezpečnostních standardů

4.1 Standardy a kriteria hodnocení informační bezpečnosti

Tato kapitola se bude věnovat problematice pouze mezinárodních kriterií hodnocení záruky bezpečnosti. Nikoliv tedy standardům a normám, které spadají pod autorský zákon a jejich šíření či veřejné publikování je trestné. Tyto mezinárodní kriteria, speciálně v případu Common Criterií se ale staly cennou předlohou pro mnohé normy.

4.1.1 Porovnání kriterií hodnocení bezpečnosti

Jednotlivá kriteria nevznikala nahodile, ale většinou jen měli přizpůsobit, respektive rozšířit danou problematiku pro účely použití v konkrétních geografických podmínkách. Jako první vznikla kriteria TCSEC na území USA. Stala se také cennou předlohou pro další navazující standardy a normy. Tato kriteria byla přijata už roku 1983, a je jasné, že vzhledem k tomuto datu už tato kriteria nemohou plně odpovídat potřebám současné doby v hodnocení bezpečnosti informační techniky, a dnes se tedy již prakticky nevyužívají. Na tento standard hodnocení navazuje dále evropská iniciativa v podobě kriterií ITSEC. Tento standard vznikl v roce 1991 v rámci iniciativy Evropského společenství, a definuje podobně jako předchozí standard sedm základních tříd bezpečnosti. Tento standard se v současné době ještě částečně využívá v rámci území Evropské unie, ale jeho význam pomalu, ale jistě upadá. Postupně je použití těchto kriterií nahrazováno novějším standardem, kriterii CC. Samotná Common Criteria byla vyvinuta opět v rámci území USA, a jejich první verze vznikla až v roce 1996. V rámci mezinárodní dohody ale zcela, nebo minimálně částečně, nahradily všechny dosavadní kriteria hodnocení bezpečnosti. Včetně kriterií TCSEC, která byla prvními průkopníky v této problematice, tak i pozdější Federal Criteria, i již zmíněná ITSEC kriteria a samozřejmě i CTCPEC. Zůstal tak tedy téměř jediný dokument popisující tuto problematiku, který jí zároveň ale sjednotil.

TCSEC	ITSEC	FC	CTCPEC	CC
D: minimální ochrana	E0			
				EAL1
C1: ochrana výběrovým přístupem	E1 F-C1			EAL2
C2: ochrana řízeným přístupem	E2 F-C2	T1	T-1	EAL3
B1: ochrana návěštím	E3 F-B1	T2	T-2	EAL4
		T3	T-3	
		T4		
B2: strukturovaná ochrana	E4 F-B2	T5	T-4	EAL5
B3: bezpečnostní domény	E5 F-B3	T6	T-5	EAL6
A1: verifikovaný návrh	E6 F-B3	T7	T-6	EAL7

Obr. 9 – Hrubé porovnání tříd standardů TCSEC, ITSEC, FC, CTCPEC a CC

Jednotlivá mezinárodní kriteria se ale značně odlišovala nejen historickým vývojem a použitím, ale také definovánými třídami. Většina kriterií obsahovala shodně sedm tříd bezpečnosti, ale ty nedefinovali vždy tu samou úroveň bezpečnosti.

4.1.2 Použití kriterií hodnocení bezpečnosti

Již představený dokument obsahující Common Criteria, se stal předlohou pro normu ISO/IEC 15408. Norma ISO/IEC 15408-1:1999, je dokonce totožná s textem zveřejněným organizacemi sponzorující projekt CC kriterií, pod názvem „*Common Criteria for Information Technlogy Security Evaluation*“, verze 2.1. Mezinárodní norma ISO/IEC 15408:1999 má status české technické normy, nesoucí pro tyto účely označení ČSN ISO/IEC 15408. Český překlad prvního dílu normy byl poprvé vydán v červnu roku 2001 českým normalizačním institutem. Překlady dalších dvou dílů byly vydány v listopadu roku 2002, přičemž jednotlivé díly normy jsou značeny jako 15408-1, 15408-2 a 15408-3.

Nejvíce se využívá již zmíněná EAL úroveň, které se člení do sedmi tříd v rámci dokumentu CC. Od nejnižší úrovně EAL1 do nejvyšší úrovně EAL 7. V praxi ale certifikované laboratoře používají tuto stupnici pouze do rozsahu EAL4. Případně do rozsahu úrovně EAL4+ značící už opravdu nejvyšší možnou úroveň záruky bezpečnosti, které může

konkrétní produkt dosáhnout. Žádný produkt tedy nemůže v současné době obdržet vyšší ohodnocení záruky zabezpečení než EAL4+.

4.2 Použití bezpečnostních standardů - dotazníkové šetření

V rámci splnění stanovených cílů pro účely průzkumu stavu informační bezpečnosti, byla zvolena forma dotazníkového šetření. K tomuto šetření byl využit dotazník obsažený v příloze č. 1 této diplomové práce. Cílem tohoto dotazníku bylo uskutečnit průzkum stavu informační bezpečnosti, s důrazem na dokument bezpečnostní politiky a mezinárodních norem v oblasti bezpečnosti informačních technologií.

4.2.1 Sestavení dotazníku

Samotný dotazník byl pro účely emailového šetření sestaven v programu MS Word 2007 ve dvou verzích. První verze obsahovala makra, určená pro usnadnění vyplňování dotazníků pomocí zaškrtávacích tlačítek (checkboxů). Jelikož jsou ale makra potenciálně zneužitelná a řada organizací je má dokonce přímo zakázána, byla vypracována i verze druhá. Tato druhá verze plně odpovídala z hlediska obsahu verzi první, pouze zde nebyli využité makro nástroje. Tato skutečnost, včetně vysvětlení důvodu existence dvou verzí, byla samozřejmě uvedena v příloze daného dotazníku, aby nedošlo ke zbytečnému zmatení respondentů, či obavám o možné ohrožení bezpečnosti.

Samotný dotazník obsahoval 15 otázek, z nichž bylo 13 otázek uzavřených, jedna otázka částečně uzavřená a jedna otevřená. Částečně uzavřená otázka byla použita pro možnost definování možnosti využívání jiných než autorem vybraných standardů, a poslední nepovinná a otevřená otázka se týkala názvu organizace. Jelikož se ale jedná o poměrně citlivé data, která jsou velmi často v rámci organizace i utajována, byla očekávána poměrně nízká návratnost dotazníků. V rámci tohoto očekávání a pro zvýšení počtu odpovědí byla v dotazníku zaručena i anonymita, pokud respondent výslovně zveřejnění názvu organizace nepovolil.

4.2.2 Cílová skupina respondentů

Primární cílovou skupinou dotazníkového šetření byli zaměstnanci IT nebo IS oddělení, případně i zaměstnanci útvaru bezpečnosti či jakéhokoliv dalšího útvaru, kteří mají ve své správě oblast informační bezpečnosti. Druhou cílovou skupinou byli řadoví zaměstnanci, kterým byly kladeny především otázky týkající se dokumentu bezpečnostní politiky a obecné informační bezpečnosti v jejich organizaci.

4.2.3 Sběr dat

Pro oslovení respondentů v rámci dotazníkového průzkumu byla využita emailová forma a zveřejnění dotazníku na internetových stránkách www.vyplnto.cz. Tyto dvě formy oslovení respondentů byly zvoleny zejména z důvodu poměrně snadného zpracování, a možnosti oslovit velký počet respondentů najednou.

Pomocí emailové korespondence bylo osloveno 50 různých organizací či institucí, napříč celou Českou republikou. Mezi oslovené organizace se řadili jak společnosti ze soukromého tak i státního sektoru. Jednalo se například o firmy působící v oblasti vývoji softwaru, poskytování síťových služeb, prodeji prvků informační či komunikační techniky, ale i bankovní instituty, akademické či státní instituce a společnosti zabývající se informačním zabezpečením či vývojem informačních systémů. Tato forma dotazování měla tedy za cíl oslovit především pracovníky odpovědné právě za informační bezpečnost ve vybraných organizací. Pro pracovníky organizace může být snazší vyplnit dotazník především z technických a časových důvodů. Naopak rizikem dotazníkového šetření emailovou formou je předpoklad ochoty respondenta. Po uběhnutí desetidenní lhůty, která byla stanovena pro ukončení šetření, bylo navráceno 14 dotazníků. Návratnost dotazníků byla tedy 28%.

Druhou formu dotazování pomocí internetových stránek www.vyplnto.cz využilo a vyplnilo 39 respondentů, z nichž byl jeden dotazník shledán jako špatně vyplněný. Celkem bylo tedy vyhodnoceno 52 řádně vyplněných dotazníků. Absolutní většina respondentů ale nedovolila zveřejnění názvu jejich organizace, což bylo nejspíše zapříčiněno citlivou povahou shromaždovaných dat.

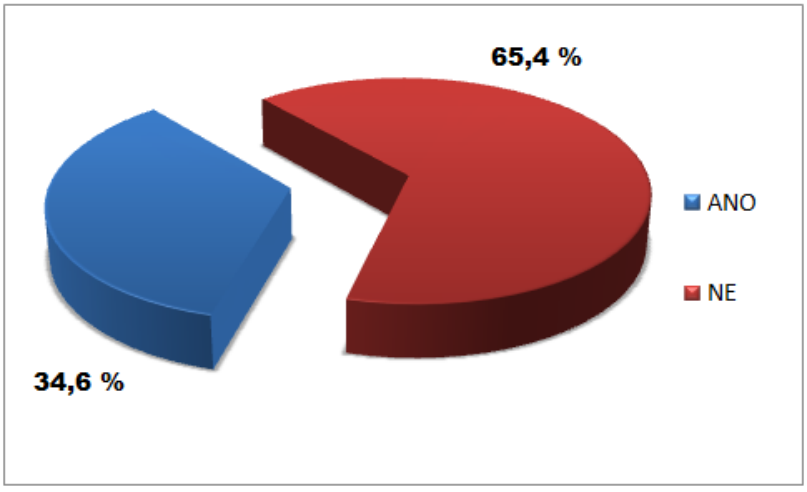
Pouze tři následující organizace povolily zveřejnění svého jména jako zdroje dotazníkového šetření:

- *AIRA GROUP, s.r.o.*
- *ENERGOPROJEKT PRAHA, a.s.*
- *KOMERČNÍ BANKA, a.s*

V rámci dotazníkového šetření a samotného dotazníků bylo využito segmentačních otázek pro oddělení dvou cílových skupin. První a primární cílovou skupinou tohoto dotazníku představují pracovníci, kteří jsou zaměstnáni v rámci informačních technologií či systémů. Druhá skupina následně prezentuje všechny zaměstnance, bez ohledu na jejich povolání či oddělení ve kterém vykonávají svojí práci. Kategorizace zde bylo využito zejména z důvodu zachování objektivity, kdy nepředpokládáme, že pracovníci kteří nepracují v oddělení IT/IS budou mít povědomí o používaných standardech v rámci informační bezpečnosti. Druhá skupina je využita zase především pro průzkum týkající se dokumentu bezpečnostní politiky a obecného stavu informační bezpečnosti v rámci jejich organizace.

Otázka č. 1

Jste zaměstnán v rámci informačních technologií?



Graf 1: Rozdělení respondentů podle profese pro potřeby průzkumu

Pro potřeby dotazníkového šetření jsme tedy rozdělili respondenty na dvě skupiny. Nejdříve se zde budeme věnovat skupině, která obsahuje pouze pracovníky zaměstnané v rámci

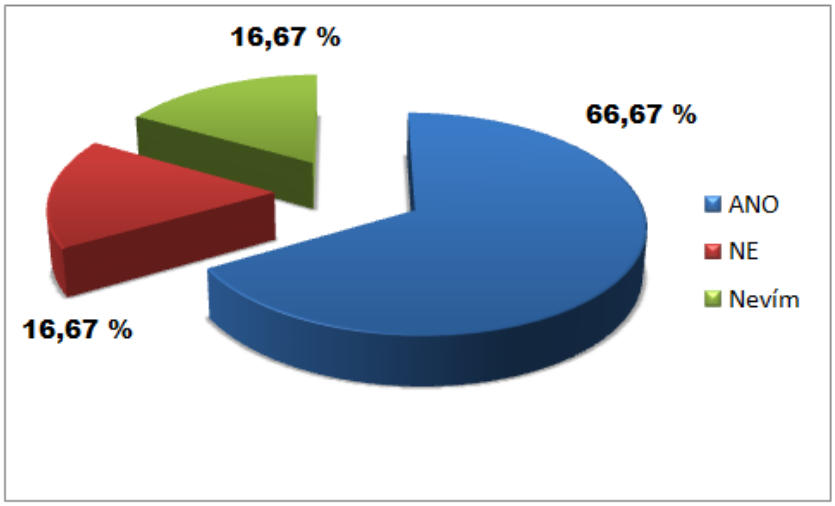
oddělení informačních technologií či informačních systémů, což je primární skupina našeho dotazníkového šetření.

