Bezpečnostní audit v organizaci

Milan Seiler – FN Motol

Ve svém příspěvku na téma „Bezpečnostní audit v organizaci“ bych se chtěl věnovat 2 problémům:

1) zdůraznit účel a podstatu bezpečnostního auditu (BA) v systému řízení bezpečnosti v organizaci, a
2) demonstrovat jeho podstatu na praktickém příkladu jeho provedení, samozřejmě ve velmi zjednodušené podobě.

1. Místo auditu v řízení bezpečnostního systému

Pokud chceme charakterizovat BA, musíme se stručně zmínit o:

a) obsahu pojmu **BEZPEČNOST**

BEZPEČNOST = stav, kdy je velikost všech rizik v organizaci na přijatelné úrovni

(rizika jsou optimalizována)

b) a o nástroji k zajištění bezpečnosti v organizaci (tj. k optimalizaci rizik v organizaci), kterým je **BEZPEČNOSTNÍ SYSTÉM**

Bezpečnostní systém se vyznačuje zejména

- **dynamikou, a**
- **trvalým vlivem řady proměnlivých faktorů na procesy, které v něm probíhají.**

Nestálými podmínkami jsou jak vnitřní tak i vnější okolnosti, které jsou velmi různorodé a působí v závislosti na povaze bezpečnostního systému. Společným faktorem změn pro většinu bezpečnostních systémů je zejména právní rámec, ve kterém působí, protože **způsob ochrany bezpečnostních zájmů organizace musí být vždy v souladu s pravidly danými právním řádem**.

Např. v oblasti bezpečnosti a ochrany zdraví při práci jde v současné době v souvislosti s implementací právního řádu Evropské unie o zásadní faktor změn, které se postupně promítají do obecně závazných právních předpisů ČR, upravujících bezpečnostní problematiku v podniku. V této souvislosti stojí za zmínku jeden z posledních, nově přijatých právních předpisů, tj. nařízení vlády č. 101/2005 Sb., o podrobnějších požadavcích na pracoviště a pracovní prostředí, účinné od 1.3.2005, které vymezuje zaměstnavateli povinnosti i v oblasti klasické, míněno fyzické bezpečnosti pracovišť, když v § 3, odst. 3 ukládá zaměstnavateli povinnost, aby před uvedením pracoviště do provozu a používání zajistil opatření pro zdolávání mimořádných událostí a zabezpečil pracoviště proti vstupu nepovolaných osob, a to i v mimopracovní době. V určitém smyslu dochází tímto nařízením k **prolomení dosud poměrně výrazně vymezených hranic mezi BOZP a ostatními bezpečnostními obory v organizaci**.

Ale vraťme se zpět k tématu. Ze zmíněné, velmi zjednodušené charakteristiky bezpečnostního systému vyplývá, že k zajištění jeho optimální funkce je nezbytné, aby v jeho životních cyklech byla udržována **rovnováha** mezi:

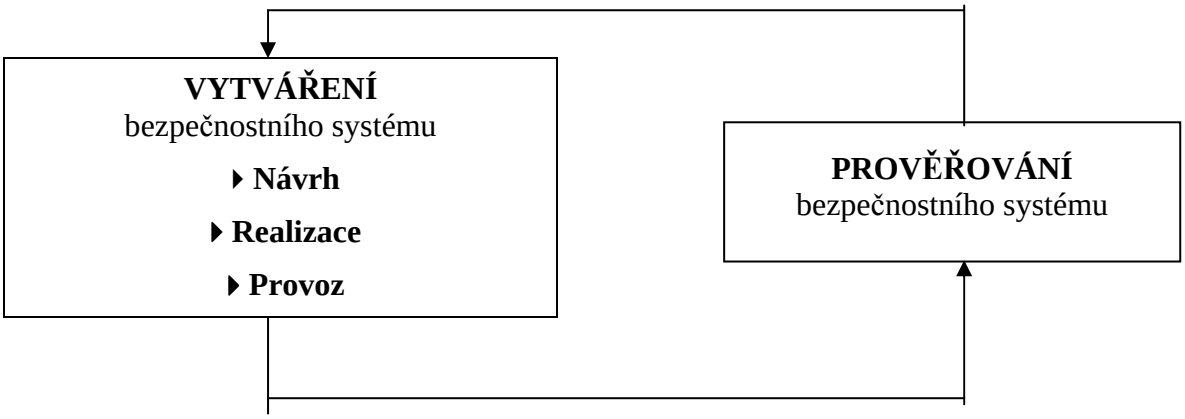
a) **dynamikou systému ovlivňovaného nestálými podmínkami**, na straně jedné a

b) **potřebou zachování jeho účinnosti**, resp. efektivnosti na straně druhé.

