VŠB - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Ing. Pavel Šenovský, Ph.D.

# Bezpečnostní informatika 2

skripta


Ostrava, 2012

**Bezpečnostní informatika II**
5. rozšířené vydání
tento text neprošel jazykovou úpravou

Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

# Obsah

# Seznam obrázků

# Seznam tabulek

# Úvod

Vážený studente, dostává se Vám do rukou učební text Bezpečnostní informatika (BI) II. Tento text je především určen studentům stejnojmenného předmětu, který naše Fakulta bezpečnostního inženýrství (FBI) nabízí ve druhém ročníku některých oborů. Jak již název napovídá, tyto učební texty navazují na skripta BI I a předpokládá se, že se čtenář s tímto textem alespoň zběžně seznámil.

Mým cílem při psaní tohoto textu bylo, aby čtenář získal základní přehled v oblasti informačních systémů a to z různých pohledů. Koncepce textu přitom není zaměřena na „informatiky“, proto se v jednotlivých probíraných tématech nejde příliš do hloubky.

Texty by ale měly umožnit čtenáři zorientování se v problematice informačních systémů, jejich použití, nasazování ve státní správě, ale také způsoby technické certifikace z hlediska bezpečnosti.

V těchto skriptech se setkáte také ve větší míře s odkazy na legislativu. To je způsobeno poměrně přísnými požadavky na použití informačních systémů ve státní správě a nároků na jejich spolupráci.

Pro zpříjemnění čtení jsem se také rozhodl zpracovat tento text formou vhodnou pro „distanční vzdělávání“ tak, aby práce s ním byla co možná nejjednodušší. Z tohoto důvodu je text jednotlivých kapitol segmentován do bloků.

Každá kapitola začíná krátkou anotací, ve které se dozvíte, o čem budeme v kapitole mluvit a proč. V bodech se pokusím shrnout, co byste po prostudování kapitoly měli znát a kolik času by Vám studium mělo zabrat. Prosím mějte na paměti, že tento časový údaj je pouze orientační, nebuďte proto smutní nebo naštvaní, když ve skutečnosti budete kapitole věnovat o něco méně nebo více času.

Pro zjednodušení orientace v textu jsem zavedl systém ikon:

**Průvodce studiem**
Slouží pro seznámení studentů s látkou, která bude v kapitole probírána.

**Čas nutný ke studiu**
Představuje odhad doby, který budete potřebovat k prostudování celé kapitoly. Jedná se pouze o orientační odhad, neznepokojujte se proto, pokud Vám studium bude trvat o něco déle nebo budete hotovi rychleji.

**Vysvětlení, definice, poznámka**
U této ikony najdete vysvětlující text, poznámku k probíranému tématu, která problém uvede do širších souvislostí, popřípadě důležitou definice.

V novém (už pátém!) vydání jsem se rozhodl pro trošičku jiný způsob přípravy skript a celá jsem je přepsal v desktop publishing (DTP) systému LaTeX. Důvodem jsou některé schopnosti, které je s

**Kontrolní otázky**
Na závěr každé kapitoly je zařazeno několik otázek, které prověří, zda jste problematice kapitoly dostatečně porozuměli. Pokud nebudete vědět odpověď na některou otázku, je to signál pro Vás, abyste se ke kapitole vrátili.

**Chvilka oddechu**
Text označený touto ikonkou neberte příliš vážně, je tam pro Vaše pobavení.

klasickými prostředky možné dosáhnout pouze stěží a také to, že řada z vás bude studovat tento text přímo v počítači (tabletu, čtečce elektronických knih nebo mobilním telefonu) a pokud se tak skutečně stane budete chtít využít všech schopností, která Vám tato zařízení poskytují.

Kolikrát jste si pomysleli - „jaké by to třeba bylo, kdybych mohl klepnout na jednu z těch divných zkratek (které informatici tak milují) a ona by mě přesměrovala automaticky na seznam zkratek“? Nebylo by lepší kdyby na daný literární pramen bylo možné se dostat přímo klepnutím na jeho číslo v textu, nebo aby jste nemuseli vybranou pasáž hledat přes čísla stránek, ale postačovalo by kliknout na jméno kapitoly v obsahu?

Mě jako studentovy by se líbily a proto doufám, že je oceníte i Vy, protože všechny výše uvedené možnosti skripta v PDF formátu obsahují. Aktivní odkazy jsou v textu zvýrazněny červenou (a v případě odkazů na literaturu zelenou) barvou.

Na konec skript byl přidán také rejstřík pojmů. Doporučuji, abyste jej v rámci přípravy na zkoušku prošli - zamyslete se nad tím, zda všechny pojmy, které jsem do něj zařadil, chápete a jste je schopni dát do souvislostí. Pokud ne je vedle pojmu odkaz na číslo stránky, kde je pojem probrán a Vy můžete rychle zaplnit případné mezery ve svých znalostech problematiky informačních systémů.

Přeji Vám, aby čas, který strávíte s tímto textem, byl co možná nejpříjemnější a abyste jej nepovažovali za ztracený.

Ing. Pavel Šenovský, Ph.D.

**Poznámka autora:**
Právě držíte v rukou páté rozšířené vydání skript. Je možné, že právě studujete na zkoušku, nebo jste se ke skriptům dostali pouze náhodou po delší době. Z tohoto důvodu by se Vám mohlo hodit stručné shrnutí změn mezi jednotlivými vydáními těchto skript.

**Modifikace 2. vydání:**
1. Přepracována kapitola věnovaná kritické infrastruktuře.
2. Přepracována podkapitola věnovaná normě Common Criteria (CC)

**Modifikace 3. vydání:**

1. Doplněny informace o architektuře tenkých klientů
2. Přidána kapitola ve které probereme informační systémy veřejné správy (ISVS)
3. Řada menších oprav a úprav

**Modifikace 4. vydání:**

1. Rozšířeno pojednání o datových schránkách ve smyslu nově přijímané legislativy
2. Aktualizována část věnována ISVS v souvislosti se zákony 111/2009 Sb. a 227/2009 Sb.

**Modifikace 5. vydání:**

1. Drobnější opravy v textu
2. Text vysázen v LaTeX, což by mělo umožnit vyšší kvalitu sazby a některé příjemné změny pro Vás čtenáře, jako jsou například aktivní odkazy, rejstřík apod.
3. V části věnované kritické infrastruktuře zapracovány změny v systému upozorňování na nebezpečí v USA a také rozpracováno postavení různých „reakčních týmů“ (Computer Emmergency Response Team (CERT) a Computer Security Incident Response Team (CSIRT)) u nás a ve světě.
4. Aktualizována sekce elektronických podatelen v souvislosti s přijetím zákona 167/2012 Sb., který poměrně výrazně upravuje problematiku elektronického podpisu
5. doplněna byla také problematika základních registrů a to zejména z důvodu, že základní registry se začínají aktivně používat 1.7.2012, pro zajímavost 5. vydání bylo připraveno během června 2012.

# Kapitola 1

# Informační systémy

**Průvodce studiem**
V rámci této kapitoly si zopakujeme základní pojmy z oblasti informatiky a vztáhneme je do oblasti informačních systémů, kterými se budeme převážně zabývat v tomto předmětu.

**Po přečtení této kapitoly budete**
**Znát**

- základní pojmy z oblasti informatiky

**Umět**

- rozčlenit systémy a informační systémy do několika kategorií

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

## 1.1 Typologie systémů

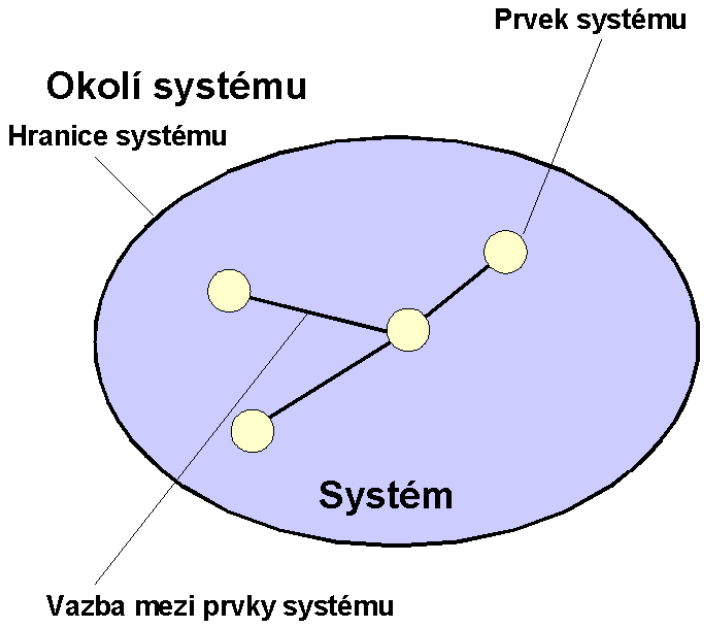
Začněme opakováním – pojem *informace*. V BI I (viz [45]) jsme si řekli, že informace je objekt nehmotné povahy, který u příjemce informace snižuje neurčitost.

*Data* oproti tomu jsou nadmnožinou informací, obsahují tedy veškeré informace a množství dalších údajů, které ale neurčitost nesnižují. Data je tedy nutné nějakým způsobem zpracovat, abychom z nich dostali požadované informace.

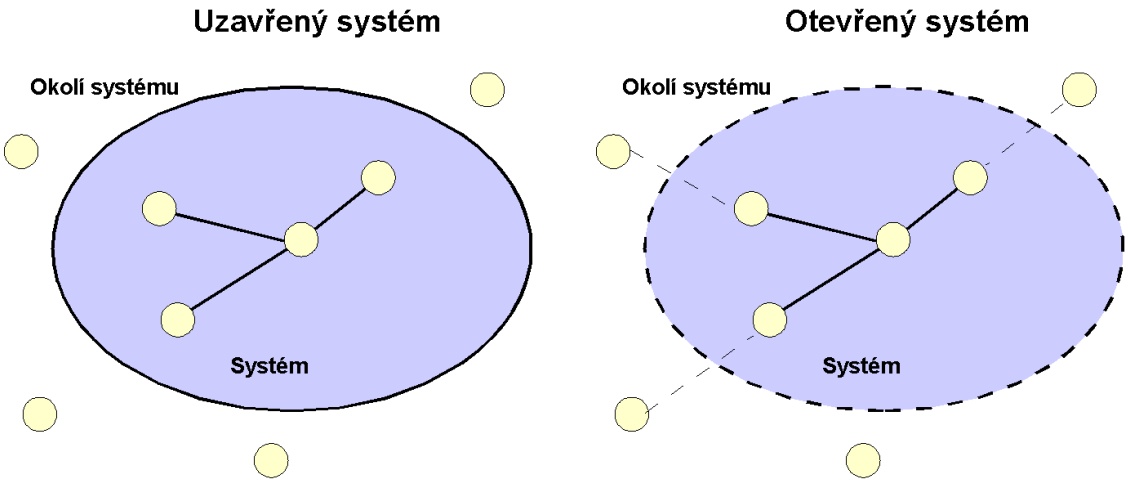
Oba tyto pojmy budeme v blízké budoucnosti potřebovat, nyní však přejdeme k pojmu jinému, a to je *systém*. V BI I jsme definovali systém jako souhrn prvků, které jsou vůči sobě v nějakém vztahu a vůči okolí působí jako celek. Takový obecný systém bychom si mohli znázornit např. podobně jako na obr. 1.1.

V definici systému jsme zmínili podstatný moment, a to že vůči okolí působí jako celek. Z toho vyplývá, že existuje nějaká *hranice systému*, kde vše uvnitř hranic je *systém* a vše vně hranic je *okolí systému*. Je logické, že podle toho, jak a zda vůbec prvky systému komunikují s okolím, můžeme systémy rozdělit na otevřené a uzavřené. Graficky bychom takovou situaci mohli znázornit podobně jako na obrázku 1.2.

*Otevřené* systémy tedy mají nějakou vazbu na prvky okolních systémů. Systémy zde chápeme v jejich obecné podobě, tedy výše uvedené skutečnosti lze aplikovat třeba na židli nebo pokročilý informační systém (IS) pro zpracování objednávek.




Obrázek 1.1: Grafické znázornění obecného systému




Obrázek 1.2: Grafické znázornění otevřeného a uzavřený systému

Možnosti komunikace s okolím však nejsou jediným kritériem, podle kterého lze systémy dělit. Dalším hlediskem použitelným pro dělení je to, zda systém vytvořil člověk. Dělíme tedy na systémy přirozené a umělé.

Systémy můžeme dále dělit podle toho, jaký aparát používáme na jejich popis. Pokud využíváme čistě matematický popis, nazýváme takové systémy tzv. *tvrdé*. Pro popis ostatních systémů využíváme *měkký* aparát – tedy alespoň částečně slovní popis.

Nadefinovali jsme pojem informace a systém, můžeme tedy nadefinovat pojem nový, který v sobě obsahuje oba tyto pojmy – IS. Spojení těchto pojmů v nás intuitivně vzbuzuje představu, že se bude jednat o nějaký systém, který napomáhá uchovávání informací a umožňuje v případě potřeby uživateli takové informace jednoduše získávat.

## 1.2 Teoretické základy informačních systémů

*Informační systém* podniku bychom mohli definovat jako souhrn lidí (peopleware), techniky (hardware) a programového vybavení (software), které jsou společně využívány v rámci podniku pro zajištění

realizace poslání tohoto podniku.

Z hlediska struktury by nám k této definici mohla ještě přibýt logistická (procesní) struktura, která popisuje logiku práce systému, ve smyslu vzájemné provázanosti prvků systému.

Informační systémy lze dělit do kategorií podle druhů informací, které zpracovávají, nebo podle úrovně řízení, kam jsou výstupy těchto IS zaměřeny.