4.2.4 Kategorie 1 – zaměstnanci oddělení IT/IS

První kategorie respondentů v rámci dotazníkového šetření zahrnuje pouze zaměstnance útvarů IT či IS. Cílem této skupiny je lépe vystihnout skutečný stav informační bezpečnosti, dále i využívání standardů či norem, ale také posoudit znalosti těchto pracovníků týkajících se mezinárodních kriterií hodnocení bezpečnosti informačních systémů. V rámci této kategorie bylo získáno 18 řádně vyplněných a relevantních dotazníků z různých organizací.

Otázka č. 2

Existuje ve vaší organizaci, ve které jste zaměstnán/á, dokument bezpečnostní politiky?

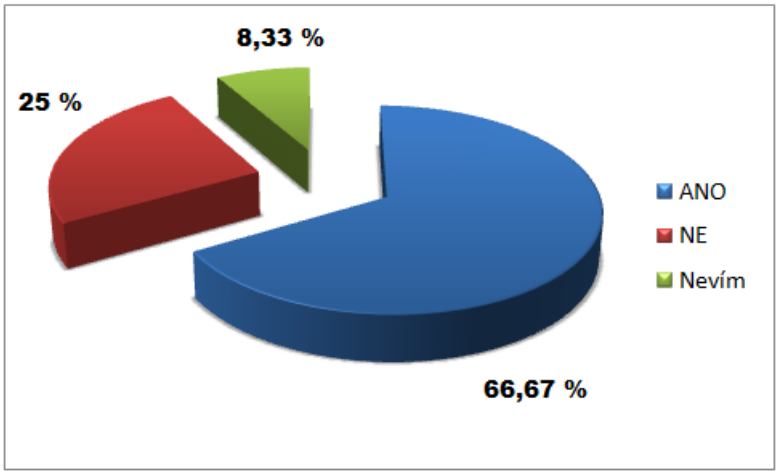


Graf 2 : Existence dokumentu bezpečnostní politiky (kategorie 1)

Jak je vidět, ve většině organizací dokument bezpečnostní politiky existuje. Pouze 16,67 % respondentů vyplnilo skutečnost, že v rámci jejich organizace dokument bezpečnostní politiky vůbec neexistuje, a stejná část označilo odpověď „nevím“. Vzhledem ke kategorii 1, která obsahuje pouze pracovníky IT oddělení a ke které je tento graf vztažený, je ale poměrně zarážející že 16,67 % pracovníků vůbec neví, zda dokument existuje.

Otázka č. 3

Jsou s tímto dokumentem bezpečnostní politiky seznamování všichni noví zaměstnanci?

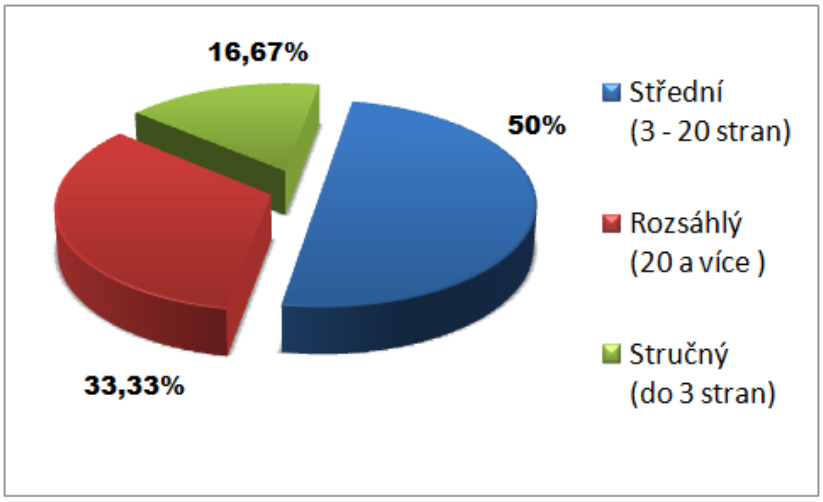


Graf 3: Seznamování nových zaměstnanců s dokumentem bezpečnostní politiky (kategorie 1)

V tomto případě bylo využito větvení dotazníku, a na tuto otázku odpovídali pouze respondenti, kteří v předchozí otázce potvrdili existenci dokumentu bezpečnostní politiky v rámci organizace. Výsledek šetření ukazuje fakt, že se většina organizací snaží v případě existence bezpečnostní politiky o její aktivní využívání všemi zaměstnanci. Přesná čtvrtina organizací ale tuto aktivitu neprojevuje, a dokument bezpečnostní politiky zde tak ztrácí smysl.

Otázka č. 4

Jaký je charakter rozsahu dokumentu bezpečnostní politiky u vaší organizace?

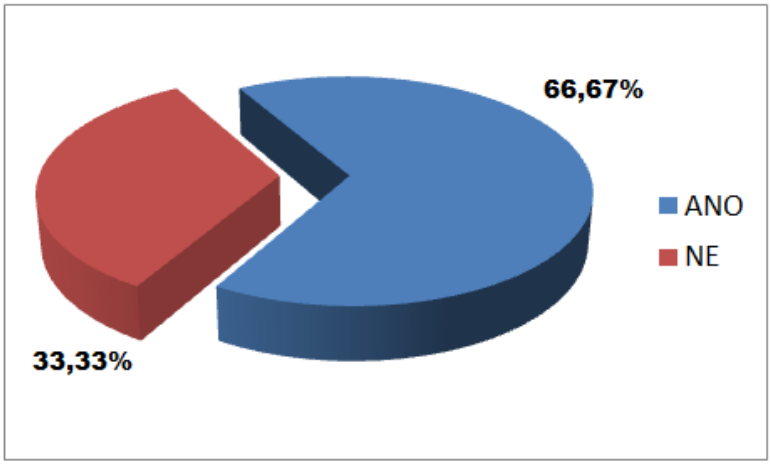


Graf 4: Rozsah dokumentu bezpečnostní politiky organizace (kategorie 1)

Opět v tomto případě bylo využito větvení dotazníků a na tuto otázku odpovídali pouze respondenti, kteří potvrdili existenci bezpečnostní politiky v organizaci. Přesnou polovinou dotázaných je hodnocen rozsah dokumentu jako střední, což je v rozumné míře 3–20ti stran. Tento rozsah umožňuje efektivní fungování bezpečnostní politiky. Rozsah dokumentu do třech stran je nedostačující, což vyplnilo 16,67% respondentů. Naopak za rozsáhlý ho označilo 33,33%.

Otázka č. 5

Znáte některé mezinárodní normy či standardy týkající se bezpečnosti informačních systémů?

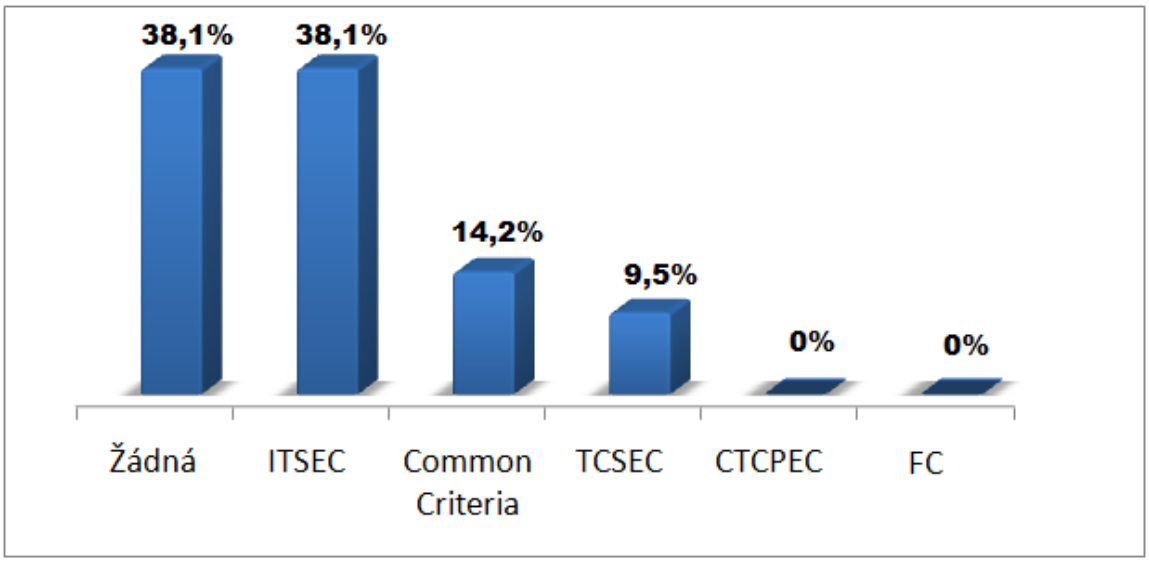


Graf 5: Znalost libovolné mezinárodní normy týkající se bezpečnosti informačních systémů (kategorie 1)

Jak je vidět, dvě třetiny pracovníků v rámci IT mají znalost některé mezinárodní normy bezpečnosti informačních systémů. Jedna třetina pracovníků sice zvolila možnost neznalosti žádné takovéto normy, ale minimálně část je bude pravděpodobně využívat v rámci větších a obecnějších souborů norem, které se netýkají pouze oblasti zabezpečení informační technologie.

Otázka č. 6

Znáte některá uvedená mezinárodní kriteria hodnocení bezpečnosti informačních systémů?

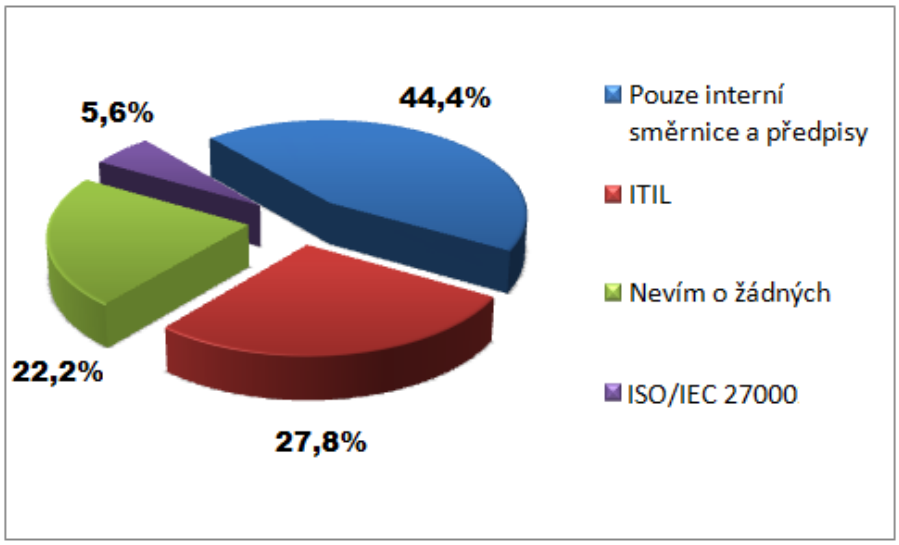


Graf 6: Znalost mezinárodně uznávaných kriterií hodnocení bezpečnosti informačních systémů (kategorie 1)

Jelikož se jedná o poměrně specifickou problematiku, byl očekáván poměrně vysoký podíl neznalosti žádných kriterií, navzdory i cílové skupině IT profesionálů. Toto očekávání se také při šetření potvrdilo. Více než třetina respondentů pracujících v rámci oddělení informačních technologií nezná podle provedeného šetření žádná kriteria. Dále pak stejný podíl respondentů uvedl znalost standardu ITSEC, což je v porovnání s novějšími Common Criterii zarážející, jelikož kriteria ITSEC jsou předchůdcem CC standardu. Tento rozdíl by mohl být způsoben historickým vývojem, kdy standard ITSEC byl první, který byl platný a sestavený právě pro území Evropské Unie, do jejíhož rámce spadá i Česká republika a námi provedený průzkum. Proto mohl tento standard zůstat nejvíce v obecném povědomí v rámci našeho státu. Další kriteria TCSEC, která jsou považována za základ celé problematiky, získala pouze 9,5%, což představuje malý podíl, ale jsou to kriteria, která vznikla na území USA a na evropském kontinentě jsou tak pravděpodobně méně známá. Podobným argumentem lze zdůvodnit i nulové podíly kriterií CTCPEC (Kanada) a FC (USA), které byli využívány většinou pouze v rámci území svého vzniku, a to pouze do doby vzniku CC kriterií.