Řízení bezpečnostního systému proto vyžaduje dohled nad procesy, které v něm probíhají.

Jedním z velmi účinných nástrojů k trvalému udržování efektivnosti a účinnosti bezpečnostního systému je jeho **systematické prověřování**, na základě něhož by měly být prováděny potřebné kvalifikované a systémově orientované korektury. **Prověřování proto musí být součásti životního cyklu bezpečnostního systému.**

Životní cyklus bezpečnostního systému, který se řídí obecnými principy řídícího cyklu, má tedy dvě základní fáze – VYTVÁŘENÍ a PROVĚŘOVÁNÍ.



Způsobů **prověřování** bezpečnostního systému existuje, a v praxi se i používá, celá řada – např. dozor, revize, prověrka, posouzení, inspekce, kontrola atd., a v míře již ne tak časté i **bezpečnostní audit.**

BEZPEČNOSTNÍ AUDIT je jedním z nejúčinnějších způsobů prověřování bezpečnostního systému. Na rozdíl od většiny ostatních způsobů prověřování **bezpečnostní audit** ověřuje :

1) nejen **funkčnost systému** (tj. stejně jako ostatní způsoby), ale i
2) **správnost jeho nastavení** v organizaci, tj. **soulad s obecně závaznými předpisy** a **dosažení optimalizace rizik** (= účinnost).

Z uvedeného vyplývá, že bezpečnostní audit lze provádět pouze tam, kde již nějaký bezpečnostní systém existuje. To je základní podmínka, jinak by se jednalo o vytváření nového systému.

Nejlépe lze podstatu BA vystihnout na příkladu jejího srovnání s kontrolou, kde si rozdíly můžeme ukázat na 4 základních aspektech:

- **zařazení v řídící struktuře organizace,**
- **na podstatě obou způsobů,**
- **na subjektu, který je provádí,**
- **na cíli.**

	Vnitřní kontrola	**Interní audit**
Zařazení	součást všech úrovní řízení	nástroj vrcholového vedení organizace
Spočívá	ve zjišťování odchylek stavu skutečného od stavu žádoucího	v nezávislém ověřování všech činností probíhajících v organizaci, jehož podstatou je **zjišťování rizik a jejich následné řízení**
Provádí	všichni řídící pracovníci	pracoviště interního auditu
Cíl	odstranění zjištěných nedostatků	**zvyšování efektivnosti** a účinnosti bezpečnostního systému

Audit hodnotí současný stav systému z hlediska budoucí perspektivy. Jeho účelem je především předcházet chybám a teprve v druhé řadě napravovat chyby, které již nastaly. Zaměřuje se tedy především na prevenci systémových nedostatků a na jejich vyhledávání ve stávajícím systému bezpečnosti podniku.

Ještě jeden důležitý rys BA – mezi jeho hlavní cíle nepatří postih odpovědných pracovníků organizace sankcemi za zjištěné nedostatky.

V zásadě platí, že BA by měl provádět subjekt, který není za auditovanou oblasti odpovědný.

Průběh bezpečnostního auditu

Průběh BA se fakticky řídí principy organizačního cyklu v obecném smyslu

PROVĚŘENÍ – shromáždění všech dostupných údajů známými metodami (rozhovor, seznámení s dokumentací, pozorování, srovnávání, modelování …. atd.)

ANALÝZA – vyhodnocení stavu z hlediska rizik, tvoří stěžejní fázi celého procesu, kvalita analýzy rizik určuje platnost závěrů a doporučení

DOPORUČENÍ – navržení opatření k optimalizaci rizik

Druhy bezpečnostního auditu

Audit můžeme rozlišovat podle řady hledisek, jako např. dle:

a) **časového kritéria**
   - **plánovaný audit** – ověřování stavu ochrany by mělo probíhat v předem nastavených periodických cyklech,
   - **mimořádný audit** – provádí se v případě významných změn v organizaci nebo podmínek, ve kterých působí, nebo pokud se vyskytnou závažné problémy (mimořádné události, havárie apod.),
   - **následný audit** – provádí se na doporučení auditora, pokud plánovaný nebo mimořádný audit inicializovaly zásadní změny bezpečnostního systému organizace,

b) **věcného kritéria**
   - dle zaměření (audit systému fyzické bezpečnosti, systému personální, informační bezpečnosti atd.),
   - nebo rozsahu (komplexní, dílčí).