Začneme s rozdělením IS podle úrovně řízení. Logickou úvahou můžeme dovodit, že druh informací vyžadovaných na jednotlivých úrovních řízení je různý.

Na obrázku 1.2 je představena modifikovaná pyramida řízení – třídění typů informačních systémů podle toho, pro jakou úroveň řízení jsou určeny.

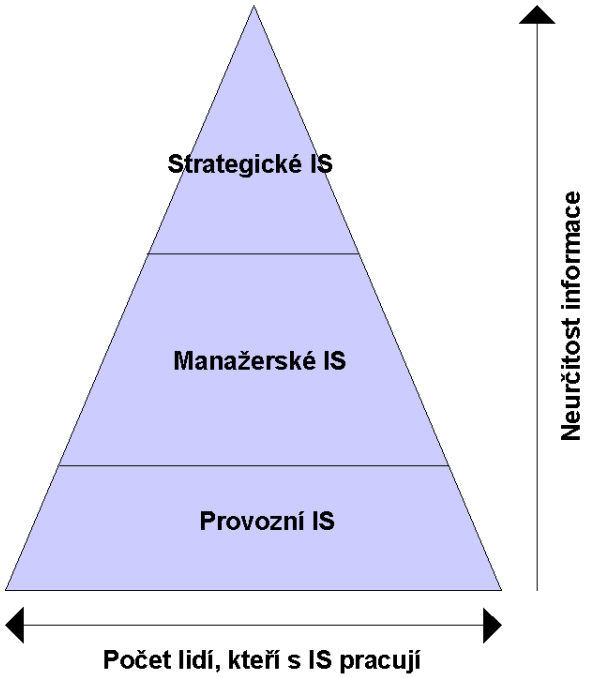
Z obrázku 1.2 vyplývá, že čím výše jsme v pyramidě, tím je menší skupina lidí, která s takovýmto systémem pracuje. Zároveň zvyšuje neurčitost informací, které jsou po informačním systému požadovány, což má přímou souvislost s typem rozhodování, které se na dané úrovni řízení provádí.

Mezi *provozní IS* můžeme zařadit systémy, se kterými pracuje běžný zaměstnanec. Může se jednat o systémy pro skladové evidence, pokladny apod., obecně tedy systémy, se kterými se pracuje neustále, dennodenně, protože s jejich pomocí je zabezpečen provoz firmy.

Nad těmito systémy fungují tzv. *manažerské IS*. Úkolem těchto systémů je poskytovat informace nutné pro efektivní řízení. U těchto systémů je již patrná určitá abstrakce, zpracování dat, která byla do celopodnikového systému zavedena prostřednictvím provozních IS.

*Strategické IS* jdou směrem k další abstrakci tak, aby vrcholový management měl k dispozici nezkreslený celkový obraz, na základě kterého lze přijímat dlouhodobá rozhodnutí.

V praxi se s takto „silně“ vymezenými IS prakticky nesetkáváme. Většina běžně provozovaných IS svou funkčností přesahuje do některé ze sousedních kategorií.




Obrázek 1.3: Pyramida řízení – obecné dělení informačních systémů

Podívejme se na obecnou architekturu informačních systémů. Většina těchto systémů je založena na architektuře **klient-server**. Každý IS bude z typologického hlediska poskytovat podobné služby:

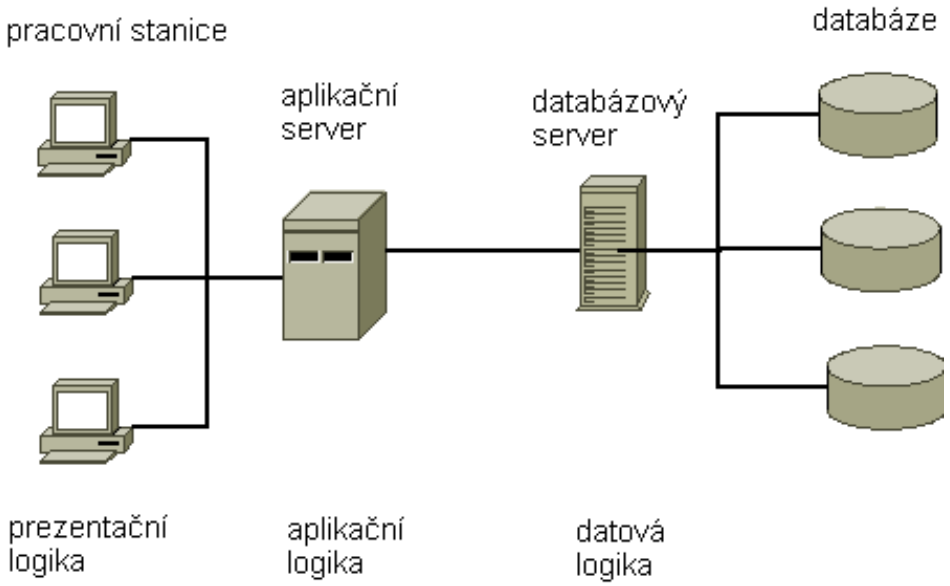
- prezentační logika
- aplikační logika
- datová logika

Prezentační logikou rozumíme především grafické uživatelské rozhraní informačního systému – tedy to jak systém vypadá a jak se chová ke koncovému uživateli. Pokyny z tohoto rozhraní jsou propagovány do aplikační vrstvy, kde jsou zpracovány a přeneseny do vrstvy datové (vkládání, editace nebo výmaz dat).

Rozdíly v architekturách klient server budou v tom, kde přesně se budou jednotlivé vrstvy nacházet.

Tradiční třívrstvá architektura je zobrazena na obr. 1.4.

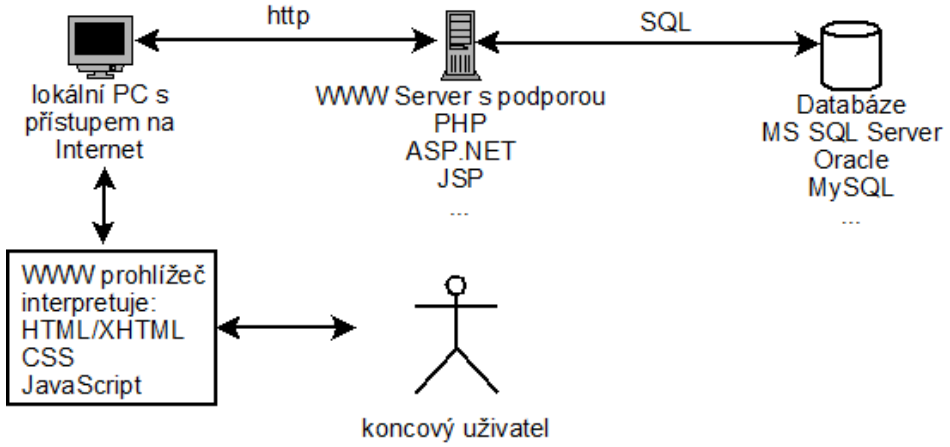
Aplikační logiku můžeme přenést oběma směry – k uživateli nebo úplně/částečně implementovat jako vnořené procedury databázového serveru. Podobně můžeme přesouvat i prezentační vrstvu. V dnešní době již není problém generovat prezentační vrstvu na serveru a pracovní stanice je tak zodpovědná pouze za vizualizaci této vrstvy ve vhodném prostředí.




Obrázek 1.4: Třívrstvá architektura klient-server

Klientům, kteří neobsahují nic víc než prezentační ani aplikační logiku, říkáme tzv. tenké klienty, ostatním logicky říkáme naopak tlusté klienty. Prostředím zobrazujícím uživatelské rozhraní často bývá prohlížeč World Wide Web (WWW).

Podívejme se tedy na architekturu informačního systému, který využívá pouze služeb tenkých klientů. Tentokráte se ale zaměříme na technologie, které mohou být využívány pro jeho realizaci. Základní představu si můžeme udělat na základě obrázku 1.5.




Obrázek 1.5: Fungování moderního tenkého klienta

Základem prakticky každého informačního systému je databázový systém. Ten umožňuje transparentně manipulovat daty v něm uchovávanými tak, aby nebyla narušena jejich referenční identita – tedy aby data byla úplná, aktuální a vždy dle potřeb přístupná.

Aplikační vrstva je zcela nebo částečně (část aplikační logiky může být obsažena na úrovni databáze a realizována pomocí trigerů) realizována na WWW serveru. Cílem je generování Hypertext Markup Language (HTML) stránek (s případnými Cascading Style Sheets (CSS) a java skripty), které se

pošlou WWW prohlížeči klienta k interpretaci.

Nosnými technologiemi v tomto ohledu bývá PHP, ASP.NET (programování v jazycích C#, VisualBasic.NET, Iron Python a další) nebo Java Servlet Pages (JSP) – programování v jazyku JAVA).

Aplikační logika naprogramovaná ve zvoleném programovacím jazyce musí na jedné straně komunikovat s databází (Structured Query Language (SQL) implementované v databázích se přitom výrobce od výrobce liší) a generovat HTML stránky pro klienta, nejlépe „oživené“ pomocí JavaScriptu – pro zvýšení pohodlnosti použití webové aplikace. Implementace HTML, JavaScriptu a CSS se přitom mezi prohlížeči také liší.

Finální aplikace tak musí být optimalizována pro zvolenou databázi a také musí být optimalizován pro cílový prohlížeč WWW.

V této směsce technologií je relativně jednoduché udělat chybu – a taková chyba se pak velmi obtížně hledá a odstraňuje.

Výhody tenkých klientů

- instalace a správa na jednom místě
- možnost práce odkudkoliv

Nevýhody tenkých klientů

- snížená rychlost a pohodlnost práce proti tlustým klientům
- rozhraní je obvykle vystaveno útokům zvenčí
- bezpečnostní rizika spojená s chybovostí a jednoduchou zneužitelností těchto chyb.

## 1.3 Práce s informací – historický pohled

Abychom mohli informační systémy rozdělit podle informací (služeb), které poskytují, musíme se nejprve podívat na vývoj informační potřebnosti ve společnosti z hlediska historického vývoje.

Z pohledu práce s informacemi lze vytipovat tři významná období. Prvním z nich je tzv. zemědělská revoluce. Počátky této etapy lze datovat někdy do pravěku, do období, kdy se tlupy kočovníků – lovců, kteří se stěhovali za potravou, postupně začali usazovat a začaly se vytvářet první stálé osady.

Konec tohoto období se datuje v Evropě do poloviny 17. století a je spojován s počátkem průmyslové revoluce. V USA se díky kolonizaci rozsáhlých území konec této etapy datuje až do poloviny století 18.

Z hlediska uchovávání a předávání informací v této etapě převažuje předávání ústní formou, později i písemně. Je si však potřeba uvědomit, že znalost čtení a psaní po velmi dlouhou dobu byla výsadou poměrně úzké skupiny bohatých, šlechty a duchovních, zatímco převážná část obyvatelstva zůstávala negramotná.

Na delší vzdálenosti byly zprávy přepravovány pomocí kurýrů. Populace v osídlených oblastech je velmi rozptýlená, dopravní infrastruktura minimální. Jednotlivá sídla jsou více či méně soběstačná, takže obchod mezi jednotlivými sídly se zaměřuje převážně na nadstandardní zboží, které v daném sídle není možné vyrobit.

Průmyslová revoluce zahajuje etapu druhou, kterou například Alvin a Heidi Tofflerovi (The Third Wave, 1980 [42]) nazývají zrodem industrializované společnosti, častěji se však používá název „průmyslové“ období.

Toto období je typické zaváděním manufaktur, které sériově chrlí výrobky, a dochází tak k postupnému vytlačování drobných řemeslníků. Koncentrace výroby na jednom místě s sebou nese zvýšené nároky na přepravu zboží a vytváří tak tlak na zlepšení dopravní infrastruktury. Navrhování, konstrukce, údržba a obsluha strojů na výrobních linkách je mnohem složitější než klasická forma ruční výroby, to s sebou nese tlak na zvyšování vzdělanosti celé populace.

Vzhledem k tomu, že v manufakturách pracuje stále větší množství lidí, dochází k přesunům lidí z venkova do měst.

S příchodem telegrafu, rádia, telefonu se prudce zvýšila možnost komunikovat a spolu s ní i využití nových komunikačních prostředků pro obchod. Zároveň se postupně mění i styl uchovávání a práce s informacemi.

Konec této etapy se uvádí začátkem druhé světové války. Druhá světová válka kromě děsivého množství obětí a ekonomických ztrát představuje také dosud největší nasazení sil a prostředků v dějinách lidstva. Nasazování a koordinace si vyžádaly vytváření nových metodik, které dnes řadíme do systémového inženýrství.

Dále se začínají nasazovat první počítačové systémy, např. německý šifrovací systém Enigma nebo systém řízení palby na Britských válečných lodích. Byly to sice systémy primitivní, avšak předznamenaly nástup moderních počítačových technologií. Schopnost efektivně zpracovávat informace pomocí těchto technologií také dalo této etapě název jako „informační“.

Pokud zemědělská revoluce trvala tisíce let, průmyslová okolo 300 let, u informační etapy se předpokládá trvání v desítkách let. Počítače jsou nasazovány do podniků pro řízení výrobních linek stejně jako pro psaní dopisů sekretářkou. Podniky jsou doslova protkány nervovým systémem vzájemně propojených počítačů, s přístupem k centrálním informačním systému s veškerými informacemi o podniku.

Pokud můžeme chápat počítačovou síť jako nervový systém podniku, potom analogicky můžeme internet považovat za nervovou síť světové ekonomiky.