Otázka č. 7

Využívá vaše organizace některé mezinárodní standardy v rámci informační bezpečnosti?



Graf 7: Znalost mezinárodně uznávaných kriterií hodnocení bezpečnosti informačních systémů (kategorie 1)

V rámci šetření byla položená částečně uzavřená otázka, týkající se používaných mezinárodních standardů či norem v rámci řízení informační bezpečnosti. Respondenti si zde mohli vybrat z předem připravených možností, či doplnit jakékoliv jiné využívané normy. V rámci skupiny IT profesionálů však nikdo možnosti vybrání jiných než předpřipravených norem nevyužil.

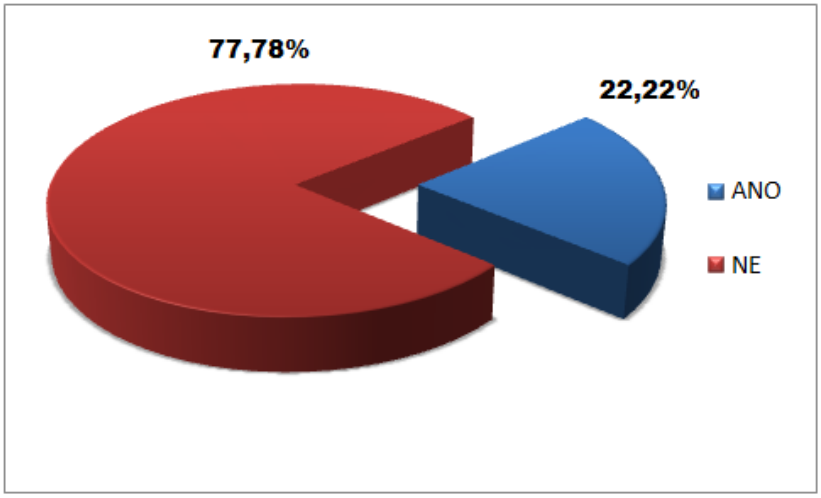
Největší podíl tedy získaly interní směrnice a předpisy, které ve většině případů vycházejí alespoň částečně z některé mezinárodní normy, ale ne vždy je tato skutečnost v povědomí uživatelů či zaměstnanců. Zejména z tohoto důvodu byla tato možnost odpovědi zahrnuta v dotazníkovém šetření. Na kolik dané interní předpisy a normy vycházejí z mezinárodních standardů, můžeme ale pouze hrubě odhadovat. Druhý největší podíl odpovědí získala možnost ITIL, což je zkratka pro "*Information Technology Infrastructure Library*". Zjednodušeně se jedná o veřejně dostupný rámec, popisující nejlepší využívané metody ve správě IT služeb. Poskytuje postupy a metody pro zvládnutí IT v organizaci a komplexně pojednává o službách se zaměřením na neustálé zlepšování kvality dodávaných služeb IT. V našem průzkumu získala tato komplexní metodika 27,8%.
Další uváděnou odpovědí byla neznalost žádných využívaných mezinárodních norem v rámci organizace. Jelikož tato možnost získala 22,2%, docházíme k poznatku, že zdaleka ne všichni

pracovníci IT oddělení jsou seznámeni s využívanými normami v rámci informační bezpečnosti. Dále pak poměrně malý počet odpovědí, směroval k normě ISO/IEC 27000. Tento soubor norem, zabývající se informační bezpečností získal pouze 5,6%.

Shrneme-li získané poznatky, docházíme k závěru, že využívanou mezinárodní normou v rámci organizací působící v ČR je především soubor ITIL a v omezeném rozsahu také ISO/IEC 27000. Téměř polovina oslovených zaměstnanců v rámci IT ale využívá především interní normy a předpisy, které ale budou pravděpodobně vycházet z některého mezinárodního standardu, minimálně v částečném rozsahu. Dalším očekávaným rámcem souboru metodik byl COBIT, které se ale nedočkal žádné odpovědi. K jeho využívání v rámci České republiky ale určitě také dochází. Podobná situace bude pravděpodobně ještě ale i u dalších neuvedených norem.

Otázka č. 8

Víte, čeho se týká norma ISO/IEC 15408?



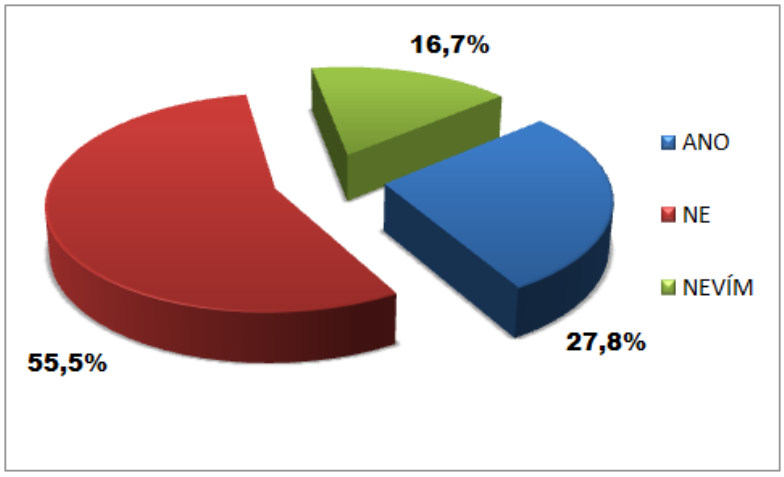
Graf 8: Znalost normy ISO/IEC 15408 (kategorie 1)

Norma ISO/IEC 15408 je totožná se zveřejněným textem v rámci dokumentu „*Common Criteria*“. Někdy bývá znám také pod názvem „Společná kritéria pro hodnocení bezpečnosti informačních technologií.“ V rámci České republiky má tento dokument i status České národní normy pod označením ČSN ISO/IEC 15408. Jak vyplývá z totožnosti textu této normy s dokumentem CC kriterii, obsahuje tato norma především kriteria a třídy záruky bezpečnosti informačních systému či jejich prvků. Tyto záruky se dělí na úrovně EAL1 -7,

které jsou významné z hlediska síťové bezpečnosti. Používají se jak pro ohodnocení bezpečnosti téměř jakéhokoliv síťového hardwaru, tak i vybraného softwaru. Z tohoto důvodu byla otázka zařazena do průzkumu. Dotazníkové šetření zde ukazuje většinovou neznalost tohoto standardu, ačkoliv je v současné praxi hodnocení pomocí úrovně EAL poměrně využívané a žádané. 77,78% respondentů z IT oborů ale tento standard nezná, zatímco jeho znalost zde uvedlo pouze 22,22%. Očekávána byla podstatně větší znalost tohoto standardu, ale svojí roli mohl sehrát i fakt, že úrovně záruky zabezpečení jsou publikovány již v dokumentu Common Crititeria. Pracovníci z řad IT odborníků je tedy mohou znát z jiného zdroje, a nevědomě tento standard využívat.

Otázka č. 9

Má vaše organizace oblast bezpečnosti IS/IT posouzenou externím nezávislým subjektem?

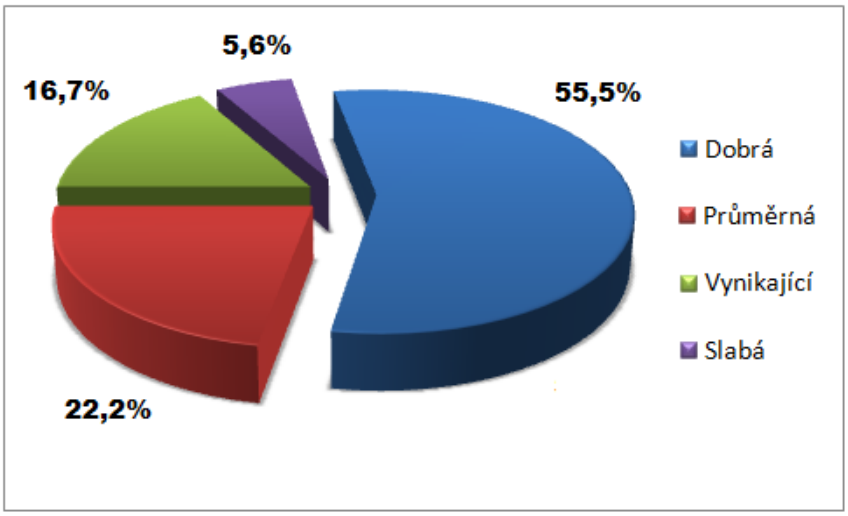


Graf 9: Posouzení IS/IT nezávislým subjektem (kategorie 1)

Každá organizace zabývající se otázkou informační bezpečnosti by měla mít tuto oblast posouzenou i externím a nezávislým subjektem. V rámci provedeného šetření ale pouze 55,5% respondentů uvedlo, že tímto způsobem posouzeno oblast IS/IT nemají. Kladně odpovědělo pouze 27,8%. Podobně jako v předchozích případech zde máme opět menší skupinu respondentů z řad zaměstnanců IT/IS, kteří na tuto otázku ani neznají odpověď. Konkrétně se zde jedná o 16,7% respondentů

Otázka č. 10

Jak hodnotíte bezpečnost vámi využívaného informačního systému?



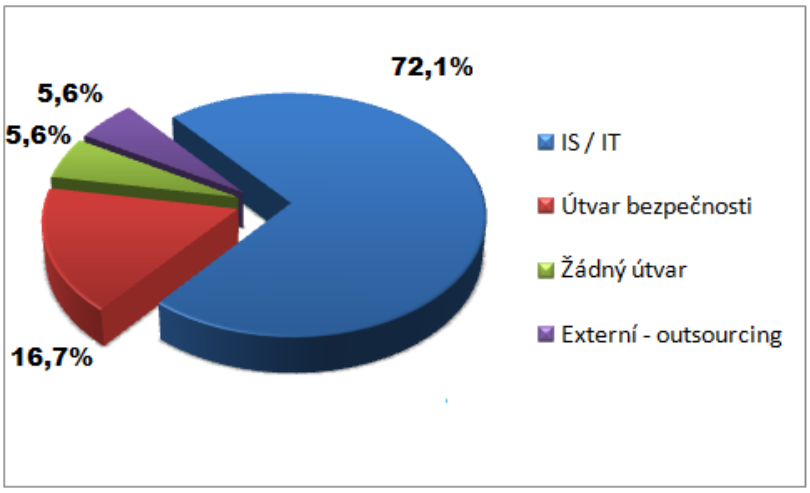
Graf 10: Posouzení úrovně bezpečnosti informačního systému v rámci organizace (kategorie 1)

Hodnocení úrovně zabezpečení využívaného informačního systému v rámci dotazníku, bylo prováděno pomocí uzavřené otázky, s pěti možnými odpověďmi. Jednalo se o odpovědi prezentující úroveň nedostačující, slabou, průměrnou, dobrou a vynikající.
Největší skupina respondentů se identifikovala s názorem dobré úrovně zabezpečení informačního systému v rámci jejich organizace. Konkrétně se jedná o 55,5%. Což pravděpodobně prezentuje skutečnost, že se respondenti nesetkávají příliš často s vážnými bezpečnostními incidenty, a jsou s mírou zabezpečení relativně spokojeni. Dále následovala skupina klasifikující zabezpečení informačního systému jako průměrné. Tento názor mělo 22,2% respondentů, kteří se tedy setkali už pravděpodobně s několika bezpečnostními incidenty, ale úroveň bezpečnosti informačního systému jim relativně nepřetržitě umožňuje vykonávat jejich práci, pouze s občasnými výpadky. Další skupina zahrnující 16,7% respondentů z řad zaměstnanců IT/IS oddělení, ohodnotila úroveň zabezpečení jako vynikající. Tito uživatelé jsou tedy spokojeni s úrovní bezpečnosti, a pravděpodobně nezaznamenaly vážnější bezpečností incidenty. Poslední skupina respondentů ohodnotila úroveň bezpečnosti informačního systému jako slabou. Tato skupina byla v rámci dotazníkového šetření zastoupená 5,6%. Tito uživatelé tedy pravděpodobně zaznamenali ohrožení a výpadky informačního systému, a jsou s jeho zabezpečením nespokojeni. V rámci dotazníkového šetření nedošlo k hodnocení zabezpečení nedostatečnou úrovni žádným

respondentem, a situace ohledně subjektivního názoru pracovníků IT/IS zodpovídající tento dotazník je tedy poměrně příznivá.

Otázka č. 11

Jaký útvar je ve vaší organizaci zodpovědný za informační bezpečnost?