2. Audit po mimořádné události

Výskyt mimořádných událostí v organizaci (krizových stavů, incidentů, selhání, výpadků v provozu, havárií apod.) je jedním z velmi objektivních **indikátorů účinnosti bezpečnostního systému v organizaci**.

Provádění BA lze z hlediska praktických zkušeností doporučit zejména u závažných mimořádných událostí nebo v případě často se vyskytujících mimořádných událostí.

Součástí opatření k mimořádné události – tj. kromě odstranění bezprostředních následků, musí být zejména přijetí opatření ke snížení pravděpodobnosti jejího vzniku. Proto by **každá mimořádná událost měla být analyzována jak z hlediska okolností, které její vznik a průběh umožnily, tak i okolností, které byly překážkou v jejím vzniku nebo průběhu** (pro potřeby prevence). **Účelem analýzy musí být**

- vyhodnocení funkčnosti všech prvků systému,

- analýza rizik,
- návrh a realizace opatření,
- viditelná reakce na událost.

Při analýze si musíme dát pozor na to, aby posouzení rizik bylo komplexní, a abychom eliminací jednoho, nepřesunuli riziko do jiné oblasti.

V závěru bych se chtěl pokusit demonstrovat podstatu BA na jeho provedení po konkrétní mimořádní události – **loupeženém přepadení pobočky banky.** S ohledem na časovou dimenzi mého vystoupení půjde jen o velmi zjednodušený příklad.

Popis místa

Toto je reálné orientační schéma pobočky (viz obr. č. 1), která byla skutečna přepadena. Nachází se zhruba v centru malé obce na Severní Moravě v 1. patře budovy, v jejímž přízemním podlaží je obchod. Samostatný vstup do pobočky je situován z boční, velmi přehledné ulice. Je vybavena kamerovým systémem osazeným 4 kamerami, dále systémem elektrické zabezpečovací signalizace s tísňovými tlačítky na přepážkách a dálkovým ovládáním vnějšího vstupu, které slouží k tomu, aby zaměstnanci při zahajování a ukončení provozní doby nemuseli opouštět zázemí, a při manipulaci s klíči u vstupu se vystavovat nebezpečí napadení.

Průběh události

Dne 3.března 2003 v 10.24 hod. – obě pracovnice jsou na přepážkách. Jedna z nich právě telefonuje se svým ústředím, když zaslechne vrznutí spodních vstupních dveří, mechanicky pohlédne na monitor a spatří postavu maskovanou kuklou, vybíhající po schodech do pobočky. Stačí ještě do telefonu oznámit, že jsou přepadení a pachatel již vniká do prostoru pro veřejnost. Další průběh je již obvyklý – pod pohrůžkou použití zbraně je mu vydána část hotovosti na přepážkách a pak spěšně opouští místo.