Vedle těchto dvou extrémů existují sítě zvláštního významu z hlediska fungování státu, které se souhrnně nazývají kritická infrastruktura. Kritické infrastruktuře věnujeme samostatnou část učebních textů. Problematika informačních systémů a jejich vývoj je přímo závislý na vývoji celého průmyslového odvětví informačních technologií. To znamená, že 50 a. 70 léta se nesla ve znamení velkých sálových počítačů a mainframů, výpočetních středisek, které pro celý podnik centrálně zabezpečovaly služby.

Jednotliví uživatelé chodili se svými požadavky za pracovníky na těchto specializovaných odděleních a ti jejich požadavky realizovali. 80. léta s sebou přinesla masivní nasazování kancelářských počítačů propojených do počítačové sítě. Řada úloh do té doby vykonávaných centrálně ve výpočetním středisku se přesunula tak, aby byly řešeny tam, kde vznikly a tak aby přinesly maximální užitek.

Dochází tedy k zániku resp. transformaci výpočetních středisek, které vykonávají podpůrnou činnost, jako je nákup, evidence, instalace a údržba počítačové sítě, centrální správa uživatelů, bezpečnostní audity informačních systémů apod.

Dnes již lze říci, že 90. léta přinesla vším prorůstající Internet. Internet také změnil pohled na využívání informačních systémů a vedl k další decentralizaci. S využitím Internetu je možné se k informačnímu systému připojit více méně odkudkoliv - z notebooku, domácího počítače, tabletu nebo chytrého mobilního telefonu.

S Internetem úzce souvisí další velmi moderní pojem - globalizace. Firmy expandovaly na řadu trhů, kam předtím neměly přístup a byly nuceny změnit způsob svého podnikání a své zaměření vůbec, aby byly schopny přežít v tomto změněném prostředí.

Informační systém je základním předpokladem úspěšného řízení a musel se tedy změnit také, aby podporoval změněné poslání firem. Zatímco ještě na počátku 90. let bylo snahou minimalizovat náklady a to například formou co možná největších unifikovaných sérií produktů, kde podnik dosahoval úspor z rozsahu, dnes se podniky spíše soustředí na osobu zákazníka. Přitom je samozřejmě nutné zachovat co nejnižší náklady a nejvyšší kvalitu, tedy hlediska, která hrála prim na počátku 90. let a dříve.

V poslední době se stáváme také svědky nástupu nového trendu, který označujeme Bring Your Own Device (BYOD) - přines si vlastní zařízení. Označuje situaci, kdy si uživatel nosí do práce své vlastní zařízení (vlastní hardware) a plní s ním běžné pracovní úlohy. To je významný posun proti stavu, který panoval dosud.

Dosud totiž firmy investovaly do vlastního hardware, který pak ale následně měly plně pod kontrolou, což je výhodné z hlediska bezpečnosti o obecně kontroly způsobu jakým je zařízení využíváno. BYOD toto mění. Pro firmy je BYOD výhodné, protože jim odpadá alespoň částečně nutnost investovat do vlastního - firemního hardware. Pro uživatele je situace také výhodná, protože zařízení je jeho a dá se tedy předpokládat, že svou funkčností bude uživateli plně vyhovovat - konečně koupil si ho sám.

Nevýhodou tohoto přístupu je naopak potenciálně nižší úroveň bezpečnosti a určité možné problémy s licencováním software.

**Kontrolní otázky**

1. Definujte pojem systém
2. Rozdělte systémy podle způsobu popisu.
3. Zařaďte jednotlivé typy informačních systémů podle úrovně řízení, na kterých jsou nasazovány.
4. Zhodnoťte z historického hlediska množství informací, které jsou ve společnosti zpracovávány.
5. Zkuste zhodnotit výhody a nevýhody BYOD.

# Kapitola 2

# Typy informačních systémů

**Průvodce studiem** V této kapitole rozdělíme informační systémy podle typů údajů, se kterými pracují.

**Po přečtení této kapitoly budete**
**Znát**

- jednotlivé typy informačních systémů používaných běžně v praxi
- oblasti, které jsou informačními systémy komplexně řešeny

**Umět**

- rozčlenit systémy a informační systémy do několika kategorií

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

## 2.1 Podniková informatika

Pohledy na informační systémy mohou být různé. V této kapitole se podíváme na určitý nereprezentativní výběr různých typů informačních systémů. V dalších podkapitolách se budeme věnovat především těm informačním systémům, které v průběhu doby si vybudovaly své pevné místo v podnikové informatice, a tedy existuje reálná šance, že se s nimi potkáte v praxi.

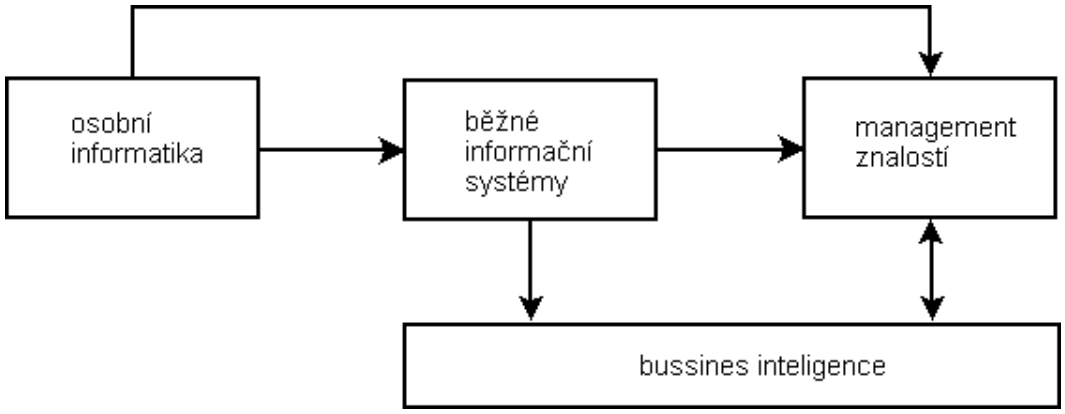
Podnikovou informatiku obecně můžeme rozdělit do několika vrstev. Určitý obrázek si můžete udělat z obr. 2.1.

Osobní informatikou rozumíme využití běžné osobní výpočetní techniky, tedy osobní počítače a běžné kancelářské produkty na nich provozované jako jsou tabulkové procesory, textové procesory apod. S osobní informatikou jste se setkali, nebo mohli setkat v předmětu *Počítačové praktikum* a do této oblasti můžeme zařadit i osobní databáze probírané v předmětu *Počítačové sítě a ochrana dat*.

Běžnými informačními systémy rozumíme především informační systémy, tak jak jsou vysvětleny v kapitolách 2.2 až 2.6.

Management znalostí a bussines inteligence již pracují nad bází dat vytvořenou běžnou prací zaměstnanců podniku v rámci sféry osobní informatiky a běžných informačních systémů. Bussines inteligence je tak určitou nadstavbou která nám umožňuje flexibilně tato data analyzovat, získávat z nich další znalosti použitelné pro efektivní řízení podniku, přijímání rozhodnutí apod.

Hlubší znalosti této problematiky můžete získat v předmětech *Statistika* (znalosti o statistických metodách analýzy dat) a *Bezpečnostní informatika 3* (datamining), viz [46].




Obrázek 2.1: Podniková informatika

## 2.2 Computer Integrated Manufacturing (CIM)

Zkratka CIM znamená v překladu počítačově řízená výrobu. Tento druh podnikového řešení dosáhl největšího rozmachu někdy v polovině osmdesátých let 20. století. Byl budován nad společnou podnikovou databází. Základními stavebními kameny, které zabezpečovaly samotnou funkčnost systému, byly systémy Computer Aided Design (CAD) - počítačem řízený návrh a Computer Aided Manufacture (CAM) - počítačem řízená výroba).

Cílem těchto systémů bylo zkrácení dlouhého produkčního cyklu výrobku na minimum. Výhoda řešení spočívá v tom, že pomocí CAD nástroje byl výrobek navržen a pomocí CAM byl tento elektronický návrh přenesen do výrobní linky.

Vše je prováděno nad jednotným informačním systémem podniku, aby byl neustále přehled, kolik výrobků bylo vyrobeno, pro koho, jaké jsou skladovací kapacity apod.

To, že hlavní rozmach tohoto typu informačních systémů byl v 80. letech, neznamená, že v dnešní době by se takové systémy nevyužívaly – pouze zevšedněly. To, co bylo v 80. letech nové, je dnes nasazováno rutinně.

Velké uplatnění mají tyto systémy především v oblasti zpracování plechu. Na základě požadavků (CAD) na jednotlivé plechové výrobky se linka sama připraví k vyřezání těchto výrobků a navíc provede optimalizaci rozložení výrobků na plechovém plátu z hlediska spotřeby materiálu.

Příklady technologických procesů, které CIM využívají, najdete na obr. 2.2.

## 2.3 Systémy plánování a řízení výroby (MRPII a PPS)

PPS rozumíme systémy pro plánování a řízení produkce. Tato zkratka se vžila zejména v německy mluvících zemích. V anglosaských zemích se hovoří o systémem pro Management and Resource Planning (MRPII), což je takřka doslovný překlad PPS.

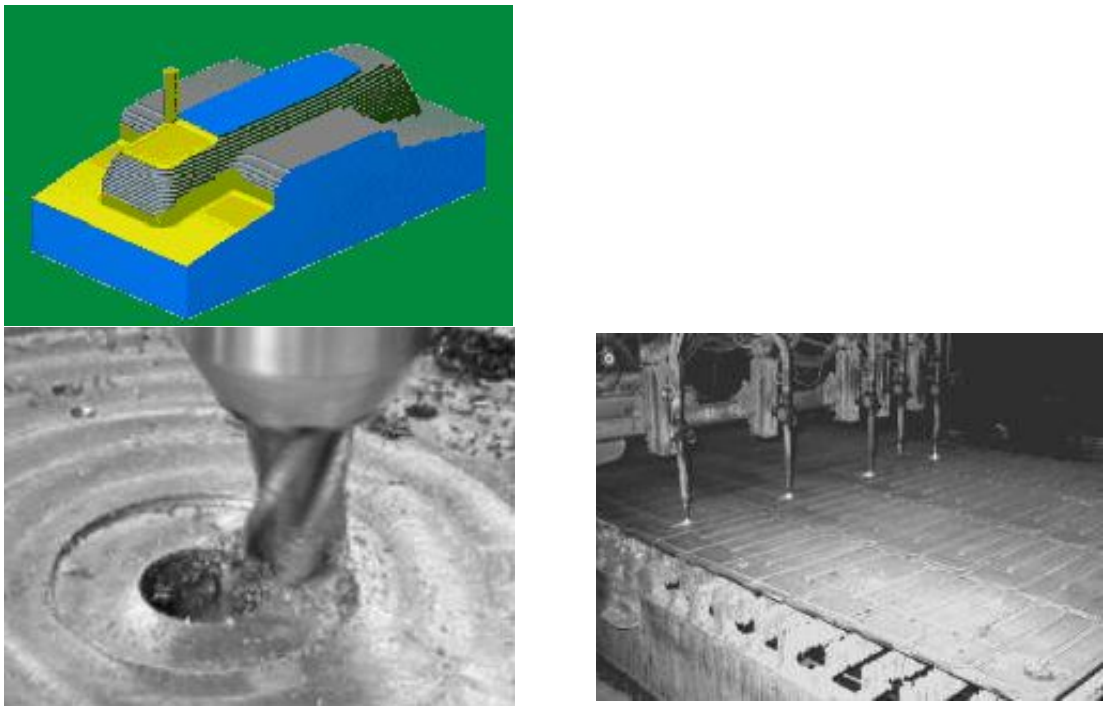
Oba pojmy přitom představují velmi podobné pojetí práce s informacemi. Tyto systémy jsou zaměřeny především na výrobní proces z hlediska jeho plánování a řízení, zatímco CIM je zaměřeno přímo na výrobu konkrétního výrobku. Rozdíl mezi PPS a CIM je jasně patrný z obrázku 2.3.

## 2.4 Enterprise Resource Planning (ERP)

ERP (Plánování zdrojů podniku) je obvykle chápáno dvojím způsobem:

1. v užším slova smyslu se používá pro označení integrace vnitropodnikových procesů (výroba, logistika, lidské zdroje, finance, ...)
2. v širším slova smyslu zde dále můžeme zahrnout další systémy jako CRM, B2B řešení, Supply chain management (řízení odběratelsko-dodavatelských řetězců) (SCM), apod.

Úkolem ERP systémů je zejména pomoci s plánováním, a to jak krátkodobým, tak střednědobým a s řízením realizace zakázek z hlediska dodržení termínů a nákladů nutných pro její realizaci. Jinými slovy pomáhá zajistit logistiku a finance.



Obrázek 2.2: Navržení produktu a jeho výroba

Na informační systémy této kategorie lze pohlížet dvojím způsobem: buď podle úrovně, ve které jsou nasazeny, nebo podle činností, které vykonávají. Na obrázku 2.4 jsou jasně patrné rozdíly. Zatímco levá část vychází z klasického pojetí řízení, pravá část obrázku reprezentuje moderní styl řízení a jeho podporu podnikovými informačními systémy.

ERP řešení tak může být tvořeno systémem od jediného výrobce jako je například SAP. Při pořizování se pak volí moduly, které mají být v rámci řešení ERP implementovány. Při nasazování se pak řeší především problém migrace na nový systém.

Alternativou může být nasazení samostatných sub-systémů ERP (CRM, SCM, apod.) od různých výrobců. Důvodem může být výrazně nižší cena než v případě nasazení komplexního řešení, je zde ale také větší množství problémů, které je nutné pro efektivní nasazení překonat. Kromě migrace dat z původních (legacy) systémů je totiž nutné řešit vzájemnou komunikaci systémů, aby bylo možné dosáhnout synergentních účinků plynoucích z analýzy dat vedených jednotlivými systémy.