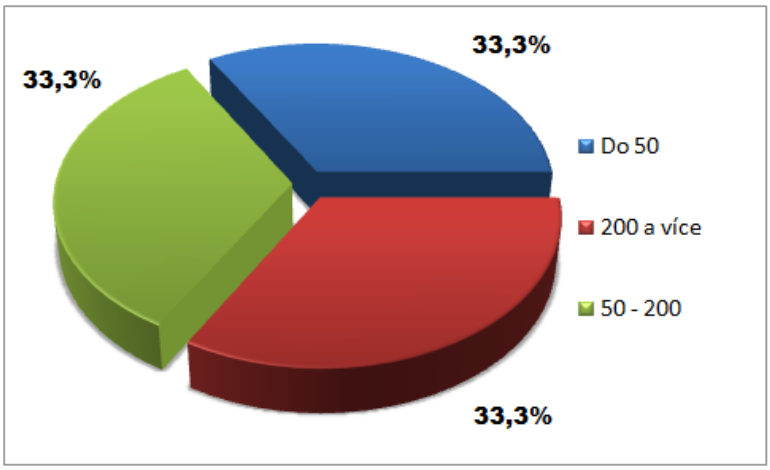
Graf 11: Útvar odpovědný za informační bezpečnost (kategorie 1)

Podle očekávání se potvrdil jako nejčastěji odpovědný útvar za informační bezpečnost útvar IS/IT. Takto odpovědělo 72,1% respondentů, tedy značná většina. Jako druhý v pořadí se umístil zvláště vyčleněný útvar pro informační bezpečnost v rámci dané organizace. Tímto způsobem už ale odpovědělo pouze 16,7%. Jako další možnost se jevila forma outsourcingu, kterou označilo pouze ale 5,6%. Stejné procentní ohodnocení bylo i v rámci možnosti žádného útvaru, kdy se respondenti doznali k faktu, že v rámci jejich organizace neexistuje podle jejich názoru útvar přímo odpovědný za informační bezpečnost. Další možnost v podobě ekonomického či finančního útvaru pro informační bezpečnosti nezvolil žádný respondent.

Další otázky, které následují v rámci první kategorie dotazníkového šetření, měli už pouze segmentační charakter, a slouží pouze pro přiblížení vzorku respondentů.

Otázka č. 12

Kolik má vaše organizace zaměstnanců?

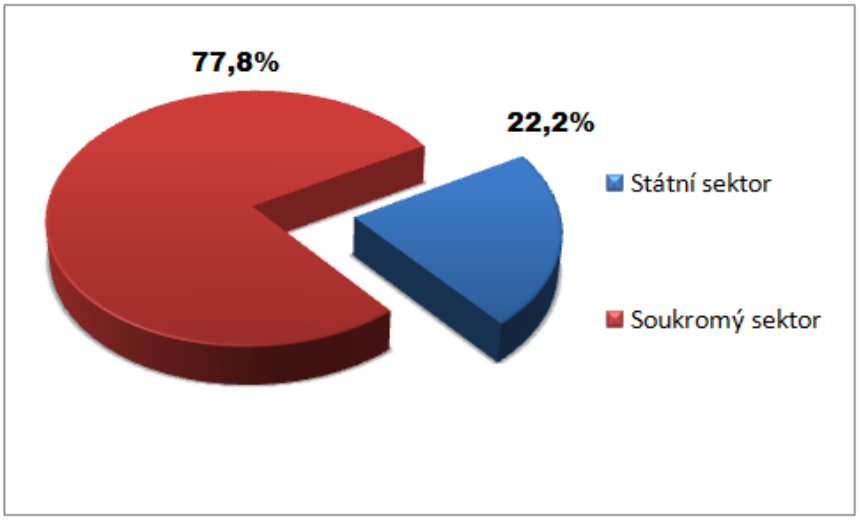


Graf 12: Rozložení organizací účastnící se průzkumu podle počtu zaměstnanců (kategorie 1)

Jak je vidět, povedlo se získat přesně vyrovnaný vzorek respondentů pro potřeby dotazníkového šetření. V rámci první kategorie, kde jsou zastoupeni pouze zaměstnanci v rámci IT/IS oddělení je tedy poměr organizací podle naší specifikace přesně vyvážen.

Otázka č. 13

V jaké sféře organizace působí?

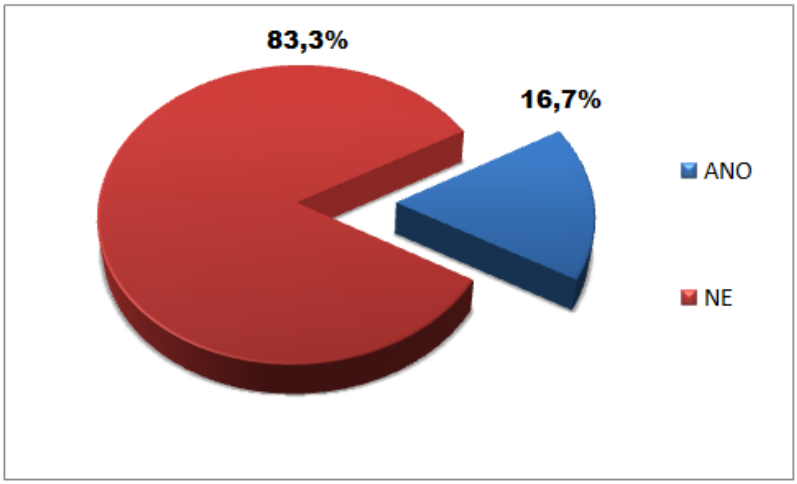


Graf 13: Rozložení organizací účastnící se průzkumu podle sféry vlastnictví (kategorie 1)

V rámci rozložení organizací podle sféry vlastnictví dané organizace je v rámci dotazníkového šetření značně nevyvážené. Většina organizací respondentů pochází ze soukromého sektoru, konkrétně 77,8 %. Státní sektor byl zastoupen pouze v 22,2%.

Otázka č. 14

Je možné zveřejnit název vaší organizace jako jeden ze zdrojů průzkumu?



Graf 14: Stanovisko týkající se zachování anonymity organizace (kategorie 1)

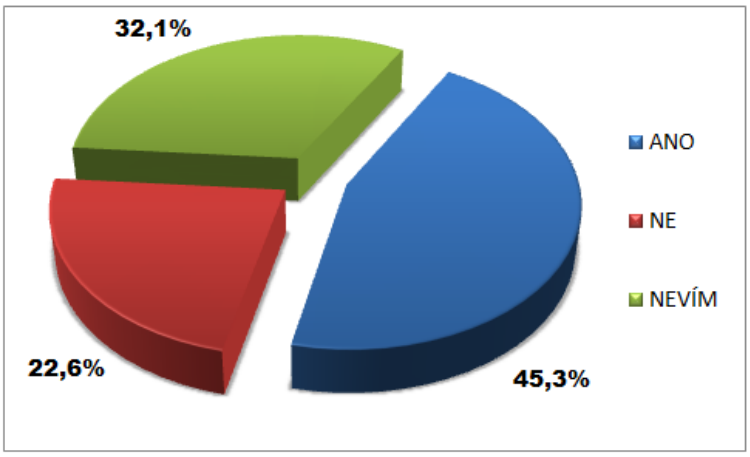
Organizace účastnící se dotazníkového šetření v rámci kategorie zaměstnanců IT/IS oddělení poměrně výraznou většinou nepovolili zveřejnění jména společnosti. Jelikož se jedná o poměrně choulostivé a mnohdy dokonce utajované informace v rámci konkurenčního boje, dá se stanovisko chápat.

4.2.5 Kategorie 2 – všichni respondenti

Druhá kategorie v rámci dotazníkového šetření zahrnuje již všechny respondenty, nejen zaměstnance útvarů IT či IS. Cílem této skupiny je lépe vystihnout stav dokumentu bezpečnostní politiky v širším vzorku respondentů, a také zhodnotit jejich znalosti týkající se bezpečnosti informačních technologií. Některé kladené otázky z dotazníku v příloze číslo 1 zde budou vynechány z důvodu možného zkreslení odborných otázek, na které měli odpovídat pouze odborníci z řad zaměstnanců IT/IS (Toto šetření bylo provedeno v kategorii 1.).
V rámci této kategorie bylo získáno 53 řádně vyplněných a relevantních dotazníků.

Otázka č. 2

Existuje ve vaší organizaci, ve které jste zaměstnán/á, dokument bezpečnostní politiky IT?

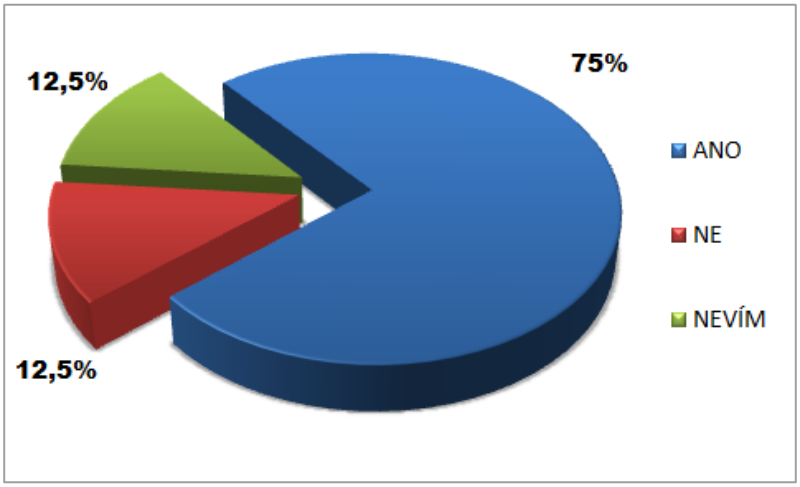


Graf 15: Existence dokumentu bezpečnostní politiky (kategorie 2)

V rámci kategorie zahrnující všechny zaměstnance, musíme konstatovat, že téměř polovina respondentů si je vědoma existence dokumentu bezpečnostní politiky. Konkrétně se jedná o 45,3% všech vyplněných dotazníků. Dalších 22,6% naopak vyplnilo opačnou možnost, tedy že žádný dokument bezpečnostní politiky v rámci organizace neexistuje. Značná část zde označilo odpověď prezentující jejich neznalost týkající se existence zmíněného dokumentu.

Otázka č. 3

Jsou s tímto dokumentem bezpečnostní politiky seznamování všichni noví zaměstnanci?

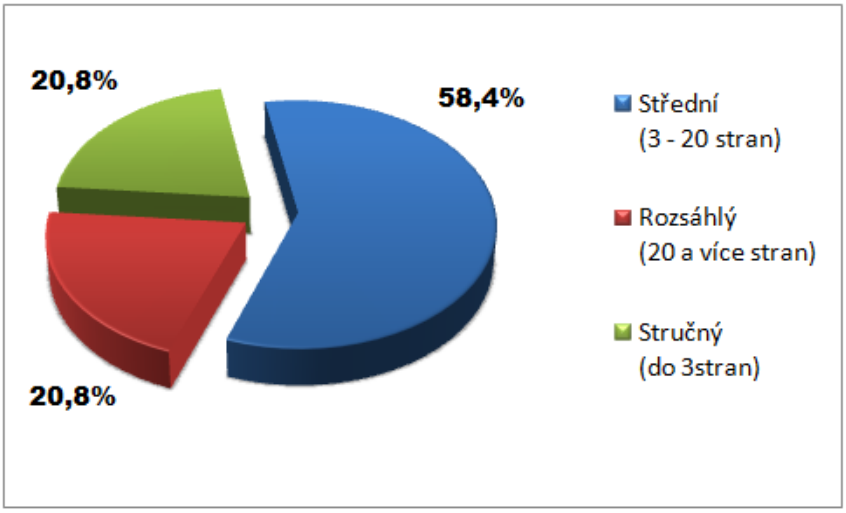


Graf 16: Seznamování nových zaměstnanců s dokumentem bezpečnostní politiky (kategorie 2)

V tomto případě celých 75% respondentů, kteří v předchozí otázce souhlasili s existencí dokumentu bezpečnostní politiky**,** vyplnilo odpověď, že všichni noví zaměstnanci jsou s tímto dokumentem i seznamováni**.** Zbylých 25% respondentů se rovnoměrně rozdělilo mezi zbývající dvě možnosti. Tedy že v 12,5% případů všichni zaměstnanci dané organizace nejsou seznamováni s dokumentem bezpečnostní politiky, a dalších 12,5% zaměstnanců tuto skutečnost nezná.

Otázka č. 4

Jaký je charakter rozsahu dokumentu bezpečnostní politiky u vaší organizace?