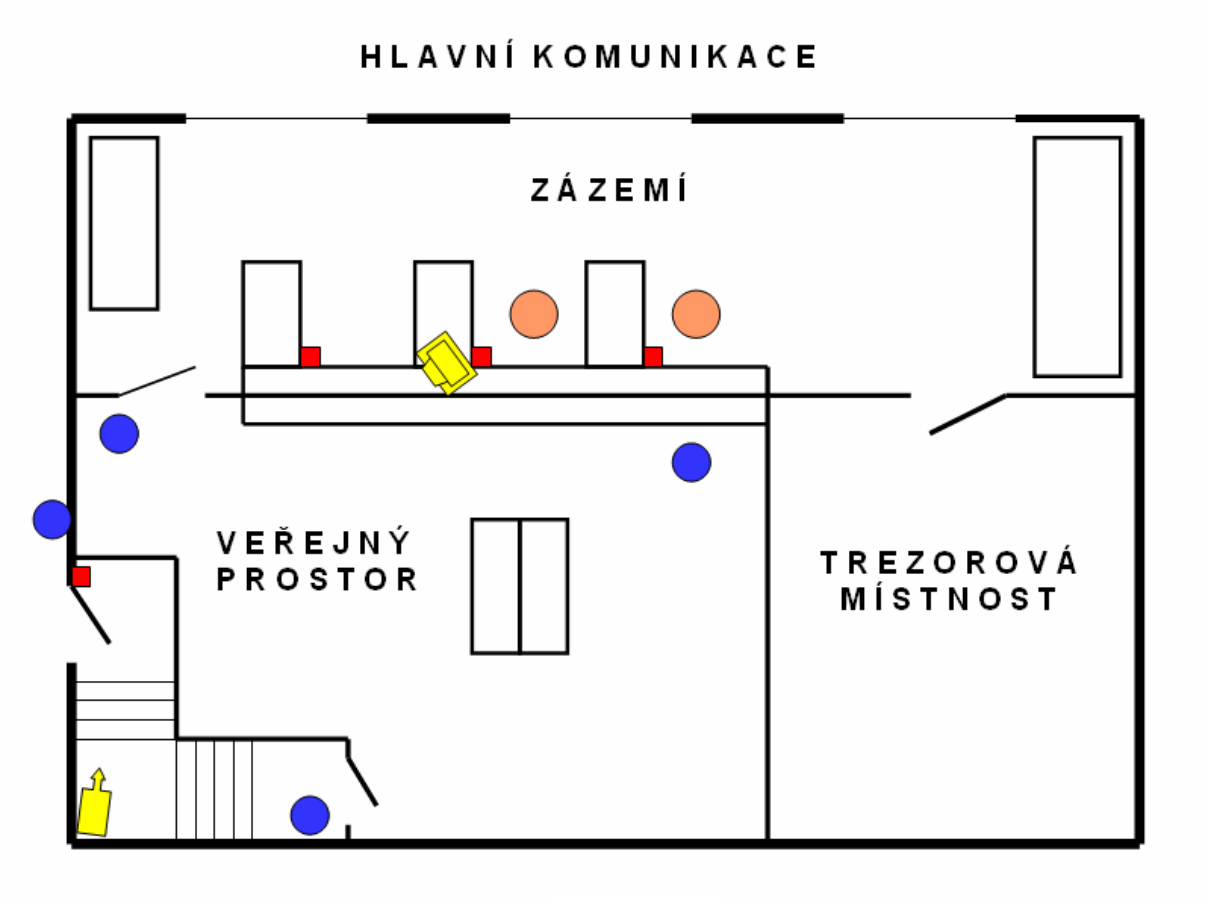
Výsledek kontroly

Následně po této události byla na pobočce provedena kontrola, která nezjistila žádné závady či porušení vnitřních pravidel, snad kromě překročení limitu pokladního zůstatku, které však nemělo na průběh události žádný dopad.

Analýza rizik

Pomiňme nyní výsledek kontroly a podívejme se na bezpečnostní systém pobočky z pohledu bezpečnostního auditu, zaměřeného na snížení rizika loupežného přepadení

1. **Základní informace o stavu ochrany máme**
2. **Pokusme se definovat rizika**, a to nezávisle na způsobu provedení uvedeného loupežného přepadení:
   - z pravidelných analýz v dané bance víme, že tato pobočka svým parametry patří mezi pobočky se zvýšenými rizikem (tj. počtem personálu, lokalitou, dispozičním řešením vstupních prostor),
   - u takto dispozičně řešených poboček může být personál napaden 5 základními způsoby – viz Obr. č.1
     - při příchodu před vstupem do budovy, při odchodu ve vnitřních prostorách budovy tvořících přístupovou cestu, při odemykání vstupních dveří v době zahájení a uzamykání při ukončení provozu, klasicky přes přepážku a při opuštění zázemí u dveří nebo dveřmi vstupu do zázemí, velikost těchto rizik lze odvodit ze statistických údajů platných pro banku (klasický způsob převažuje cca 70%, zbytek ostatní, druhý nejčastější při příchodu nebo u vstupu).