Jednotlivé bloky ERP totiž kromě toho, že vytvářejí vlastní, nezávislé datové základny, mohou dokonce preferovat různé databázové systémy, na kterých běží. Agregace dat z těchto různých zdrojů tak může být velmi problematická.

## 2.5 Customer Relationship Management (CRM)

Řízení vztahu se zákazníky umožňuje s vynaložením co možná nejmenších nákladů oslovit s nabídkou co možná největší počet potenciálních zákazníků, o kterých existují záznamy z předchozí spolupráce s firmou. Podle těchto informací se určí, že by mohli mít o výrobek popř. službu zájem.

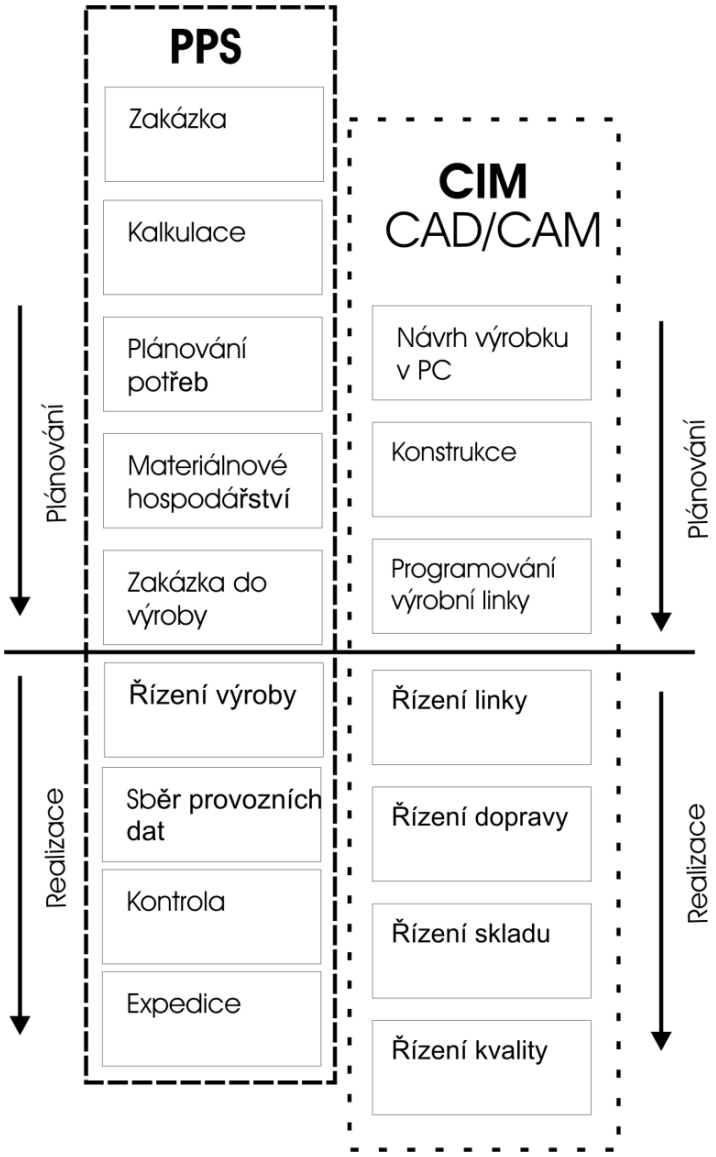
Dlouhodobé sledování a vyhodnocování chování zákazníka umožňuje podniku, aby vytipoval cílové skupiny zákazníků a pro ně přizpůsobil nabídku svých produktů.

Analýzou cílových skupin lze také upřesnit směrování podniku tedy, kteří zákazníci jsou pro podnik perspektivní, a je tedy efektivní přizpůsobit jim svou nabídku, a kteří perspektivní nejsou. Některé průzkumy veřejného mínění udávají, že až 70% zákazníků, kteří opustí dodavatele, tak učiní kvůli špatným službám nebo špatné podpoře. CRM přímo podporuje zkvalitnění komunikace mezi podnikem a zákazníkem, takže se snaží toto číslo snížit.

Na obrázku 10 je zobrazeno základní uživatelské rozhraní open source řešení pro CRM SugarCRM.

Podívejme se tedy na funkce, které CRM obvykle obsahuje:

- správu kontaktů a informací o zakázkách pro obchodní zástupce




Obrázek 2.3: Srovnání CIM a PPS koncepce informačních systémů

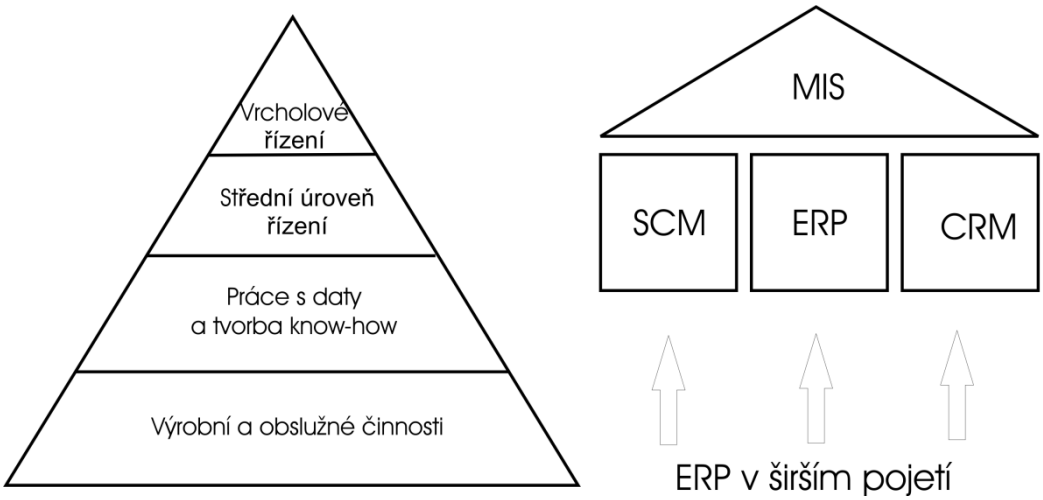
- analýza stávajících prodejních dat
- synchronizace kontaktů, emailů, událostech v kalendáři mezi CRM a MS Outlook/MS Exchange
- nástroje pro návrh marketingových kampaní a nástroje pro vyhodnocení její úspěšnosti
- podpora zákazníků ve smyslu zaznamenání reklamací, jejich příčin, frekvence výskytu, způsobu vyřízení

CRM systémy mohou obsahovat i další funkce, které je mohou napojovat na systémy řízení projektů (ve smyslu termínů, úkolování apod.), popřípadě další funkce, které se liší podle zvoleného řešení.

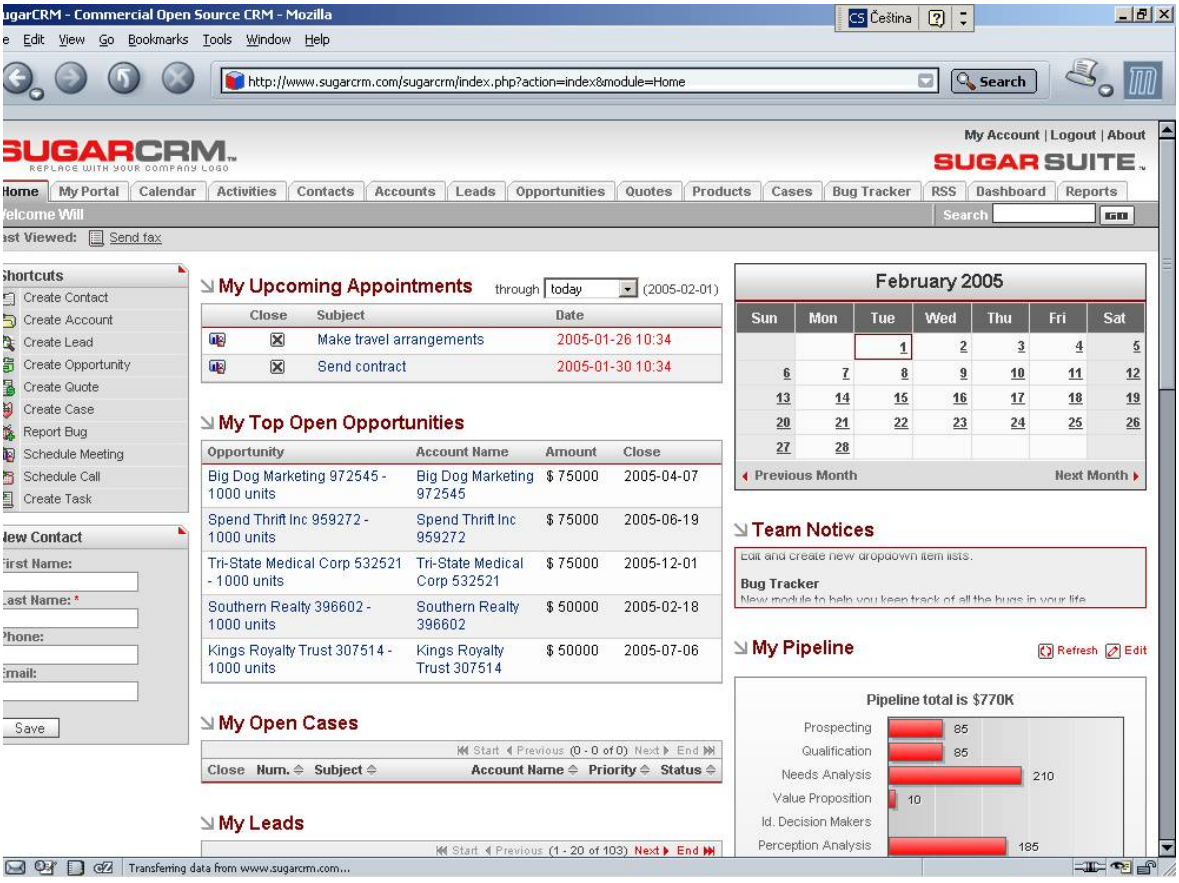
## 2.6 Supply Chain Managment (SCM)

Suply Chain Management (řízení dodavatelského řetězce) umožňuje řídit dodávky nutné pro provoz podniku a optimalizovat tím náklady tak, aby bylo možné zkrátit čas dodávek na minimum, zabezpečit kvalitu dodávaných surovin pro výrobu apod.

Masivní nasazování managerských technik řízení výroby jako jsou dodávky Just in Time (JIT), tedy dodávky, které pokud možno co nejkratší dobu zůstanou na skladě nebo jdou přímo do výrobního procesu, vyžaduje i změnu v používání informačních systémů. Nemít výrobky na skladě má očividně své výhody, na druhou stranu v souvislosti s nasazováním těchto technik je nutné čelit novým výzvám




Obrázek 2.4: Pyramida řízení vs rozšířený ERP model




Obrázek 2.5: Open source CRM řešení SugarCRM [7]

– například v oblasti kontroly kvality, logistiky dodávek a podobně.

Většina organizací, pro které se vyplatí uvažovat o těchto technikách řízení odběratelsko-dodavatelských řetězců, má implementován nějaký systém řízení jakosti, v podmínkách České Republiky je to obvykle systém řízení jakosti dle ISO 9000. Společným rysem prakticky všech systémů řízení jakosti je, že vyžadují přísnou kontrolu jakosti vstupů jako základního předpokladu pro udržení kvality výrobního procesu.

Tedy ideálně by se vzorek z každé dodávky měl testovat z hlediska určitých vlastností nutných pro zachování kvality výroby. To však vyžaduje čas, peníze, a pokud má organizace zaveden systém JIT tak

na skladě ani nemusí mít vstupy, které by mohl testovat. Tento problém se řeší často zaváděním jednotných systémů řízení jakosti v rámci celého odběratelsko-dodavatelského řetězce. V takovém případě pak výstupní kontrola jakosti dodavatele může být přejata jako vstupní kontrola jakosti odběratele.

Takové přejímání kontrol je pak čistě byrokratickým aktem, který je možno vhodně automatizovat pomocí informačních systémů typu SCM. Dalším problémem jsou samotné dodávky. Vzhledem k tomu, že dodávka jde ideálně přímo do výroby, není možné použít klasické postupy pro objednávání a dodávání – dodavatel musí předvídat potřeby svých odběratelů v rámci řetězce, tak aby vhodně naplánoval své výrobní kapacity. Toto není možné zajistit na základě veřejně dostupných údajů – musí dojít do určité k integraci informačních systému odběratele a dodavatele tak, aby dodavatel získával vhodné signály o potřebách svého odběratele a získal přístup k jeho projekcím vývoje trhu, ve kterém působí.

SCM může působit i přímo v logistice dodávek. Začíná se stále více prosazovat použití Radio Frequency Identification (identifikace na rádiové frekvenci) (RFID) čipů, které je možno použít spolu se snímači, aby se automaticky zaregistrovalo dodané zboží do skladové evidence minimem nutné manuální práce.

Obecně se o SCM dá říci to, že se vyplatí především pro velké výrobní organizace s implementovaným systémem řízení jakosti. U těchto společností se také předpokládá, že i jejich informační systémy budou řešeny komplexně – tedy budou konstruovány tak, aby data v nich uchovaná mohly být jednoduše využity dalšími informačními systémy. Jednotlivé informační systémy jsou proto obvykle dodávány jediným dodavatelem jako moduly jím dodávaného systému například SAP, komplexní řešení dodávají také firmy IBM, Oracle a řada dalších.

## 2.7 Řešení Business to Business (B2B) a Business to Customer (B2C)

B2B je řešení, které se snaží usnadnit navázání a udržování obchodních vztahů. Toto usnadnění spočívá v masivním nasazování Internetových technologií a veřejná přístupnost tohoto procesu prostřednictvím Internetových tržišť.