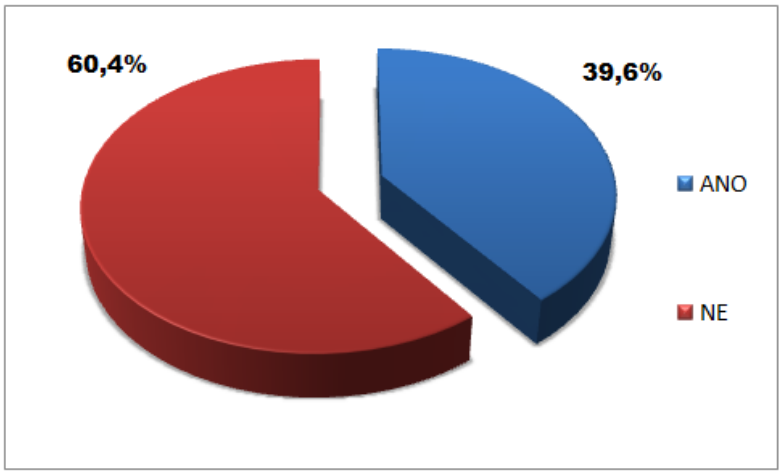


Graf 17: Rozsah dokumentu bezpečnostní politiky organizace (kategorie 2)

V rámci této otázky 58,4% všech respondentů označilo rozsah dokument bezpečností politiky v rámci jejich organizace za střední. Dalších 20,8 % pak za stručný, a stejná část respondentů i za rozsáhlý. Nadpoloviční většina organizací vlastnící dokument bezpečnostní politiky ho tedy udržuje v poměrně rozumném rozsahu.

Otázka č. 5

Znáte některé mezinárodní normy či standardy týkající se bezpečnosti informačních systémů?

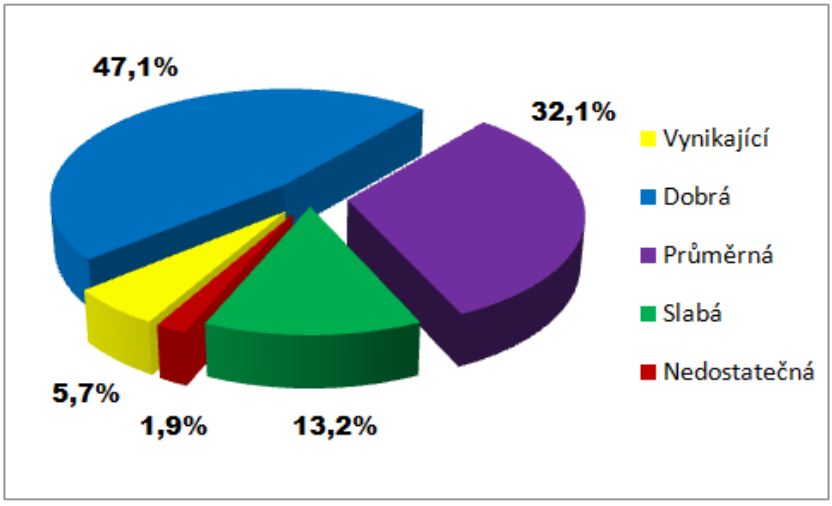


Graf 18: Znalost libovolné mezinárodní normy týkající se bezpečnosti informačních systémů (kategorie 2)

Tato otázka byla zařazena do vyhodnocení pouze pro orientační úsudek obecného podvědomí o bezpečnostních normách v rámci IT, jelikož je samozřejmě očekáváno, že znalost mezinárodních norem pro bezpečnost informačních systémů je výsadou převážně IT odborníku, kterým byla tato otázka také kladena v rámci kategorie 1.

Otázka č. 10

Jak hodnotíte bezpečnost vámi využívaného informačního systému?



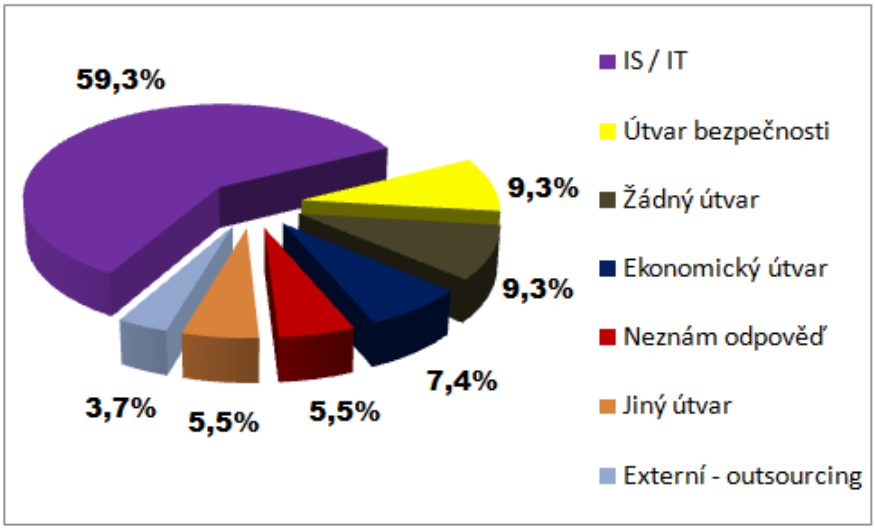
Graf 19: Posouzení úrovně bezpečnosti informačního systému v rámci organizace (kategorie 2)

V rámci druhé kategorie, kde byli zahrnuty všechny správně vyplněné dotazníky, jsme stejně jako v první kategorii zahrnuly vyhodnocení názoru na bezpečnost využívaného informačního systému. Toto hodnocení respondentů bylo prováděno v rámci uzavřené otázky, s pěti možnými odpověďmi. Jednalo se odpovědi označené jako úroveň nedostačující, slabá, průměrná, dobrá a vynikající.

Názor spočívající ve vynikající úrovni zabezpečení využívaného IS prezentovalo 5,7% respondentů. Jednalo se tedy o velmi malou část všech uživatelů. Dobrou úrovní ohodnotilo bezpečnost systému 47,1% účastněných uživatelů, tedy téměř polovina. Další úroveň, která byla označená v dotazníkovém šetření jako průměrná, použilo 32,1% uživatelů. Z těchto výše uvedených zjištěných poznatků, lze vypozorovat poměrně optimistické názory na hodnocení bezpečnosti využívaného informačního systému. Této orientaci odpovídá i předposlední skupina, prezentující názor ve slabé úrovni zabezpečení. Konkrétně tento názor vyslovilo 13,2% respondentů. Poslední skupina, kde se hodnotila bezpečnost jako nedostatečná má už velmi malé zastoupení v podobě 1,9%.

Otázka č. 11

Jaký útvar je ve vaší organizaci zodpovědný za informační bezpečnost?



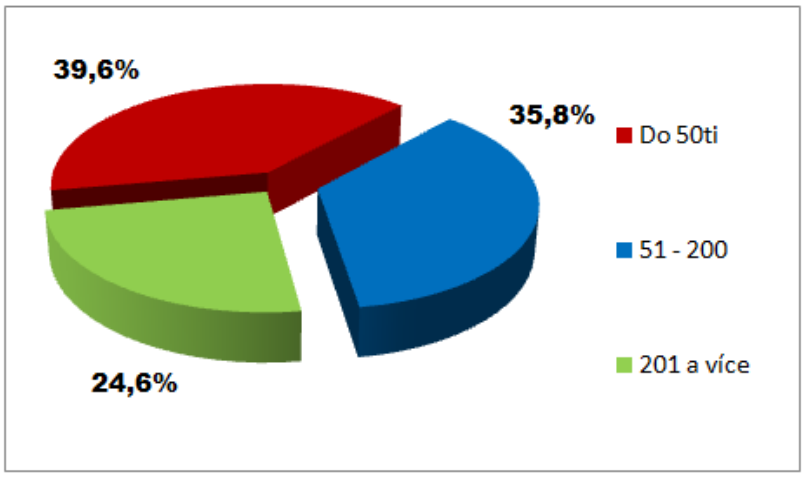
Graf 20: Útvar odpovědný za informační bezpečnost (kategorie 2)

Při zahrnutí celého vzorku respondentů jsme získali sedm vybraných odpovědí na výše zmíněnou otázku. Největší podíl respondentů, 59,3% odpověděl, že útvar odpovědný za informační bezpečnost je IT/IS. Dále následovala odpověď v podobě útvaru bezpečnosti,

který získal 9,3%. Stejný podíl získala i odpověď, která zahrnovala možnost neexistence útvaru, který je odpovědný za informační bezpečnost. Předpokládáme, že tuto možnost vybrali především malé organizace. Další odpovědí byl ekonomický útvar, s ohodnocením 7,4%. Možnosti jiného útvaru, který nebyl v rámci možností definován, stanovilo 5,5%, tedy stejný podíl jako u možnosti kdy respondent nezná odpověď. Poslední možností bylo zajištění informační bezpečnosti externí firmou, kterou zvolilo pouze 3,7% respondentů.

Otázka č. 12

Kolik má vaše organizace zaměstnanců?

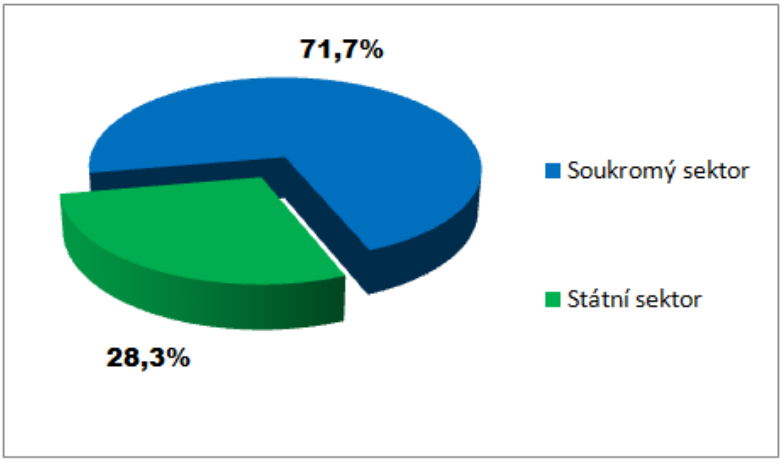


Graf 21: Rozložení organizací účastnící se průzkumu podle počtu zaměstnanců (kategorie 2)

V rámci dotazníkového šetření se ve druhé kategorii rovněž podařilo zajistit poměrné rovnoměrné zastoupení organizací z hlediska jejich velikosti. Menší organizace zde mají ale největší zastoupení v 39,6%. Střední organizace byly zastoupeny z 35,8% a nejmenší podíl v dotazníkovém šetření měli organizace většího rozsahu. Konkrétně měli tedy tyto organizace podíl 24,6%.

Otázka č. 13

V jaké sféře organizace působí?



Graf 22: Rozložení organizací účastnící se průzkumu podle sféry vlastnictví (kategorie 1)

Z hlediska sféry vlivu oslovených organizací došlo podobně jako u předchozí kategorie k většímu zastoupení soukromého sektoru. Ten byl zastoupen v 71,7%, zatímco státní sektor pouze v 28,3% případů

4.2.6 Shrnutí dotazníkového šetření

Při shrnutí poznatků vyplývajících z dotazníkového šetření týkající se dokumentu bezpečnostní politiky musíme konstatovat, že zhruba v 45% oslovených organizací tento dokument skutečně existuje, a zaměstnanci si ho jsou vědomi. Dále ale 32% oslovených respondentů nedokázala s určitostí říci, zda daný dokument v rámci organizace existuje či neexistuje. I kdyby zde ale existoval, nemůže zde plnit svůj účel, jelikož ho zaměstnanci neznají, respektive nejsou seznámeni s jeho obsahem. V přibližně 23% však tento dokument dokonce podle názorů respondentů vůbec s určitostí neexistuje. Tyto zjištěné skutečnosti tak ukazují, že zhruba v 55% dokument bezpečnostní politiky neexistuje, nebo minimálně neplní zcela svůj hlavní účel. Tento nedostatek by měl být velmi rychle odstraněn, jelikož bez dokumentu bezpečnostní politiky se celé řízení informační bezpečnosti stává velmi obtížnou a chaotickou záležitostí. Samotná existence tohoto dokumentu ale nestačí, je nutné ho také uvést do praxe a zajistit aby s ním byli seznámeni i všichni zaměstnanci dané organizace.