Obr. č. 1

Opatření

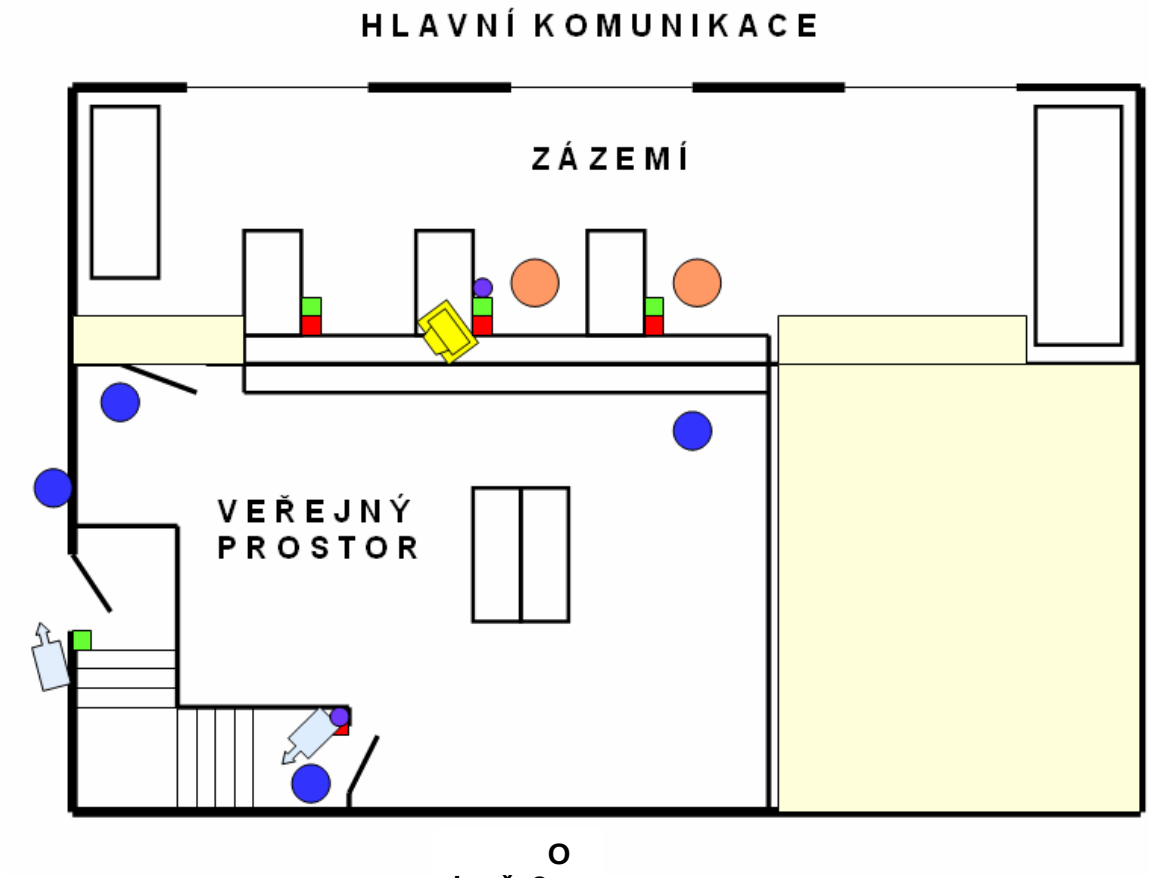
Naše opatření by měla směřovat především ke **snížení rizika přepadení přes přepážku, protože je toto riziko nejvyšší.** Jak? Změnou filosofie zabezpečení pobočky.

Z analýzy loupežných přepadení banky vyplývá důležitý poznatek, útok lze překazit nebo snížit jeho následky, jestliže je **potenciálně nebezpečná situace včas zpozorována personálem** (čím dříve tím lépe), a tento **má vytvořené podmínky pro odpovídající reakci**,