Předpokladem úspěšnosti takových řešení je tedy existence nezávislého provozovatele tržiště, který je dostatečně známý a také důvěryhodný pro případné účastníky tržiště. Požadavek na známost je dán tím, že úspěšnost tržiště je odvozená od počtu aktivních účastníků – tedy určitá jistota, že pokud na tržišti vypíši poptávku, na tuto poptávku zareaguje dostatečné množství potenciálních dodavatelů.

V rámci B2B pak mohou jednotliví dodavatelé o tento kontrakt soutěžit a předhánět se výhodností svých nabídek, což je velkým přínosem, kdo službu nebo výrobky poptává.

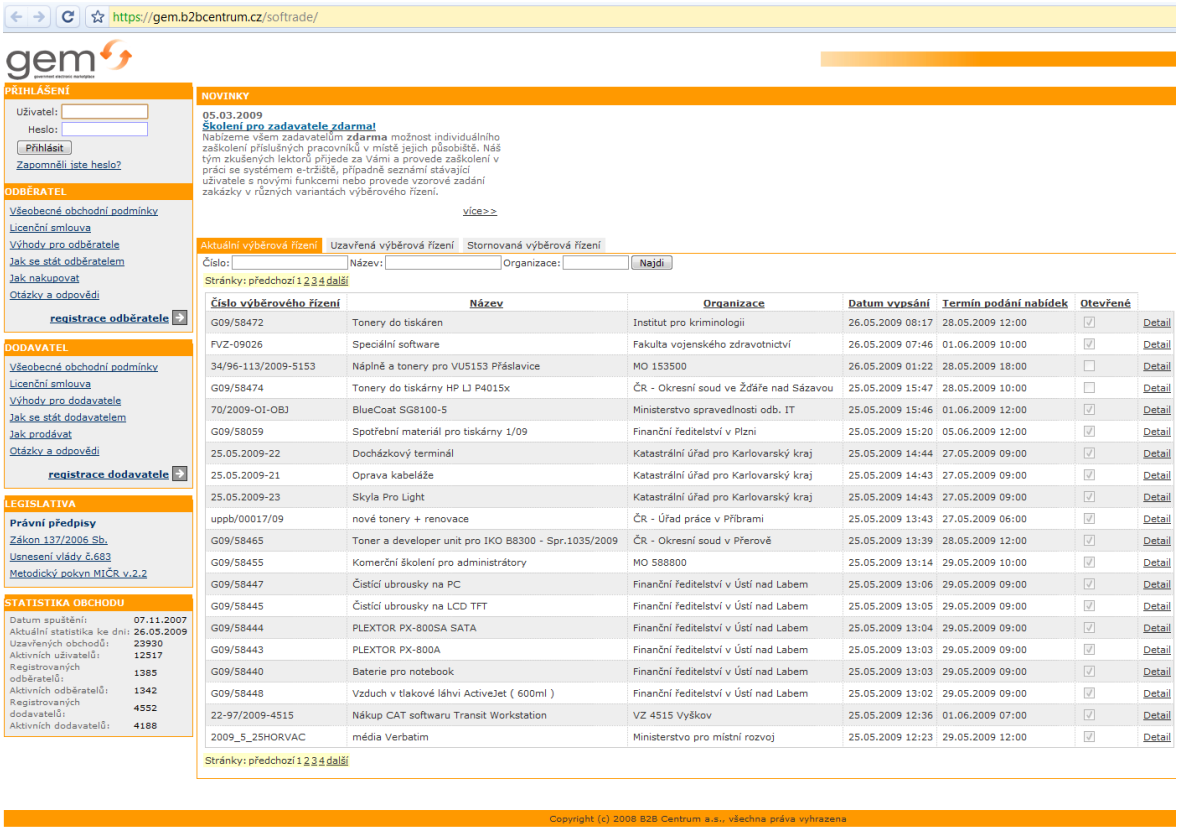
B2B řešení jsou určena především pro jednorázové kontrakty. Při opakování je často výhodnější uzavření kontraktu s jedním dodavatelem a využít tak určitých synergických účinků pravidelnosti odběru (např. lepší ceny apod.).

Další výhodou je možnost využití určité automatizace celého procesu. Tato tržiště totiž často podporují elektronickou výměnu údajů mezi informačními systémy. V oblasti B2B je často využíván standard UN/EDIFACT, který byl normalizován jako ISO 9735 ( [25]).

To, jak takové tržiště B2B vypadá, můžete vidět na obr. 2.6.

V případě Busimes to Customer (B2C) se už jedná o klasický elektronický obchod pro koncového zákazníka. Oproti řešením B2B neobsahuje obvykle nástroje pro výměnu dat mezi IS – protože tato výměna v tomto případě postrádá smysl.

Na druhou stranu může být efektivní k elektronickému obchodu připojit další užitečné služby, jako jsou například recenze uživatelů, hodnocení spokojenosti s produktem, diskuzní fóra apod.




Obrázek 2.6: Tržiště B2B [5]

### Kontrolní otázky

1. Jaké okolnosti vedly k vývoji a nasazování systému CIM?
2. Proč je výhodné pro řešení zásobování firem použít systémy SCM?
3. Vysvětlete dva proudy v chápání ERP systémů.
4. Zamyslete se nad zařazením jednotlivých typů informačních systémů do pyramidy řízení z předchozí kapitoly.

# Kapitola 3

# Informační systémy a krizové řízení

**Průvodce studiem**
Informační systémy a havarijní plánování a krizové řízení jsou do značné míry propojené. Styčným bodem jsou informace, resp. nakládání s nimi. Podnik je potřebuje pro svou každodenní činnost, v rámci havarijního plánování jsou informace nutné pro vytváření havarijních plánů a také pro řešení krizí. Informace jsou potom v rámci podniku primárně shromažďovány v nejrůznějších informačních systémech.

**Po přečtení této kapitoly budete**
**Znát**

- jak souvisí informační systémy a práce s nimi s havarijním plánováním a krizovým řízením
- pojem kritická infrastruktura

**Umět**

- rozčlenit systémy a informační systémy do několika kategorií

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

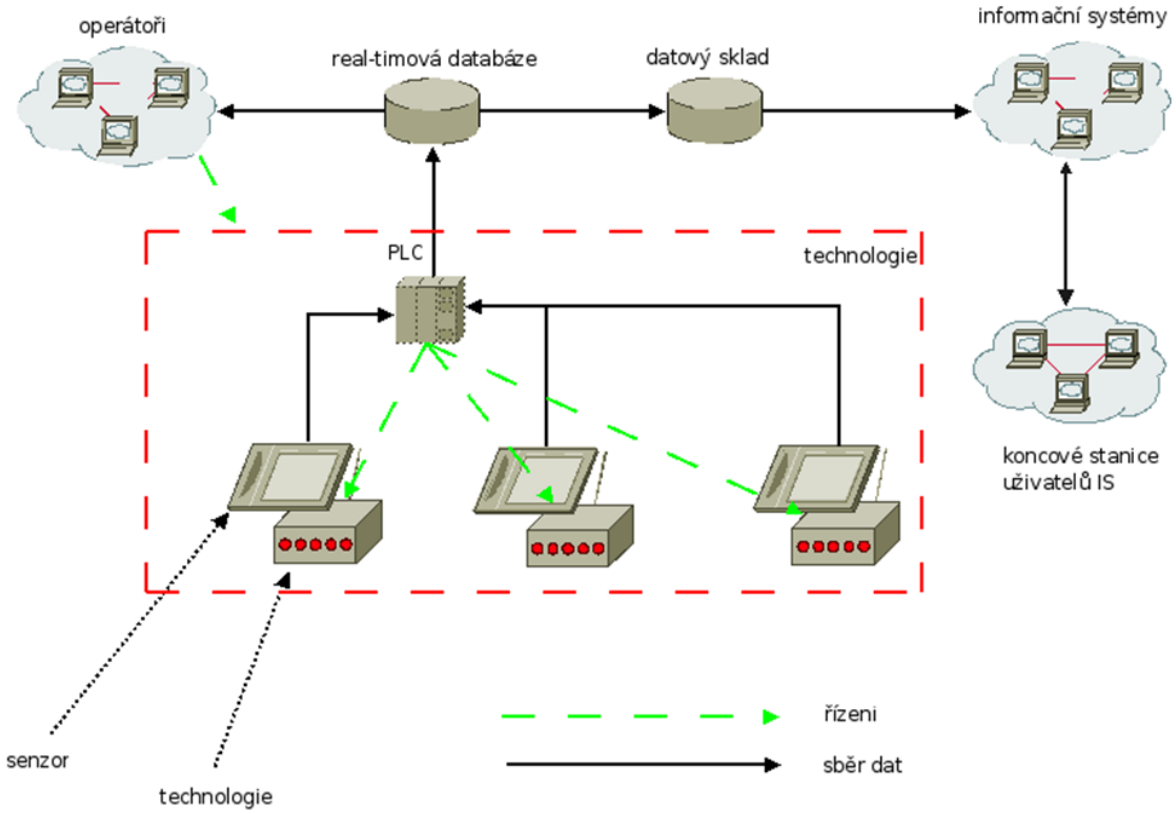
## 3.1 Rozdělení informačních systémů a krizové řízení

Po přečtení prakticky celé kapitoly dva, Vás možná napadá, proč vůbec informační systémy byly v tomto textu, který je primárně zaměřen na obor havarijní plánování a krizové řízení, vymezeny tak, jak byly – tedy spíše z ekonomického hlediska. Odpověď je nasnadě: protože o peníze jde vždy až v první řadě.

Tedy pokud informační systémy podniku (výčet IS v předchozích podkapitolách nebyl v žádném případě vyčerpávající) tvoří mozek podniku, pak jakákoliv havárie se v těchto systémech projeví.

Existuje celé odvětví podnikové informatiky, které se touto oblastí zabývá, říkáme jí průmyslová automatizace. Do této oblasti řadíme veškeré automatizované průmyslové řídící a monitorovací systémy. Primární oblastí použití je samozřejmě řízení výrobního procesu a pro tento účel jsou informace získávané průmyslovými senzory a informace předávané řídícími systémy, obvykle vizualizovány do pro člověka přehlednější podoby. Nástroje, které k tomuto účelu používáme, se nazývají Supervisory Control and Data Acquisition - Dispečerské řízení a sběr dat (SCADA) systémy.

Zapojení průmyslové automatizace do podnikové informatiky je znázorněno na obr. 3.1.




Obrázek 3.1: Architektura průmyslové automatizace

Vždy lze vysledovat nějaké indikátory havárie, které napoví, o jaký druh havárie se jedná, v jakém je rozsahu, kde se udál apod. Tyto indikátory spolu se základní metodikou hodnocení by měly být současně východiskem pro sestavení a nakonec i použití havarijního plánu. Podrobnosti o průmyslové automatizaci můžete získat v předmětu Bezpečnostní informatika III [46].

Z jiného pohledu jsou data obsažená ve výše uvedených informačních systémech i systémech ostatních to nejdůležitější, co podnik vlastní. Zatímco budovy, výrobní linky apod. jsou obvykle pojištěny proti škodám, ztráta dat o zákaznících již takto pojištěna není, je tedy nutné v případě nebezpečí tato data nějakým způsobem ochránit – z tohoto pohledu jsou tedy informační systémy také předmětem zájmu havarijních plánů.

Problematikou ochrany dat se budeme zabývat ještě v kapitole věnované bezpečnostní politice, podrobněji se jí však budeme věnovat v předmětu Počítačové sítě a ochrana dat (dříve Počítače a ochrana dat).

A konečně existují specializované informační systémy pro vytváření a správu havarijních a krizových plánů. Jedním z výrobců takových produktů byla např. firma Medium Soft a.s., která v oblasti krizového řízení vstoupila informačním systémem nazvaným Krizové plány. V současné době Medium Soft již dodává nástupce tohoto systému nazvaného C3M [38].

V České Republice je hlavním konkurentem Medium Softu v této oblasti firma T-Soft se svým produktem Emergency Office [41].

## 3.2 Kritická infrastruktura

Pro účely tohoto textu budeme krizové řízení chápat jednoduše jako řízení lidských, finančních a technických zdrojů pro zvládnutí nepříznivých mimořádných situací (krizí).

V roce 1998 byla v USA na příkaz administrativy tehdejšího prezidenta Clintona zřízena komise, která hodnotila systémy národního významu, tzn. systémy, jejichž vyřazení (byť třeba krátkodobého charakteru) by vedlo k velkým ztrátám na životech nebo by vedly k velkým výpadkům v oblasti hospodářství. Pro takovéto systémy zavádí pojem kritická infrastruktura.

Zde zmíněná komise v USA do této kritické infrastruktury zařadila:
- systémy dodávky elektřiny
- systémy dodávky vody
- kanalizační systém
- přepravní síť
- komunikační a energetické systémy
- bankovní a finanční sektor
- další sektory závislé na počítačových systémech

Informační technologie jsou přímo předmětem dvou položek kritické infrastruktury (zvýrazněny tučně) a v ostatních kritických systémech hrají významnou integrující roli. Souhrnně bychom je mohli nazvat komunikační a informační systémy.

Nutnost zabývat se kritickou infrastrukturou začala být v celosvětovém měřítku patrná zejména po událostech 11. září 2001. Intenzita zkoumání se zvyšuje i v USA, kde vzniká ministerstvo Vnitřní bezpečnosti, které všechny tyto snahy zastřešuje.

Podle této koncepce (viz [33–35]) je terorizmus prakticky jediný zdroj ohrožení kritické infrastruktury, jelikož přírodní katastrofy typu zemětřesení, záplav, tsunami[1], hurikánů, tornád apod. mají vždy pouze lokální charakter a jelikož se vyskytují přibližně na stejných místech, jsou místní orgány „zvyklé“ a dobře připravené tyto události řešit.