V rámci dotazníkového šetření byl také zkoumán fakt, zda jsou právě s tímto dokumentem seznamováni i všichni nově přijatí zaměstnanci. Zde už vyšlo šetření lépe, a prokázalo, že v 75% organizacích ve kterých dokument bezpečnostní politiky existuje, jsou s jeho obsahem seznamováni i všichni noví zaměstnanci. Ale stále je zde prostor pro možná zlepšení. Dále byla v rámci tohoto dokumentu šetřena jeho rozsáhlost. Jako rozumný rozsah se jeví dokument o 3-20 stranách, v závislosti na velikosti, typu a povaze podniku. V šetření 58,4% všech respondentů označilo právě tento rozsah z nabízených možností. Zde je tedy možné vydat pouze doporučení, aby rozsah dokumentu bezpečnostní politiky nepřesáhl dvacet stránek, ale aby ani neobsahoval méně než tři stránky. Vždy ale závisí na konkrétních podmínkách, ve kterých organizace působí.

Dalším bodem zájmu v rámci dotazníkového šetření byla znalost mezinárodních norem, respektive standardů týkajících se bezpečnosti informačních systémů. Tento bod byl šetřen pouze u respondentů, kteří jsou zaměstnání v rámci informačních technologií. První byla šetřena znalost mezinárodních kriterií pro hodnocení bezpečnosti informačních systému či jednotlivých prvků. Průzkum mezi zaměstnanci IT ukázal největší znalost kriterií ITSEC, ačkoliv tento standard je již poměrně zastaralý a existuje novější nástupce. Znalost těchto kriterií vykázalo 38,1% respondentů. Největší znalost právě tohoto standardu se dá vysvětlit geografickou polohou, jelikož se jedná o první standard, který byl vyvinut na území Evropského kontinentu, a byl tedy jako první využíván i na území České republiky. Druhým nejvíce známým standardem v rámci kriterií hodnocení informačních systémů skončila Common Criteria. Tato kriteria jsou uplatňována také v rámci Evropy, ale i v rámci jiných územních celků. Jedná se totiž o iniciativu, která nahradila všechna dosavadní kriteria, a sjednotila přístup. Proto je poměrně logické jejich umístění na druhém místě, se znalostí 14,2% respondentů. Dále následovala americká verze kriterií, která je základem pro danou problematiku a vznikla jako první už v roce 1983, označována jako TCSEC. Tato kriteria získala už pouze 9,5%. Dále byly zahrnuty v rámci komplexnosti problematiky i kriteria CTCPEC vzniklá v rámci Kanadského územního celku, a Federal Criteria která jsou opět záležitostí USA. Ale oboje kriteria byla pro naše respondenty z řad IT pracovníků neznámá. Jako vysvětlení se jeví opět geografická poloha, jelikož v našich podmínkách se zmíněné standardy nikdy víceméně nepoužívaly.

Dalším bodem dotazníkového šetření byly využívané mezinárodní standardy v rámci informační bezpečnosti. Oslovené organizace podle výsledného zjištění preferují především

interní směrnice a předpisy, které ale mohou do značné míry vycházet i z některého standardu. Druhý největší podíl odpovědí získala možnost ITIL, která představuje veřejně dostupný rámec, popisující nejlepší využívané metody ve správě IT služeb. Využívání tohoto rámce vykázalo 27,8% respondentů z řad zaměstnanců IT/IS. Poslední zbývající standard založený na souboru norem ISO/IEC 27000 označilo pouze 5,6%. Naopak poměrně velká část, konkrétně 22,2% zaměstnanců IT/IS oddělení různých organizací přiznalo skutečnost, že si nejsou vědomi žádného mezinárodního standardu, který by jejich organizace v rámci bezpečnost informačních technologií využívala. Nakolik jsou tedy využívané mezinárodní normy nelze přesně říci, z důvodu řízení se organizací především podle interních norem a předpisů. Další otázka v rámci dotazování se ptala na znalost už konkrétní normy ISO/IEC 15408. Tato otázka do jisté míry navazovala na mezinárodní kriteria hodnocení bezpečnosti informačních systémů, ze kterých tato norma bohatě čerpala. V rámci české republiky má tento dokument i status české národní normy pod označením ČSN ISO/IEC 15408. Znalost této normy vykázalo 22,22% respondentů, a naopak neznalost 77,78%. Tato skutečnost tedy jasně mluví v neprospěch oslovených organizací, respektive dotazovaných zaměstnanců.

Dále se v rámci dotazníků kladla otázka, zda má organizace posouzenou oblasti IT/IS nezávislým a externím subjektem. Posouzení informačního systému či oblasti informačních technologií nezávislým subjektem, přináší mnohé výhody nejen z hlediska bezpečnosti. Nezávislý odborník může odhalit slabé místa či nedostatky, kterých si interní zaměstnanci nemusí být vždy vědomi. Tito nezávislí oborníci mají navíc přehled v rámci IS/IT, a vědí na základě zkušeností, na které oblasti se mají soustředit, či jaké nedostatky hledat.
Z tohoto důvodů je obecně doporučováno mít oblast bezpečnosti IS/IT externě posouzenou a zhodnocenou. V rámci provedeného šetření ale 55,5% respondentů z různých organizací uvedlo, že tímto způsobem posouzeno oblast IS/IT nemají. Kladně odpovědělo pouze 27,8%. Jak je tedy vidět, i v této oblasti jsou mnohé nedostatky, a je zde velký prostor pro případné zlepšení.

4.3 Základní průzkum bezpečnosti sítě LAN

Pro potřeby této diplomové práce, a pro přiblížení problematiky síťové bezpečnosti, byl proveden základní bezpečnostní průzkum sítě LAN. Cílem tohoto průzkumu bylo posoudit stav lokální počítačové sítě, která se využívá v rámci menší organizace. Cílová organizace ale bohužel nedovolila zveřejnění svého jméno. Můžeme pouze říci, že zmíněná společnost se zabývá výrobou produktů ze dřeva a působí v rámci středočeského kraje. V rámci použití prostředků výpočetní techniky využívá čtyři osobní počítače. Jeden počítač je ve stolním provedení, zbylé jsou v provedení přenosném.

4.3.1 Technické parametry sítě

Společnost, u které byl proveden tento průzkum, využívá pro svoje potřeby tedy již zmíněné čtyři osobní počítače. Tyto počítače jsou zapojeny pro účely sdílení dat v místní LAN síti, jejímž centrálním prvkem je switch od společnosti D-Link. Přesněji se jedná o model nesoucí označení DES-1005D. Tento síťový přepínač obsahuje 5 portů pro připojení pěti možných počítačů či dalších prvků výpočetní techniky. Tento switch tedy zatím potřebám společnosti dostačuje. Konfigurace již zmíněných počítačů jsou následující:

1. Stolní počítač **AMD Athlon II X4 635**, obsahující procesor 2,9 GHz, RAM 4GB s operačním systémem Windows 7.(IP 192.168.1.1)

2. Přenosný počítač **AMD Sempron mobile**, obsahující procesor 2GHz, RAM 896MB s operačním systémem Windows XP. (IP 192.168.1.2)

3. Přenosný počítač **Apple MacBook Pro 13**, obsahující procesor 2,4GHz, RAM 4GB s operačním systémem Windows 7. (IP 192.168.1.12)

4. Přenosný počítač **ACER Aspire One A150**, obsahující procesor 1,6 GHz, RAM 1GB s operačním systémem Windows 7. (IP 192.168.1.13)

Z hlediska bezpečnosti informační techniky využívají všechny počítače antivirus NOD32 od společnosti ESET, samozřejmě pod legální licencí. Dále v rámci operačního systému zmíníme ještě využívání interního firewallu. Jak antivirový software, tak i jednotlivé operační systémy jsou udržovány v aktualizovaném stavu. Vzhledem ale k využití i operačního systému Windows XP, kterému již skončila oficiální podpora od společnosti Microsoft, je počítač využívající tento operační systému udržovaný v aktualizované podobě pouze relativně. Proto byla doporučena výměna operačního systému za novější, a případné navýšení RAM paměti pro tyto účely. Netřeba dodávat, že vzhledem ke zkoumané problematice síťové bezpečnosti představuje tento počítač i zvýšené riziko vzhledem k ostatním počítačům.

Společnost, na kterou byl zacílen tento průzkum, samozřejmě využívá i připojení k celosvětové síti Internet. Toto připojení je zde řešeno ale pouze pomocí mobilního připojení nabízeného společností O2, nikoliv tedy v rámci používané LAN sítě. Konkrétně jsou uzavřeny smlouvy na dvě mobilní připojení. Majitel dané společnosti uvedl, že mu toto připojení plně vyhovuje, jelikož poměrně často cestuje a pro potřeby emailové korespondence či obsluhy webové prezentace toto připojení plně dostačuje. V kontextu této otázky jsme ale zjistili i skutečnost, že některé prostředky výpočetní techniky jsou využívány i pro soukromé účely. Což je ale vzhledem k velmi malému rozsahu společnosti poměrně pochopitelné.

4.3.1 Použitý software –Tenable Nessus

Pro účely průzkumu bezpečnosti výše popsané LAN sítě byl zvolen nástroj v podobě síťového skeneru Nessus. Konkrétně byla vybrána verze, která nese označení *Nessus-4.4.1-i386.msi* v distribuci pro operační systém Windows. Tento software je pod licencí GPL, a je tedy volně využitelný bez poplatku. Síťový scanner Nessus představuje nástroj pro zjišťování nedostatků v oblasti sítově bezpečnosti, a je velmi často také využíván síťovými administrátory pro svoji účinnost v odhalování bezpečnostních děr. Zmíněný program obsahuje dvě aplikace. Aplikaci určenou pro správu a zajištění přehledu, a druhou aplikaci, ve které se provádějí samotné testy.

V rámci metodiky prováděných testů musíme zmínit skutečnost, že byl po konzultaci s majitelem využit počítač označený na začátku této kapitoly číslem 2, který byl poskytnut v rozsahu jednoho dne pro potřeby průzkumu síťové bezpečnosti. V rámci zachování

objektivity by bylo patrně lepší využít pro potřeby průzkumu nezávislý počítač, ale jelikož se jedná pouze o základní průzkum, byli testy prováděné právě pomocí nabídnutého počítače AMD Sempron. Postupně byly tedy otestovány všechny počítače v rámci cílové LAN sítě.

4.3.2 Skenování sítě a vyhodnocení

Po nastavení jednotlivých konfigurací a parametrů skenování, byly spuštěny již samotné testy v rámci síťového skeneru. Po doběhnutí všech modulů, které testovali různé aspekty bezpečnosti, byl uživatelovi programem poskytnut základní výstup v následující podobě.

Host	Total	High	Medium	Low	Open Port
192.168.1.1	54	0	0	36	18
192.168.1.2	61	1	3	43	14
192.168.1.12	34	0	0	24	10
192.168.1.13	27	0	2	19	6

Obr. 10 – *Přehled testovaných počítačů a nalezených bezpečnostních nedostatků.*

Jak je tedy vidět, síťový skener v našem průzkumu odhalil některé nedostatky v rámci síťové bezpečnosti. U prvního počítače, označeného zde pomocí IP adresy 192.168.1.1 software nezjistil žádný závažné nedostatky ohodnocené prioritou High nebo Medium. U tohoto počítače bylo zachyceno pouze 36 menších nedostatků, ohodnocené nejnižší možnou prioritou. Nejedná se závažnější porušení bezpečnosti a z tohoto důvodu se jim zde nebudeme detailněji věnovat. Dále skener nalezl celkem 18 otevřených portů, což je poměrně velké číslo. Majiteli tedy byla doporučena revize portů, které jsou připraveni k naslouchání v rámci datové komunikace, a porovnání těchto s portů se spektrem využívaných služeb.

Dále byl v rámci průzkumu síťové bezpečnosti skenován počítač označený IP adresou 192.168.1.2. U tohoto přenosného počítače bylo nalezeno nejvíce bezpečnostních nedostatků z celého testování. Jedna hrozba zde dokonce byla ohodnocena nejvyšší možnou prioritou.

komplet › 192.168.1.2 › 445 / tcp List Detail 1 results

Plugin ID	Name	Port	Severity
42411	Microsoft Windows SMB Shares Unprivileged Access	cifs (445/tcp)	High

Obr. 11 – *Zjištěný kritický nedostatek u počítače 192.168.1.2*

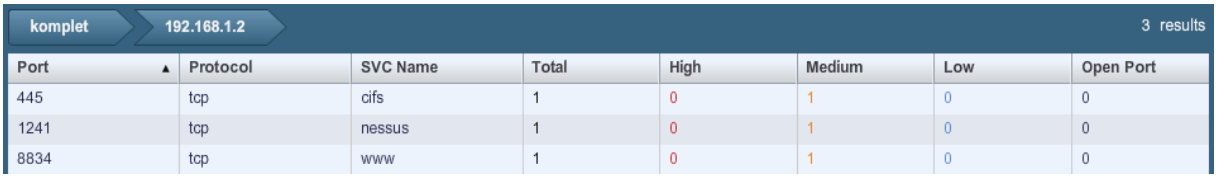
Při bližším zjišťování informací jsme zjistili poznatek, že daný nedostatek byl detekován v rámci služby SMB a nastavených pravidel týkajících se sdílení dokumentů. Při

vyhledávání informací k této službě v rámci veřejně dostupných zdrojů jsme zjistili, že účelem této funkce je zabezpečení a správa sdílených dat v rámci operačního systému Windows. Pokusili jsme se zjistit také další informace v rámci využitého softwaru, a došli jsme k následujícímu grafickému výstupu.