- z popisu průběhu události víme, že zaměstnanci jsou schopni **registrovat přicházející osoby** ještě před vstupem do pobočky,
- proto **dálkově ovládaný zámek** přesuneme na vstupní dveře do prostoru pobočky a doplníme jej
- **komunikačním zařízením,** které bude sloužit pro komunikaci s příchozími, které personál nevpustí dovnitř,
- **změníme směr otevírání vstupních dveří do pobočky** - protože ze zkušeností víme, že vstupující klient do banky by měl být z pohledu personálu dveřním křídlem odkrývám nikoliv zakrývám, **otočíme smysl zavírání dveří,**
- **zajistíme signalizaci otevření venkovních dveří** - aby zaměstnanci byli včas informováni o osobách vstupujících do budovy, **osadíme vstupní dveře optickou a akustickou signalizací vyvedenou na přepážkách**, na kterou mohou včas reagovat – zámek uzamknout v případě vzniku ohrožující situace, nebo jej mít trvale uzamčený (vycházejme z důležité skutečnosti - personál s ohledem na velikost lokality a délku praxe v pobočce drtivou většinu svých klientů vizuálně pozná), příp. může být zámek uzamčený jen v kritických časech v průběhu dne (zahájení provozu a cca 30 min. po něm, polední doba, ukončení provozu a cca 60 min. před ním),

- **úprava kamer** – současně s tím je potřebné **přesunout kameru před vstup do prostoru pobočky**, důvody jsou dva – abychom umožnili personálu kontrolu osob před uzamčenými dveřmi, a současně prodloužili čas mezi vstupem osoby do budovy (signalizací vstupu) a možností její kontroly na monitoru, pokud se personálu v tu chvíli nenachází na svých pracovních místech,
- **skryté kamery** - v zájmu snížení předvídatelnosti prostředí pachatelem, by bylo vhodné **provést obě kamery umístěné mimo vnitřní prostory pobočky jako skryté,**
- také **vstupní dveře do zázemí** by měly být provedeny tak, aby lépe odolávaly možnému pokusu o násilné překonání z veřejného prostoru pobočky – tzn. **změnit směr jejich otevírání tak, aby se opíraly o zárubeň ve směru z haly pobočky,**
- **vymezit únikové prostory** – neměli bychom zapomenout stanovit tzv. únikové prostory, tj. prostory, ve kterých je možnost ohrožení zaměstnanců banky střelnou zbraní při loupeži značně ztížena (nejsou pod vizuální kontrolou pachatelů) nebo zcela vyloučena (nejsou pod vizuální kontrolou a současně chráněni před účinkem zbraně), z povahy těchto míst vyplývá, že jsou určeny k umístění všech prvků důležitých pro bezpečnost provozu pobočky (klíče od vstupů, úschovných objektů, řídící jednotky zabezpečovacích systémů apod.).

Výsledný způsob zabezpečení pobočky na základě doporučení bezpečnostního auditu je patrný z Obr. č. 2.



Kromě těchto opatření bylo v tomto konkrétním případě potřebné

- **změnit nastavení zobrazení kamer na monitoru** umístěném na přepážce tak, aby byly zobrazeny pouze záběry kamer v prostoru, který není pod přímou vizuální kontrolou personálu,

- **vyřešit světelné podmínky v pobočce**, kde v důsledku venkovního světla za zády personálu tomuto brání odlesky na prosklených bezpečnostních nástavbách v nerušeném výhledu do prostoru pro veřejnost,
- **upravit dveřní kukátko** na vstupních dveřích do budovy, které bylo umístěno ve výšce, která neodpovídala výšce zaměstnanců, bylo tedy mimo jejich dosah,
- **vybavit zaměstnance mobilními tísňovými hlásiči** pro případ napadení při příchodu či odchodu nebo v situaci mimo dosah pevných tísňových hlásičů,
- **provést kvalifikované poučení zaměstnanců** o smyslu a filosofii daného způsobu zabezpečení a doporučených způsobech chování, včetně postupu při řešení předpokládaných situací,
- **seznámení s únikovými prostory**, jejich účelem a postupu při jejich využití v ohrožující situaci.

Závěrem je potřebné dodat, že uvedená opatření neodstraňují riziko loupežného přepadení zcela, ale podstatným způsobem zvyšují pravděpodobnost jeho překažení.

Tento příklad neměl být návodem na způsob řešení ochrany bankovních poboček, ale demonstrací způsobu provedení bezpečnostního auditu v konkrétních podmínkách.

Literatura

Nečas, S., Seiler, M., Porada, V., Chmelík, J., Straus, J.: *Loupežná přepadení pracovišť s peněžním provozem a jejich bezpečnost (policejní, kriminalistické a technické aspekty teorie a praxe ochrany osob a majetku)*. Praha : PA ČR, 2004

JUDr. Milan Seiler, FN Motol, V Úvalu 84, Praha 5, E-mail:milan.seiler@seznam.cz