Mění se také kategorizace sektorů kritické infrastruktury:
- zemědělství a potraviny
- voda
- veřejné zdraví
- záchranné služby
- základna obranného průmyslu
- telekomunikace
- energie
- přeprava
- bankovnictví a finance
- chemické a nebezpečné látky
- pošta a přeprava nákladu

Kromě sektorů kritické infrastruktury zavádí tento nový přístup ještě pojem budovy zvláštního významu (key assets), kam jsou zařazovány především:
- národní památníky a kulturní památky
- jaderné elektrárny
- přehrady
- vládní úřady
- komerční klíčové prvky

Jak si zajisté všimněte, tak se sektorů kritické infrastruktury v této nové kategorizaci vypadly informační technologie jako samostatný sektor. Není tomu tak proto, že by tyto systémy byly považovány jako bezvýznamné, ale naopak proto, že jsou extremně významné a jsou nedílnou součástí všech sektorů kritické infrastruktury, takže je potřeba je chránit komplexně napříč jednotlivými sektory. Strategie pro ochranu přinesla několik zajímavých opatření ke zvýšení bezpečnosti. Kromě nezbytných změn v legislativě mající za cíl plynulejší výměnu informací napříč státní správou a samosprávou je zde in tzv. *Homeland Security Advisory System* (viz. obr. 3.2) mající za cíl informovat vlastníky kritické infrastruktury o stupni ohrožení teroristickým útokem.

Tento systém pak byl součástí všech webových stránek orgánů státní správy (viz. obr. 3.3) - a tedy „na očích“ široké veřejnosti.

Účelem Homelan Security Advisory systému bylo umožnit vlastníkům prvků kritické infrastruktury vytvářet odstupňované plány, které by mohly být aktivovány v souvislosti s vyhlášeným stupněm nebezpečí. Optimalizovány by tak byly náklady vynakládané na ochranu jednotlivých prvků KI.

Dlouholetá praxe však ukázala, že změny ve stupních ohrožení se prakticky nedějí – zůstávají na úrovni high, výjimečně elevated. V důsledku toho byl tento systém zrušen a nahrazen systémem novým National Terrorist Advisory System (NTAS) [32].

Tento systém je podstatně podrobnější. Je zaměřený pouze na hrozby spojené s terorizmem a sleduje tyto hrozby po jednotlivých zájmových sektorech . V době psaní těchto skript (červen 2012),

[1] v češtině by se správně mělo psát *cunami*, což odpovídá české transkripci japonské abecedy katakana, v praxi se ale spíše používá anglická transkripce tsunami - a proto byl tento zápis zvolen i v těchto skriptech


Obrázek 3.2: Homeland Security Advisory System

NTAS neobsahoval žádná varování.

Kromě toho je zde patrná snaha vytvářet sektorové, nezávislé instituce, mající za úkol zajistit sdílení bezpečnostně orientovaných informací napříč tímto sektorem. Obecně jsou tato centra nazývaná ISAC. Pro oblast informačních technologií zajišťuje tuto funkci CERT [20], což je zkratka pro Computer Emergency Response Team.

V české republice stanovila Bezpečnostní rada státu následující základní oblasti kritické infrastruktury.

1. Energetika
   (a) Elektřina
   (b) Plyn
   (c) Tepelná energie
   (d) Ropa a ropné produkty
2. Vodní hospodářství
   (a) Zásobování vodou
   (b) Zabezpečení a správa vod
   (c) Systémy odpadních vod
3. Potravinářství a zemědělství
   (a) Produkce potravin
   (b) Péče o potraviny
   (c) Zemědělská výroba
4. Zdravotní péče
   (a) Přednemocniční neodkladná péče
   (b) Nemocniční péče
   (c) Ochrana veřejného zdraví
   (d) Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5. Doprava
   (a) Silniční
   (b) Železniční
   (c) Letecká
   (d) Vnitrostátní vodní
6. Veřejná správa
   (a) Státní správa a samospráva
   (b) Sociální ochrana a zaměstnanost
   (c) Výkon justice a vězeňství
7. Nouzové služby
   (a) Hasičský záchranný sbor a jednotky PO
   (b) Policie České republiky
   (c) Armáda České Republiky


Obrázek 3.3: Web department of Homeland Security

   (d) Monitorovací služby radiační, chemické a biologické ochrany
   (e) Předpovědi, varování, hlásná služba
8. Bankovnictví a finanční sektor
   (a) Správa veřejných financí
   (b) Bankovnictví
   (c) Pojišťovnictví
   (d) Kapitálový trh
9. Komunikační a informační systémy
   (a) Služby pevných sítí
   (b) Služby mobilních sítí
   (c) Rádiová komunikace a navigace
   (d) Satelitní komunikace
   (e) Rádiové a televizní vysílání
   (f) Poštovní a kurýrní služby
   (g) Přístup k internetu a datovým službám

Kritéria k rozhodnutí o tom, které prvky přináležejí do kritické infrastruktury, jsou definovány v nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury [28]. Oproti sektorům kritické infrastruktury USA zde máme celý sektor komunikačních a informačních systémů. Je otázka, zda je takovéto vyčlenění úplně vhodné – může totiž evokovat, že pokud organizace nepodniká přímo v oblasti komunikačních a informačních systémů, pak zabezpečení informační bezpečnosti kyberprostoru sektoru kritické infrastruktury, kterou vlastní se jí vlastně netýká, což ovšem není pravda.

Ve srovnání aktivit ČR popř. EU s USA, jsou USA o několik řádů aktivnější, což je důvod, proč jsem se řešení kritické infrastruktury v USA věnoval více. Poměrně komplexně je problematika kritické infrastruktury řešena také SRN.

## 3.3 CERT a CSITR týmy a jejich význam

Jak je tedy řešena bezpečnost IT na celostátní úrovni? Stát na této úrovni má spíše roli koordinační. Umožňuje výměnu a sdílení informací mezi soukromým a veřejným sektorem. Rolí státu naopak není nařizovat konkrétní obranná opatření a kontrolovat jejich realizaci (až na výjimky). Za tímto účelem zřizují jednotlivé státy tzv. CERT/CSIRT národní týmy.

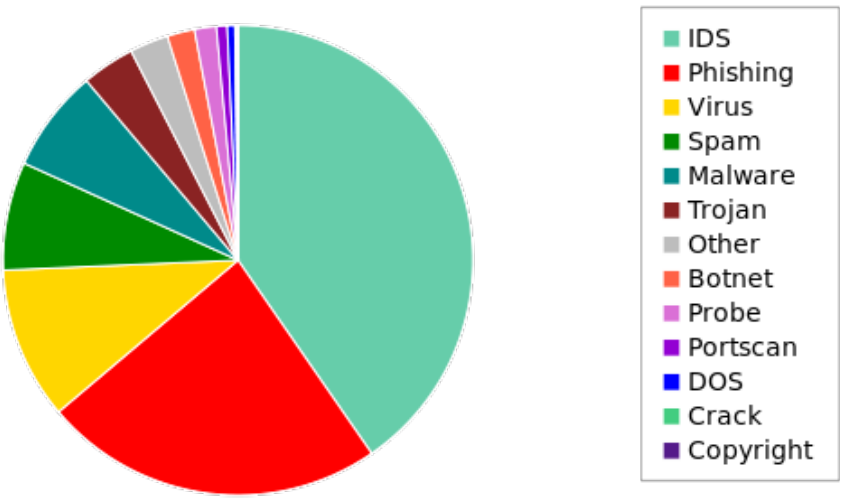
V České Republice roli národního CSIRT týmů zastává CSIRT.CZ provozovaný sdružením CZ.NIC od 1. ledna 2011. Obdobný národní tým v USA US-CERT vznikl už v roce 2008 (už od 80. let 20. století ale fungoval CERT při Carnegie Mellon Universitě). V Polsku CERT.GOV.PL vznikl v roce 2008, na Slovensku CSIRT.SK byl zřízen nařízením vlády 479/2009 Sb. [9].

Role jednotlivých CSIRT týmů může být odlišná, například CSIRT.CZ popisuje [2] svoji roli následovně:

- Udržování zahraničních vztahů - se světovou komunitou CSIRT týmů a organizacemi, které tuto komunitu podporují.
- Spolupráce se subjekty v rámci ČR - Internet Service Provider (ISP), poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi.
- Poskytování služeb v oblasti bezpečnosti:
  - Řešení a koordinace řešení bezpečnostních incidentů
  - Osvětová a školící činnost
  - Proaktivní služby v oblasti bezpečnosti

US-CERT definuje [43] své poslání jinak: Posláním US-CERT je zlepšit národní postavení v oblasti kyber bezpečnosti, koordinovat sdílení informací a proaktivní řízení kyber rizik ohrožující USA při ochraně ústavních práv Američanů. Vizí US-CERT je stát se důvěryhodným globálním vůdcem v oblasti kyber bezpečnosti – spolupracující, agilní a pružný v komplexním prostředí.

CSIRT týmy menších států pochopitelně nemohou aspirovat na vedoucí úlohu v oblasti IT bezpečnosti, ale řada činností by se měla překrývat. Činnost jednotlivých týmů lze zkoumat pomocí statistik a analýzou činnosti na domácích stránkách týmů. Rozložení řešených bezpečnostních incidentů týmu CSIRT.CZ je znázorněn na obr. 3.4.




Obrázek 3.4: Typové rozložení řešení bezpečnostních incidentů týmu CSIRT.CZ v letech 2008-2011 (převzato z [30])

Většinu bezpečnostních incidentů připadá na detekované průniky do sítí následované phishingovými útoky a napadení různými typy malware. CSIRT tým pracuje tak, že upozorní správce zdrojové

sítě útoku a pomůže (informační podpora) případně s identifikací problému. Na WWW stránkách CSIRT.CZ je následující přehled činností [31]: 4 tiskové zprávy, organizace 1 workshopu, 2 účasti na mezinárodním cvičení (Cyber EUROPE, Cyber Atlantic 2), 1 doporučení, aktivní účast na bezpečnostně orientovaných konferencích, připomínkování věcného záměru zákona o kybernetické bezpečnosti.

CERT.GOV.PL [**?**] kromě standardní minimální úrovně služeb (jak je realizována např. týmem CSIRT.CZ), poskytuje ještě aktuální informace, doporučené nástroje, doporučení na konfigurace systémů a také zpracovávání bezpečnostních incidentů ARAKIS-GOV [29]. CSIRT.SK jako slovenský národní CSIRT tým byl akreditován teprve v polovině roku 2011, přesto poskytuje oznámení a varování, základní návody a doporučení pro konfiguraci a zabezpečení IT aktiv. Jako etalon toho, jaký typ informací může poskytovat CERT, lze použít US-CERT [44]. Tento národní tým poskytuje údaje o hrozbách a zranitelnostech, aktualizacích, ale také aktivitách a dalších zdrojích a to v úpravě pro techniky (IT odborníky), netechniky (domácí a podnikové uživatele), státní správu a samostatně řeší také bezpečnost řídicích systémů.

Bez ohledu na to, jaké přesně úkoly CSIRT tým dostává od svého zřizovatele, existují některé úkoly, které mají všechny týmy a to především sloužit jako místo pro reportování bezpečnostních incidentů a být nápomocni při jejich řešení. K tomuto účelu je ale vyžadováno, aby jednotlivé CSIRT byly certifikovány, tedy aby někdo ručil za to, že CSIRT tým je skutečně určen pro řešení takových problémů, a zájemce o využití služeb tak získal určitou jistotu, že důvěrné informace o bezpečnostním incidentu nepadnou do nepovolaných rukou.

Pro tyto účely se uznávané CSIRT týmy sdružují do různých mezinárodních uskupení. Na úrovni EU funguje European Network and Information Security Agency (ENISA) [3]. ENISA jako instituce je poradním orgánem Evropské komise v oblasti IT bezpečnosti, zabývá se také organizací konferencí, seminářů, školení a cvičení pro národní CSIRT týmy.

CSIRT týmy samotné se v Evropě sdružují do organizace The Trans European Research and Education Networking (TERENA) [8] jako platformy zprostředkovávající výměnu bezpečnostně orientovaných informací, školení apod. mezi CSIRT týmy.