Obr. 12 – *Bližší informace z programu Nessus, týkající se zjištěného nedostatku s High významností u počítače s ip adresou 192.168.1.2*

Při detailním studiu daného nedostatku zjišťujeme, že tento počítač má nastavené sdílení jedné nebo více složek, které muže být případně zneužito. Útočník se může potenciálně pokusit číst či změnit sdílená data, na základě získaného oprávnění. Pomocí výstupu programu nessus jsme zjistili, o jaké konkrétní složky počítače se jedná. Výstraha se týkala jednoho adresáře, pojmenovaného jako „Sít“. Po konzultaci s majitelem organizace jsme došli k závěru, že je daná skutečnost v pořádku. Tato složka je určená pro sdílení dat v rámci lokální sítě mezi jednotlivými počítači. Upravili jsme tedy pouze práva pro čtení a zápis, a vyhodnotili situaci za uspokojující ve vztahu k tomuto varování. Byla ale vyslovena připomínka směrem k majiteli společnosti, týkající se skutečnosti, že daleko vhodnější by bylo přesunout tuto složku na stolní počítač, který není mobilní a nepřipojuje se do jiných sítí. Majitel sice oponoval tvrzením, že se tento notebook využívá většinou pouze v rámci firmy, ale nakonec připomínku uznal a dokumenty přesunul na stolní počítač.

Dále bylo v rámci tohoto počítače zjištěno skenerem nessus malé množství nedostatků, které byli ohodnoceny stupněm Medium. Jedná se o následující tři služby běžící v rámci protokolu TCP :

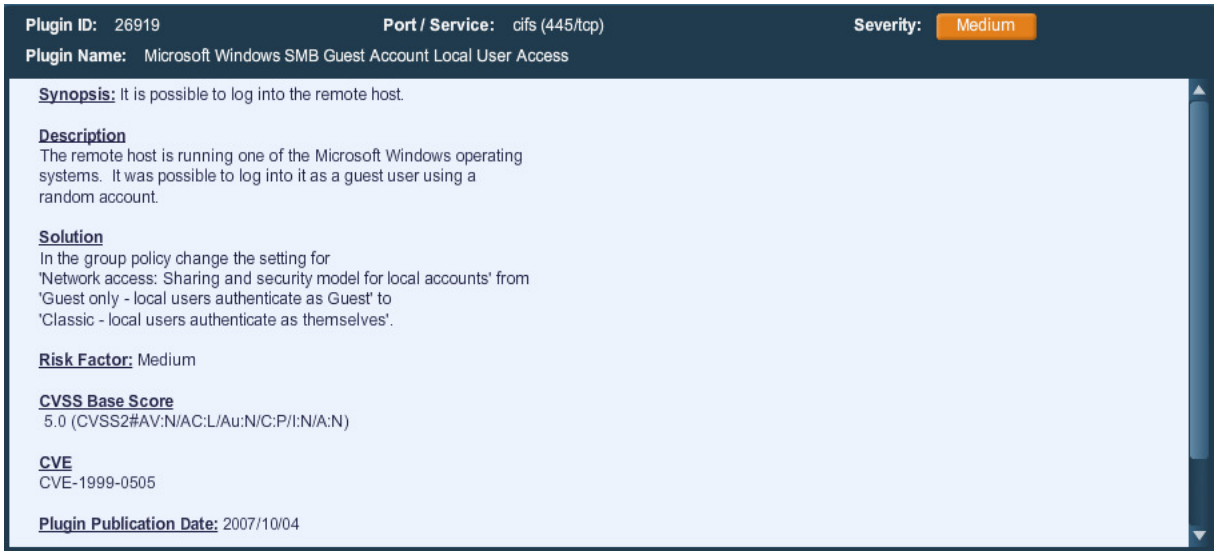


komplet | 192.168.1.2 | 3 results

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
445	tcp	cifs	1	0	1	0	0
1241	tcp	nessus	1	0	1	0	0
8834	tcp	www	1	0	1	0	0

Obr. 13 – *Medium nedostatky zjištěné u IP adresy 192.168.1.2*

Předchozí výstup z programu byl vyhodnocen jako částečně chybný, jelikož dva ze tří detekovaných nedostatků se týkali samotného programu Nessus, respektive navázaného internetového spojení s domovskou organizací našeho skeneru. Konkrétněji se chyby týkali nedůvěryhodností certifikátu SSL, který nebyl podepsán žádnou veřejnou organizací, kterou daný počítač důvěřuje. Následně byla zjištěna skutečnost, že během probíhajícího testování byl minimalizován prohlížeč internetových stránek, jehož prostřednictvím se samotná aplikace Nessus stáhla. Tyto dva detekované nedostatky tedy byly ignorovány. Třetí nedostatek se už ale týkal jiné skutečnosti. Výstup skeneru v rámci této detekované skutečnosti je následující:



Plugin ID: 26919 **Port / Service:** cifs (445/tcp) **Severity:** Medium

Plugin Name: Microsoft Windows SMB Guest Account Local User Access

Synopsis: It is possible to log into the remote host.

Description
The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it as a guest user using a random account.

Solution
In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'.

Risk Factor: Medium

CVSS Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

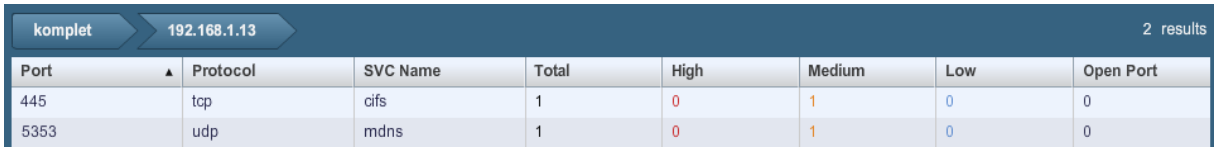
CVE
CVE-1999-0505

Plugin Publication Date: 2007/10/04

Obr. 14 – *Detailní informace týkající se zjištěného Medium nedostatku*

Další detekovaný nedostatek opět spočíval ve službě SMD, podobně tedy jako v případě detekce High nedostatku v rámci tohoto stroje. Skener Nessus nám zde oznamuje, že je potenciálně možné se přihlásit jako Guest uživatel v rámci síťových práv. Bylo tedy využito řešení popsané přímo skenerem Nessus, a byla upravena politika práv v rámci uživatelských účtů, pro eliminování tohoto nedostatku.

V rámci počítače 192.168.1.2 tedy byly zhodnoceny všechny hrozby a detekované nedostatky, a ty případně upraveny. Jako další se podrobil skenování počítač s IP adresou 192.168.1.12, ale zde nebyly stejně jak v případě adresy 192.168.1.1 nalezeny žádné závažnější nedostatky. V rámci tedy již posledního počítače s IP adresou 196.168.1.13, byly detekovány následující nedostatky:

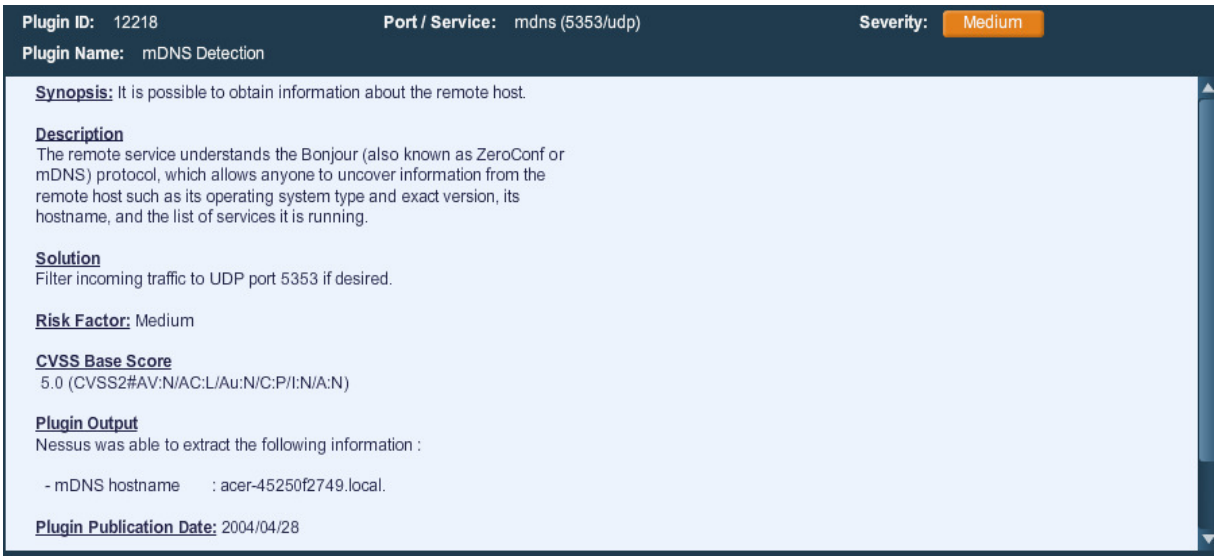


komplet | 192.168.1.13 | 2 results

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
445	tcp	cifs	1	0	1	0	0
5353	udp	mdns	1	0	1	0	0

Obr. 15 – *Přehled informací týkající se zjištěných Medium nedostatku*

Přehled detekce v rámci posledního počítače ukázal dvě možné bezpečnostní hrozby, ohodnocené střední prioritou. První hrozba se opět týká služby SMB. Při detailnějším pohledu jsme zjistili, že se dokonce jedná o stejné zjištění týkající se uživatelského účtu Guest. Bylo tedy přijato stejné opatření jako v případě počítače 192.168.1.2, a upravena politika přístupových práv. Druhé a zároveň poslední závažnější detekované narušení síťové bezpečnost se týkalo služby mDNS.



Plugin ID: 12218 **Port / Service:** mdns (5353/udp) **Severity:** Medium

Plugin Name: mDNS Detection

Synopsis: It is possible to obtain information about the remote host.

Description
The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

Solution
Filter incoming traffic to UDP port 5353 if desired.

Risk Factor: Medium

CVSS Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Output
Nessus was able to extract the following information :

- mDNS hostname : acer-45250f2749.local.

Plugin Publication Date: 2004/04/28

Obr. 16 – *Detailní informace týkající se zjištěného Medium nedostatku v rámci počítače s IP adresou 192.168.1.13*

Skener Nessus zde detekoval „Bonjour“ protokol, který je někdy známý také jako „ZeroConf“, umožňující prakticky komukoliv odkrýt informace, týkající se daného počítače.

Přesněji se může jednat o prozrazení typu operačního systému a jeho přesné verze, zjištění názvu počítače či poskytnutí seznamu využívaných služeb. V rámci tohoto zjištění bylo vydáno doporučení majiteli společnosti, týkající se filtrování příchozího provozu na portu 5353.

4.3.3 Shrnutí síťového průzkumu a přijatá opatření

V rámci provedeného základního průzkumu stavu síťové bezpečnosti, v cílové organizaci, byly zjištěny výše popsané nedostatky. Jeden nedostatek byl ohodnocen dokonce vysokou prioritou a pěti dalším byla přiřazena priorita střední. Další detekované hrozby byly vzhledem ke svému nízkému významu ignorovány, jelikož tato práce má omezený rozsah a toto zkoumání by si vyžádalo už značně detailní provedení analýzy stavu síťové bezpečnosti.

Následně po ukončení testování byla přijatá opatření týkající se politiky uživatelských práv, kde byl upraven zejména Guest účet, ale i opatření týkající se sdílených dokumentů v rámci lokální sítě. V tomto případě byla přesunuta složka sdílených dokumentů na pevný disk stolního počítače. Zejména z důvodu zamezení mobility těchto dát, kdy docházelo i k situacím, že se přenosný počítač s těmito daty, která byla připravena ke sdílení v rámci sítě, přihlašoval do cizích a veřejných sítí. Přesunem na disk pevného počítače se tak tomuto jevu zamezilo. V rámci posledního detekovaného nedostatku bylo vydáno doporučení směřující k zavedení filtrování provozu na otevřených portech, případně jejich deaktivaci pokud se tyto porty nevyužívají.

5. Závěr

Porovnáme-li dosažené poznatky se zadanými cíli, docházíme k závěru, že první cíl obsahující seznámení čtenáře této diplomové práce s problematikou síťové bezpečnosti byl splněn. Konkrétně ke splnění tohoto cíle došlo v rámci části literární rešerše, kde byla tato problematika představena. V rámci této kapitoly došlo i k představení základních principů síťové bezpečnosti a seznámení se s dokumentem bezpečnostní politiky organizace. Následně byla představena i mezinárodní kriteria pro hodnocení bezpečnosti prvků informačních systémů.

V rámci stanoveného druhého cíle, došlo k vykonání dotazníkového šetření, v jehož rámci byla zjištěna zejména poměrně alarmující neznalost dokumentu bezpečností politiky, respektive jeho obsahu a způsobu využívání. V této problematice byly nalezeny značné rezervy, týkající se využívání tohoto dokumentu oslovenými organizacemi. Došlo i k porovnání znalostí jednotlivých mezinárodních kriterií IT profesionály, v rámci kterého byla prokázána největší znalost kriterií ITSEC, navzdory faktu existence novějších kriterií CC, které se dočkali implementace i v rámci české státní normy pod označením ISO/IEC 15408. Další závěry vyvozené ze získaných dat v rámci dotazníkového šetření jsou uvedeny v rámci kapitoly 4.2.6 – Shrnutí dotazníkového šetření.

Třetím cílem bylo vykonání základního bezpečnostního auditu v rámci již konkrétní počítačové sítě. Pro tyto účely bylo využito síťového skeneru Nessus. Tento cíl byl splněn v rámci kapitoly 4.3 – Základní průzkum sítě LAN. Ze skenování cílové sítě vyplynulo celkem šest možných ohrožení bezpečnosti vážnějšího charakteru, přičemž jeden nedostatek byl ohodnocen nejvyšším možným stupněm ohrožení, a pět zbylých stupněm středním. Všechny tyto nedostatky byly podrobeny dalšímu zkoumání a většina jich byla téměř ihned odstraněna. Pro tyto účely se tedy jevil zvolený softwarový nástroj jako velmi vhodný pomocník, jelikož nejen že dané nedostatky a možná ohrožení v rámci sítě detekoval, ale každé i poměrně podrobně popsal a uvedl nejčastější způsob jejich možné eliminace. Cíl ukázky bezpečnostního auditu, respektive počítačové sítě v elementární podobě byl tedy v rámci této kapitoly také splněn.

6. Seznam použitých zdrojů

[1] BARTOŠEK, M.. *Krátce z historie Internetu*. Zpravodaj ÚVT MU. ISSN 1212-0901, 1995, roč. V, č. 3, s. 10-13.

[2] ČERMÁK Miroslav. *Řízení informačních rizik v praxi.* 1. vydání, Brno: Tribun EU, 2006. 133 s. ISBN 978-80-7399-731-1.

[3] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP – Bezpečnost.* 2. aktualizované vydání. Praha: Computer Press, 2003. 572 s. ISBN 80-7226-849-X

[4] LUDVÍK, Miroslav. *Teorie bezpečnosti počítačových sítí.* 1.vydání. Kralice na Hané: Computer Media, 2008. 98 s. ISBN 978-80-866686-35-6

[5] ODOM, Wendell. *Počítačové sítě, bez předchozích znalostí.* 1.vydání, Brno: CP Books, 2005. 384 s. ISBN 80-251-0538-5.

[6] THOMAS M. Thomas. *Zabezpečení počítačových sítí.* 1.vydání, Brno: CP Books, 2005. 338 s. ISBN 80-251-0417-6.

[7] *Analýza rizik: Jemný úvod do analýzy rizik* [online]. 2007[cit. 2011-03-17]. Dostupný z WWW: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[8] *Bezpečnost informačních system* [online] 2000[cit. 2011-03-22]. Dostupný z WWW:< http://aplikace.mvcr.cz/archiv2008/micr/files/479/uvis_bezpecnost_20000701.pdf>

[9] *Bezpečnost IS/IT* [online] 2006[cit. 2011-03-29] Dostupný z WWW:< https://akela.mendelu.cz/~lidak/bis/6cc.htm>

[10] *Bezpečnostní politika v praxi* [online] 2010[cit. 2011-03-17].Dostupný z WWW:< http://ictsecurity.cz/odborne-clanky/bezpecnostni-politika-v-praxi.html>

[11] *CIA: Důvernost-Integrita-Dostupnost* [online]. 2007[cit. 2011-03-17]. Dostupný z WWW: < http://www.cleverandsmart.cz/duvernost-integrita-dostupnost/>

[12] *Common Criteria* [online] 2006[cit. 2011-03-29] Dostupný z WWW:< http://www.commoncriteriaportal.org>

[13] *Hodnocení informační bezpečnosti* [online] 2002[cit. 2011-03-24] Dostupný z WWW:< https://akela.mendelu.cz/~lidak/share/snimky-bis/prednaska5.ppt>

[14] *Informace o hodnocení bezpečnosti informačních technologií* [online] 2002[cit. 2011-03-28] Dostupný z WWW:< http://www.nbu.cz/_downloads/bezpecnost-informacnich-systemu/container-nodeid-748/infoobit.pdf>

[15] *Jak vypracovat bezpečnostní politiku v podniku* [online]. 2005[cit. 2011-03-20]. Dostupný z WWW: < http://securityworld.cz/securityworld/jak-vypracovat-bezpecnostni-politiku-v-podniku-1269>

[16] *Ochrana IT infrastruktury v akademické prostředí* [online]. 2007[cit. 2011-03-20]. Dostupný z WWW: http://www.securityrevue.com/article/2010/09/ochrana-it-infrastruktury-v-akademickem-prostredi//

[17] *Počítačové sítě – Co je to počítačová síť?* [online]. 2001[cit. 2011-03-10]. Dostupný z WWW: < http://site.the.cz/index.php?id=1>

[18] *Řížení a správa uživatelských oprávnění v informačních systémech* [online]. 2008[cit. 2011-03-19]. Dostupný z WWW: < http://www.peakpointnet.cz/cs/klienti/zustante-s-nami/clanky/rizeni-a-sprava-uzivatelskych-opravneni-v-informacnim-systemu>

7. Přílohy

7.1 Dotazník

Dobrý den,
jsem studentem studijního programu Systémového inženýrství na České zemědělské univerzitě v Praze. V současné době píši diplomovou práci na téma síťové bezpečnosti a standardů. Za tímto účelem si Vás dovoluji poprosit o vyplnění níže uvedeného dotazníku, týkajícího se informační bezpečnosti a mezinárodních norem.

Jsem si vědom, že se může jednat o poměrně citlivé informace, a prohlašuji, že všechny poskytnuté informace budou zpracovány anonymně, pokud na konci dotazníku nepovolíte zveřejnění názvu organizace. I v tomto případě bude ale vaše organizace uvedena pouze jako zdroj informací v rámci dotazníkového šetření v mé diplomové práci. Žádné bližší data ani konkrétní odpovědi nebudou pod názvem vaší organizace v žádném případě nikde zveřejněny.

1. Existuje ve vaší organizaci dokument bezpečnostní politiky IT?

Ano	Nevím	Ne

2. V případě že existuje, jsou s tímto dokumentem bezpečnostní politiky seznamování všichni nový zaměstnanci? (Pokud neexistuje nevyplňujte)

Ano	Nevím	Ne

3. Jaký je charakter rozsahu dokumentu bezpečnostní politiky u vaší organizace? (Pokud dokument neexistuje nevyplňujte)

Stručný (do 3 stran)	Střední (3 - 20 stran)	Rozsáhlý (20 a více stran)

4. Znáte některé mezinárodní normy či standardy týkající se bezpečnosti informačních systémů?

Ano	Ne

5. Znáte některá z níže uvedených mezinárodních kriterií hodnocení bezpečnosti informačních systémů? (Označte ta, která znáte)

TCSEC	CTCPEC	ITSEC	FC	Common Criteria

6. Využívá vaše organizace některé mezinárodní standardy v rámci informační bezpečnosti?

Pouze interní směrnice a předpisy
ISO/IEC 27000
ITIL
Standardy a směrnice vydané EU pro oblast bezpečnosti IS
Nevím o žádných
Jiná odpověď:

:

7. Víte, čeho se týká norma ISO/IEC 15408?

Ano	Ne

8. Má vaše organizace oblast bezpečnosti IS/IT posouzenou externím nezávislým subjektem?

Ano	Nevím	Ne

9. Jak hodnotíte bezpečnost vámi využívaného informačního systému?

Vynikající	Dobrá	Průměrná	Slabá	Nedostatečná

10. Jaký útvar je ve vaší organizaci zodpovědný za informační bezpečnost?

IS/IT
Útvar bezpečnosti
Ekonomický či finanční útvar
Jiný útvar
Externí - outsourcing
Žádný útvar
Nevím

11. Kolik má vaše organizace zaměstnanců?

Do 50ti	50 - 200	201 a více

12. V jaké sféře organizace působí?

Státní sektor	Soukromý sektor

13. Jste zaměstnán v rámci IT oddělení?

Ano	Ne

14. V jaké organizaci jste zaměstnán? (Uveďte název)

15. Je možné zveřejnit v rámci průzkumu pro potřeby diplomové práce název vaší organizace?

(*V případě souhlasu se zveřejněním názvu vaší organizace, bude jméno organizace uvedeno pouze v rámci zdrojů dotazníkové šetření, za žádných okolností nedojde ke zveřejnění poskytnutých odpovědí pod názvem konkrétní organizace či instituce*)

Ano	Ne

7.2 Vybrané grafické výstupy z programu Nessus

7.2.1 Počítač 192.168.1.1

komplet | 192.168.1.1 — 21 results

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	udp	general	1	0	0	1	0
0	tcp	general	7	0	0	7	0
0	icmp	general	1	0	0	1	0
80	tcp	www	6	0	0	4	2
135	tcp	epmap	3	0	0	1	2
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	3	0	0	1	2
443	tcp	www	6	0	0	4	2
445	tcp	cifs	9	0	0	7	2
554	tcp	rtsp?	2	0	0	0	2
3260	tcp	iscsi-target	3	0	0	1	2
3261	tcp	starwind_ctl	3	0	0	1	2
7135	tcp	unknown	1	0	0	0	1
19201	tcp	unknown	1	0	0	0	1
49152	tcp	dce-rpc	1	0	0	1	0
49153	tcp	dce-rpc	1	0	0	1	0
49154	tcp	dce-rpc	1	0	0	1	0
49155	tcp	dce-rpc	1	0	0	1	0
49156	tcp	dce-rpc	1	0	0	1	0
49157	tcp	dce-rpc	1	0	0	1	0
50914	tcp	dce-rpc	1	0	0	1	0

7.2.2 Počítač 192.168.1.2

komplet | 192.168.1.2 — 11 results

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	10	0	0	10	0
22	tcp	ssh	6	0	0	4	2
123	udp	ntp	1	0	0	1	0
135	tcp	epmap	2	0	0	0	2
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	3	0	0	1	2
445	tcp	cifs	13	1	1	9	2
1241	tcp	nessus	8	0	1	5	2
7135	tcp	unknown	1	0	0	0	1
8834	tcp	www	15	0	1	12	2
19201	tcp	unknown	1	0	0	0	1

7.2.3 Počítač 192.168.1.12

komplet > 192.168.1.12 — 16 results

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	udp	general	1	0	0	1	0
0	tcp	general	6	0	0	6	0
0	icmp	general	1	0	0	1	0
135	tcp	epmap	3	0	0	1	2
137	udp	netbios-ns	2	0	0	2	0
139	tcp	smb	3	0	0	1	2
445	tcp	cifs	8	0	0	6	2
554	tcp	rtsp?	2	0	0	0	2
7135	tcp	unknown	1	0	0	0	1
19201	tcp	unknown	1	0	0	0	1
49152	tcp	dce-rpc	1	0	0	1	0
49153	tcp	dce-rpc	1	0	0	1	0
49154	tcp	dce-rpc	1	0	0	1	0
49155	tcp	dce-rpc	1	0	0	1	0
49156	tcp	dce-rpc	1	0	0	1	0
49157	tcp	dce-rpc	1	0	0	1	0

7.2.4 Počítač 192.168.1.13

komplet > 192.168.1.13 — 8 results

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	7	0	0	7	0
0	udp	general	1	0	0	1	0
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	3	0	0	1	2
445	tcp	cifs	12	0	1	9	2
5353	udp	mdns	1	0	1	0	0
7135	tcp	unknown	1	0	0	0	1
19201	tcp	unknown	1	0	0	0	1