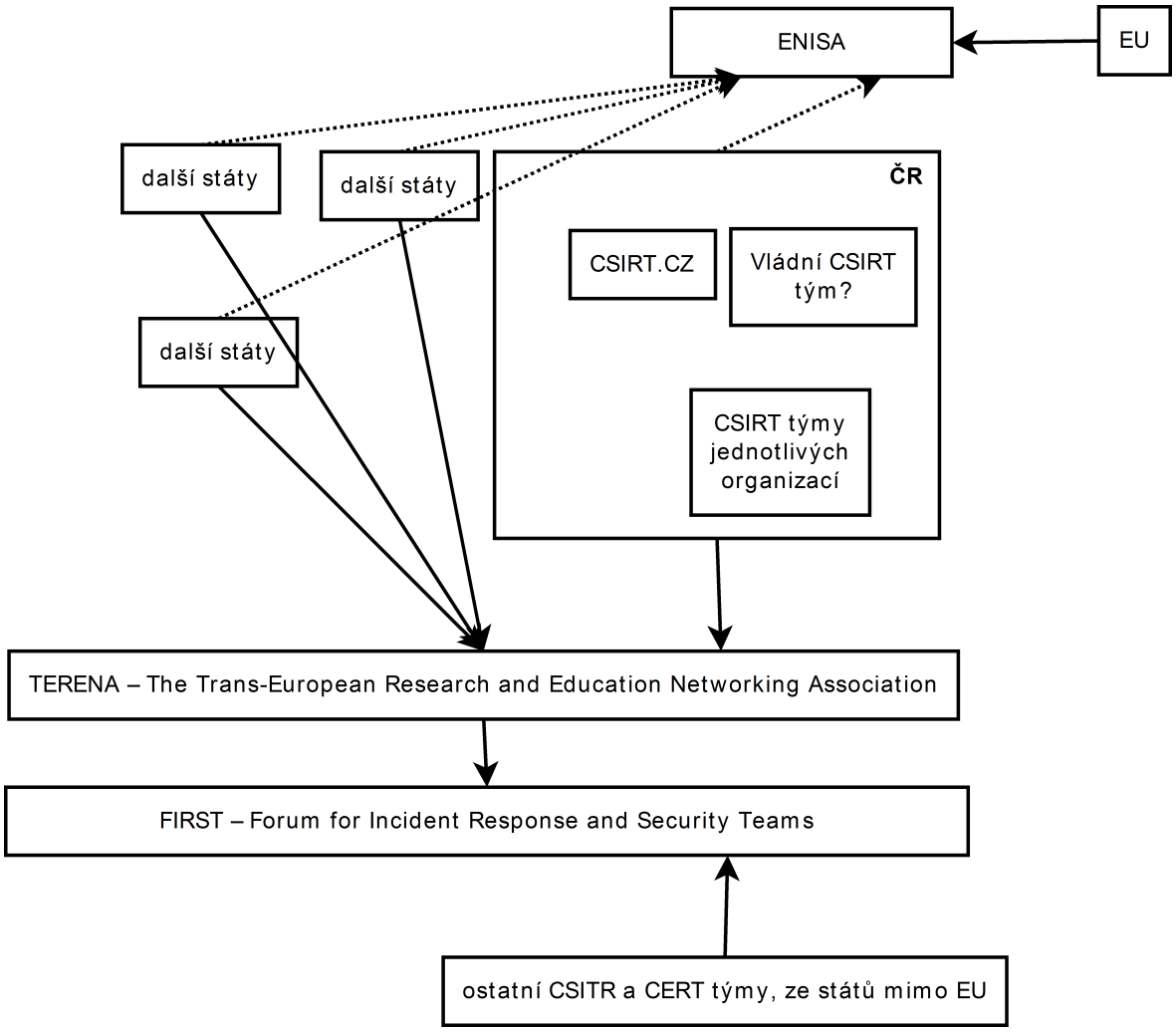
Samotná registrace je realizována pomocí mezinárodní organizace Forum for Incident Response and Security Teams (FIRST) [4]. Pro registraci je nutné, aby se za uchazeče o registraci zaručil nějaký již uznávaný člen fóra. Tímto způsobem se zajišťuje jeden z pilířů spolupráce – dobrá komunikace na mezinárodní úrovni. CSIRT tým tedy musí nejprve navázat „neformální“ spolupráci s jinými CSIRT týmy a teprve poté se může ucházet o registraci v rámci FIRST.

Schematicky si můžeme spolupráci na mezinárodní úrovni představit podobně jako na obr. 3.5.

Na závěr této problematiky zbývá již jen formálně definovat rozdíl mezi národním a vládním CSIRT týmem. Byť je technicky možné, aby úkoly národního a vládního týmu zabezpečoval jediný tým (takto realizováno např. v USA) je obvyklé, že úlohy jsou realizovány samostatnými týmy.

Ne nepodstatnou výhodou je také podstatně lepší kontrola nad prací s informacemi ve státní správě a samosprávě a lepší provázání procesů z hlediska bezpečnosti. Vládní CSIRT tým může např. vytvářet různé metodiky nebo standardy, které budou pro státní správu popř. samosprávu závazné.

Česká republika v současnosti nemá vládní CSIRT tým, ačkoliv se již poměrně dlouho diskutuje o potřebě jeho zřízení.




Obrázek 3.5: CSIRT týmy – mezinárodní spolupráce

**Národní vs vládní CSIRT tým**

Národní CSIRT tým slouží pro řešení bezpečnostních incidentů na národní úrovni. Jeho uživateli tak mohou být soukromníci, firmy, ale také slouží jako kontaktní místo pro zahraniční CSIRT týmy, které řeší bezpečnostní incidenty s přesahem do ČR.

Funkce vládního týmu je ale definována mnohem úžeji. Slouží pro řešení bezpečnostních incidentů ve státní správě popř. samosprávě. Vládní CSIRT tým je obvykle provozován státem a jako takový má ve veřejném sektoru mnohem větší pravomoci než národní CSIRT tým vůči sektoru privátnímu.

**Kontrolní otázky**

1. Pokuste se zařadit problematiku bezpečnosti informačních systémů do svého studijního oboru (havarijní plánování, bezpečnostní inženýrství apod.)
2. Pokuste se vyjmenovat prvky kritické infrastruktury.
3. Zamyslete se nad tím, zda byste do kritické infrastruktury nedokázali zařadit nějaký další prvek.
4. Co je CSIRT tým a co je jeho úkolem?
5. Jaký je rozdíl mezi národním a vládním CSIRT týmem?

# Kapitola 4

# Bezpečnostní politika

**Průvodce studiem**
Základním nástrojem pro vymezení cílů bezpečnosti, povinností jednotlivých uživatelů (různých profesí) je bezpečnostní politika. V této kapitole se pokusíme tento pojem definovat.

**Po přečtení této kapitoly budete**
**Znát**

- co znamená pojem bezpečnostní politika informačního systému
- kdo by se měl na vývoji bezpečnostní politiky podílet

**Umět**

- rozčlenit bezpečnostní politiky podle jejich restriktivnosti

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 20 minut.

Bezpečnostní hledisko práce IS by mělo být ošetřeno v bezpečnostní politice podniku, kterou zpracovává osoba bezpečnostního pracovníka informačních systémů. Východiskům konstrukce tohoto dokumentu vzhledem k celkovému zaměření se budeme věnovat dále v této kapitole.

Základními dokumenty, ze kterých bezpečnostní pracovník při tvorbě politiky vychází, jsou plány. Plány jsou běžně používaným prostředkem pro řízení podniku. Cílem politiky je, aby požadavky vytyčené těmito plány byly vhodně ošetřeny z hlediska bezpečnosti informačních systémů.

Plány můžeme rozdělit podle období, pro které jsou připraveny, na:

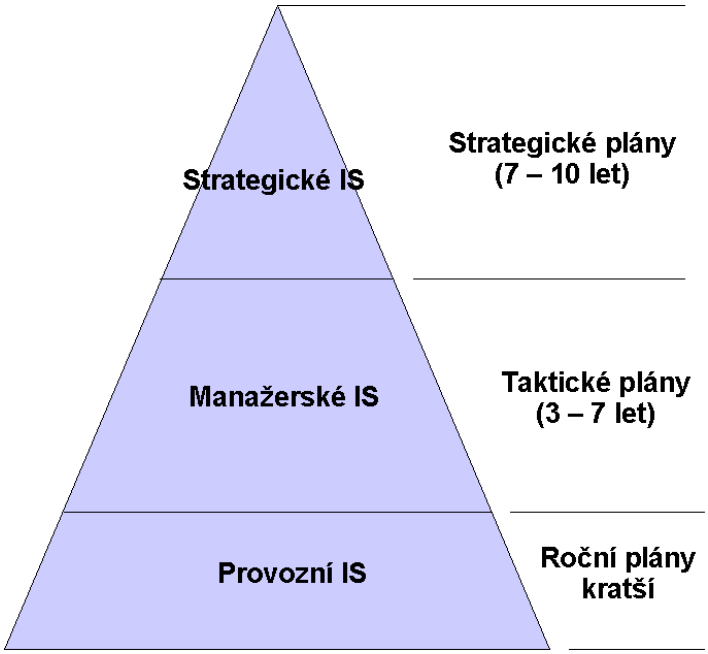
- strategické (7 - 10 let)
- taktické (3 - 5 let)
- roční
- další dle potřeb podniku

Výše uvedené doby, pro které se plánuje, si podnik určuje sám v závislosti na dynamice odvětví, ve kterém podniká.

Strategickým plánem podnik vymezuje svoje zamýšlené postavení na trhu, východiska a směry, kterými se bude ubírat v příštích řekněme sedmi až desíti letech. Jedná se dlouhodobý plán, který obsahuje odhady tržeb v budoucnosti, představy o modernizaci výrobních prostředků, případné akvizice dalších firem.

Taktický plán a roční plány konkretizují strategický plán.

Jako strategické dokumenty má firma samozřejmě zájem plány ochránit a také zajistit, aby realizace kroků v strategii načrtnutých neznamenaly bezpečnostní riziko.




Obrázek 4.1: Použití informačních systémů pro plánování

Mezi obzvláště rizikové činnosti jsou fůze firem, kdy dochází k úplnému pohlcení cizí firmy včetně kompletních informačních systémů resp. dat, která obsahují, zaměstnanců a podobně. Podobné akce nelze vytvářet bez předem připravené formalizované bezpečnostní politiky, pomocí které se minimalizují negativní dopady těchto kroků. Jak tedy vhodně vymezit bezpečnostní politiku IS? V bezpečnostní politice je potřeba zohlednit:

- co je třeba chránit
- proti komu budeme ochranu budovat
- jak budeme chránit

Zdánlivě se jedná o jednoduché otázky. Ve skutečnosti pravý opak je pravdou. Nadefinování bezpečnostních politik tak, aby na jedné straně odpovídaly realitě a zůstaly přitom stručné, snadno pochopitelné a snadno aplikovatelné.

**Pozor**
Kategorizace informačních aktiv organizace (co je třeba chránit) ani proti komu nebo čemu je potřeba chránit (analýza rizik) nejsou přímou součástí bezpečnostní politiky, jsou to však nezbytné podklady pro vytvoření bezpečnostní politiky. Vytváříme je tedy předem a teprve na jejich základě vytváříme samotnou bezpečnostní politiku, která řeší způsoby ochrany informačních aktiv společnost tak, aby byla dosažená určitá (zvolená) míra bezpečnosti.

Jednotlivé plány, vzhledem k tomu, že jsou zaměřeny do budoucnosti, mohou a nemusí být realizovány. Bezpečnostní politika tento fakt musí zohlednit. Bezpečnost z tohoto pohledu je tedy sumou možného – kompromis bezpečnosti za rozumnou cenu. V krizovém managementu se používá pojem ekonomicko-sociálně přijatelná úroveň rizika. Výsledkem odpovědí na výše uvedené otázky s finančními omezeními vyplývající z možného je jedna ze čtyř typů bezpečnostních politik:

- **promiskuitní bezpečnostní politika (BP)** - všichni uživatelé mohou vykonávat všechny činnosti, tedy i takové činnosti, které by z titulu své funkce vykonávat neměli
  *výhody*
  - nízké náklady

  *nevýhody*
  - bezpečnost musí být zajištěna mimo IS (nebo vystavujeme IS útoku hackera)
  - zmatek v kompetencích, celková neuspořádanost systému

- **liberální BP** - umožňuje uživateli dělat vše, co není explicitně zakázané. Je založena obvykle na řízení přístupu na bázi identity uživatele
  *výhody*
  - vyšší bezpečnost než u promiskuitní BP
  - nízká cena

  *nevýhody*
  - nelze využít v systémech s vyšším rizikem

- **racionální BP** - zakazuje dělat vše, co není explicitně povoleno. V rámci této politiky je nutné provést klasifikaci všech objektů BP (dat, serverů, nástrojů ...) a subjektů BP (uživatelů) a na základě klasifikace přidělit práva.
  *výhody*
  - vysoká bezpečnost

  *nevýhody*
  - nákladná na zavedení

- **paranoidní BP** - zakazuje dělat vše, co je potencionálně nebezpečné včetně toho, co by nemuselo být explicitně zakázané
  *výhody*
  - maximální bezpečnost
  - nízké náklady

  *nevýhody*
  - minimální počet uživatelů (je nutné je kontrolovat)
  - omezení funkčnosti systému - dělá pouze to, pro co je určen a ani o trochu více

**Pozor**
Bezpečnostní politika se obvykle nenadepíše jako paranoidní nebo promiskuitní – restriktivnost hodnotíme spíše z obsahu bezpečnostní politiky. Tuto restriktivnost obvykle zavádíme ve smyslu nastavení rolí bezpečnostně ošetřovaných systémů.

Při popisu jednotlivých typů bezpečnostních politik jsme zmínili možnost identifikace uživatele a přidělení práv k jednotlivým objektům informačního systému. To odpovídá principu adresné odpovědnosti. Je tedy nutné stanovit odpovědnosti jednotlivých profesí jako je třeba administrátor, uživatele IS, managementu při práci s IS apod. Zároveň správná implementace tohoto požadavku umožní protokolování činností uživatelů.

*Princip znalosti* požaduje, aby všichni uživatelé byli proškoleni pro správné užívání IS a jejich právech a povinnostech vyplývajících z bezpečnostní politiky podniku.

*Princip integrity* má zajistit, aby cíle bezpečnostní politiky byly v souladu se zamýšlenou strategií podniku, tedy aby bezpečnostní politika byla pro podnik a ne podnik pro bezpečnostní politiku. V literatuře [37] lze najít ještě řadu dalších principů, které se doporučuje dodržovat, ale vzhledem k omezenému prostoru se tady jimi zabývat nebudu.

Naplnění cílů definovaných v bezpečnostní politice musí být přizpůsobena struktura podniku. Každý podnik samozřejmě strukturu upraví tak, aby odpovídala jeho možnostem a potřebám, nicméně činnosti, které jednotlivé prvky struktury budou vykonávat, zůstanou rámcově zachovány:

- bezpečnostní výbor IT organizace - schvaluje bezpečnostní politiku, obrušuje třecí plochy mezi odděleními způsobené implementací bezpečnostní politiky, hodnotí účinnost politiky,
- bezpečnostní manager IT organizace - osoba, která je za bezpečnost odpovědná, řídí implementaci bezpečnostních programů, je přímo odpovědná bezpečnostnímu výboru,
- bezpečnostní správce systému IT - odpovědný za provozování bezpečnostních funkcí dle bezpečnostní politiky podniku,
- bezpečnostní auditor - kontrolní orgán.

Integrální roli v zajištění počítačové bezpečnosti hraje bezpečnostní manažer IT, který může mít dokonce v organizační struktuře samostatné oddělení. Z hlediska pravomocí tak dochází k určitému překryvu mezi různými odděleními. Situaci zobrazuje obr. 4.2.


Obrázek 4.2: Překryv pravomocí oddělení

Oddělení informačních technologií se obvykle stará o běžné, provozní záležitosti spojené s provozováním informačních technologií organizace (nákup výpočetní techniky, instalace softwaru, údržba).

Oddělení bezpečnosti se zabývá bezpečnostními aspekty použití informačních technologií. Právě do gesce tohoto oddělení spadá vytváření a prosazování bezpečnostních politik.

Konečně oddělení fyzické bezpečnosti má za úkol ostrahu objektu, tedy ochranu po fyzické stránce. Všechna tato oddělení se musí vhodně doplňovat, tak aby bezpečnost IT mohla vůbec fungovat. Konkrétní rozdělení pravomocí ale každá organizace řeší sama. V některých případech proto např. Oddělení bezpečnosti IT vůbec neexistuje a jeho úkoly plní oddělení IT apod.

V případě, že IS podniku je rozsáhlý, je někdy výhodné nevytvářet jedinou bezpečnostní politiku pro celý tento systém, ale vytvářet několik dílčích politik, které se budou zabývat dílčími aspekty bezpečnosti IS. Výhodou takového přístupu je např. možnost pružněji reagovat na změny v systému.

Jednotlivé bezpečnostní politiky by se pak mohly zabývat např. IS z hlediska neoprávněného přístupu k terminálům, ochranou budov apod., další by se mohla zabývat programem vzdělávání uživatelů a jejich upozorňování na hrozby plynoucí z možných útoků, apod.

**Kontrolní otázky**

1. Vysvětlete pojem bezpečnostní politika a specifikujte k čemu slouží.
2. Vyberte si jeden z typů bezpečnostní politiky a zamyslete se, jaký by její realizace přenesla efekt při realizace v nějakém známém podniku ve Vašem okolí – náklady, rizika, přínosy.

# Kapitola 5

# Kritéria hodnocení počítačových systémů

**Průvodce studiem**
Pro objektivní hodnocení bezpečnosti informačních systému existuje řada metodik. V této kapitole se seznámíme s několika z nich.

**Po přečtení této kapitoly budete**
**Znát**

- základní metodiky hodnocení bezpečnosti informačních systémů

**Umět**

- vysvětlit základní pojmy z této oblasti

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

V oblasti hodnocení bezpečnosti bylo vykonáno velké množství práce, které vedlo k přijetí řady různých standardů v různých státech. Nejdůležitějším z nich pro pozdější vývoj v oblasti hodnocení bezpečnosti byly TCSEC – Kritéria hodnocení zabezpečených počítačových systémů, někdy také nazývané pro barvu obálky oranžová kniha. Tento standard byl využíván pro hodnocení americkým ministerstvem obrany.

Především v Evropě byly zkušenosti s bezpečností na podobné úrovni a vedly k navržení vlastních kritérií. Ve Velké Británii to bylo CESG Memorandum Number 3 (CESG3) pro použití zejména pro státní účely a takzvaná zelená kniha (DTIEC) pro komerční produkty. Německá bezpečnostní informační služba v roce 1989 publikovala první verzi vlastních kritérií (ZSIEC).

Přibližně ve stejné době byly vyvíjeny ve Francii podobná kritéria v takzvané modré-bílé-červené knize (SCSSI).

## 5.1 Trusted Computer System Evaluation Criteria (TCSEC)

Hodnocení bezpečnosti počítačových systémů je závažný problém. Jako první si to uvědomili v USA někdy v průběhu šedesátých let minulého století. Už do roku 1967 se datuje snaha pod vedením Defense Science Board spojit celý počítačový průmysl zabývající se otázkami bezpečnosti počítačových systémů. Výsledkem bylo několik zpráv, které obsahovaly obecná doporučení týkající se ochrany těchto systémů. Na základě těchto zpráv Department of Defense (DoD) v roce 1972 a 1973 vydal dvě direktivy, které obsahují jednotnou politiku DoD, požadavky na zabezpečení, doporučení pro jejich

administrativní zajištění. V roce 1977 DoD Computer Security Initiative pod vedením Secretary of Defense for Research and Engeneering se zaměřilo do oblasti podmínek počítačového zabezpečení. Zároveň s touto iniciativou byly zahájeny pod vedením National Bureau of Standards (NBS) práce na definici problémů souvisejících s návrhem, implementací a kontrolou provozu zabezpečených počítačových systémů.

Z doporučení obou výše zmíněných iniciativ vyšla ve své činnosti MITRE Corp., která se zaměřila především na kritéria hodnocení počítačového hodnocení s tím, že výsledkem hodnocení by mohl být stupeň důvěry v bezpečnost systému.

V roce 1981 bylo založeno DoD Computer Security Center, teď už pouze za účelem rozšíření zabezpečených systémů tam, kde se pracuje s utajovanými skutečnostmi. Výsledná kritéria by uživateli měla pomoci zhodnotit stupeň ochrany, kterou daný systém poskytuje, a poskytnout základnu pro definici požadavků ochrany v bezpečnostní politice. Výsledkem celého přibližně dvacetiletého vývojového úsilí je norma nazvaná *Trusted Computer System Evalueation Criteria* (TCSEC) [27], tedy kritéria hodnocení zabezpečených počítačových systémů. Vzhledem k datu přijetí (1983) je jasné, že tento systém je zastaralý, a proto se od něj postupně přechází na nová kritéria. Přesto základní myšlenky, které se v TCSEC objevily, jsou stále v platnosti a z tohoto důvodu je dobré se o těchto kritériích zmínit.

Podle TCSEC jsou systémy rozděleny z hlediska bezpečnosti do čtyř skupin (A - D) a tyto skupiny se mohou ještě rozpadat do několika tříd. Třídy standard označuje číselně. Systém skupin je navržen z hlediska abecedy sestupně, tedy nejméně zabezpečený systém zařadíme do skupiny D a nejlépe zabezpečený systém zařadíme do skupiny A. Jednotlivé třídy jsou konstruovány přesně naopak, tedy čím vyšší číslo, tím větší bezpečnost v rámci dané skupiny systémů. Systémy tedy můžeme rozdělit následovně:

**skupina D: Minimální ochrana**
zde se zařazuje vše, co bylo hodnoceno a nevyhovělo požadavkům žádné vyšší třídy bezpečnosti.

**skupina C: Výběrová ochrana**
systémy začleňují prověřovací schopnosti výběrovou ochranou.

- *Třída C1: Zabezpečení ochrany výběrem* - vyhovují systémy oddělující uživatele a data. To umožňuje omezení přístupu k datům tak, aby uživatel měl k dispozici data, která potřebuje a za která je odpovědný. Tento typ ochrany je implementován v jednotlivých programech, se kterými uživatel pracuje.
- *Třída C2: Ochrana řízeným přístupem* - je přísnější v tom, že se vyžaduje nějaká forma autentifikace na úrovni celého systému, ne jenom určitého programu. Tyto systémy mají možnost logování významných událostí apod.

**Skupina B: Direktivní ochrana**

- *Třída B1: Ochrana bezpečnosti návěštím* - Oproti C2 musí být navíc přítomen neformální model bezpečnostní politiky. Zavádí také pojem návěští dat, které uchovává neustále informaci o tom, v jakém režimu utajení se data nacházejí a toto návěští je také využito pro řízení přístupu k objektům systému.
- *Třída B2: Strukturovaná ochrana* - bezpečnostní politika musí být formulována formálně. Vyžaduje se řízení přístupu ke všem objektům systému.
- *Třída B3: Bezpečnostní zóny* - přístup subjektů systému k objektům systému je zprostředkován jediným zařízením (v normě je toto zařízení nazváno referenční monitor).
  Jinými slovy říkáme, že mohou existovat v hodnoceném systému určité služby nebo funkce, které by neměly být přístupné odkudkoliv, ale pouze z určitého přesně vymezeného místa, které obvykle máme pod úplnou kontrolou.

**Skupina A: Verifikovaná ochrana**
Systémy, u kterých je verifikováno (ověřeno), že implementované bezpečnostní funkce skutečně fungují tak, jak fungovat mají.

- *Třída A1: Verifikovaný projekt* - funkčně jsou shodné se systémy třídy B3, narozdíl od nich ale ověřujeme, že naprojektované funkce jsou v systému správně implementovány – tedy ověřujeme, že systém dělá přesně to a pouze to, co dle projektové dokumentace dělat má. Toto zjištění má velký význam pro systémy s vysokými požadavky na bezpečnost (banky, policie apod.).

## 5.2 Trust Technology Assesment Program (TTAP)

Do poloviny 90. let byla jedinou organizací, která se zabývala certifikací, National Security Agency (NSA). Primární funkce NSA je přitom samozřejmě jiná a proto zdroje, které k tomuto účelu mohou být uvolněny, omezené. V důsledku těchto faktorů je počet produktů, které mohou projít procesem certifikace podle Trusted Product Evaluation Program (TPEP), značně omezen – obvykle na produkty, o které mělo zájem Ministerstvo obrany.

Výše uvedené skutečnosti si vyžádaly razantní změny v certifikačním programu – roku 1997 byla spuštěna pilotní fáze certifikačního programu Trust Technology Assesment Program (TTAP) [36] – Program pro hodnocení zabezpečených technologií, s cílem odstranit brzdy v certifikaci produktů.

NSA je v USA vysoce ceněna v bezpečnostní oblasti, zároveň se jedná o státní orgán, měla by u něj tedy být záruka, že bude sledovat především bezpečnostní kritéria a ne kritéria komerční. Využití jediné organizace umožnilo udržovat pouze jeden seznam zabezpečených produktů (Entrusted Product List (EPL) - Seznam zabezpečených produktů).

Zásadní nevýhodou tohoto přístupu kromě malé hodnotící kapacity, která již byla zmíněna výše, je tady i nemožnost hodnotit produkty takovým způsobem, aby bylo možno uznávat certifikované produkty všude ve světě bez dalšího testování.

To však NSA zařídit nemůže, k tomu už je potřeba koordinace se standardizačním úřadem.

Na realizaci nového certifikačního programu proto s NSA spolupracuje National Institute for Standards and Technology (NIST).

TTAP umožňuje zakládání nezávislých akreditačních ústavů (TTAP Evaluation Facility (TEF)), které budou provádět hodnocení produktů. Aby byla zajištěna objektivita, tak udělování akreditace jednotlivým TEF je svěřeno Dohledovému výboru TTAP (TTAP Oversight Board), který je výhradně složen z členů NSA a NIST.

Výbor dále dohlíží nad manipulací s důvěrnými informacemi o hodnocených produktech – zejména na to, že veškeré podkladové materiály shromážděné v průběhu certifikačního procesu jsou buď navráceny nebo skartovány.

## 5.3 Information Technology Security Evaluation Criteria (ITSEC)

Zkušenosti s implementací bezpečnostních standardů přijatých řadou evropských států ukázaly nutnost jejich vzájemného sladění. Nepraktičnost existence velkého množství vzájemně nekompatibilních standardů v otevřeném trhu tehdejšího Evropského společenství (ES) dělala problémy podnikům s působností ve více státech ES. Navíc základní prvky hodnocení bezpečnosti byly ve všech státech stejné, proto bylo logickým krokem na bázi v praxi ověřených norem vybrat jejich nejlepší myšlenky a použít je pro navržení normy nové s celoevropskou působností.

Výsledkem je norma ITSEC [26] – Kritéria hodnocení informačních technologií).

Z hlediska tohoto standardu jsou informační technologie (IT) oblastí primárního zájmu a jsou chápány jako konkrétní instalace technologie za nějakým účelem ve známém operačním prostředí.

IT se přitom myslí hardware i software, ať už jsou implementovány kdekoliv.

Aby IT splnila bezpečnostní cíle, musí mít implementovány funkce pro zajištění bezpečnosti. Tím se myslí například řízení přístupu, bezpečnostní audity, schopnost zotavování se při chybách apod. Jednotlivé třídy hodnocení této normy vycházejí přímo z kritérií specifikovaných v German National Criteria (Německých národních kritériích - ZSIEC) a svou náplní se více méně blíží požadavkům tříd TCSEC.

Před samotným provedením hodnocení je třeba zjistit, co se bude hodnotit:

1. Zadavatel specifikuje operační prostředí systému.
2. Hodnotitelé poznávají prostředí, ve kterém má být systém nasazen, aby bylo možné specifikovat nebezpečí, která systém musí mít ošetřena.
3. Na základě právních a jiných předpisů se vytipují bezpečnostní cíle systému.
4. Stanovení bezpečnostních cílů umožňuje stanovit funkce pro zajištění těchto cílů.
5. Zadavatel zadá úroveň, podle které chce systém hodnotit.

ITSEC se na bezpečnostní vlastnosti dívá ze tří nezávislých pohledů.

1. Bezpečnostní cíle.
2. Funkce zabezpečující bezpečnost.
3. Bezpečnostní mechanismy.

Tabulka 5.1: Srovnání tříd hodnocení ITSEC a TCSEC

| **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 |

Z výše vyjmenovaných pojmů jsme se nesetkali pouze s pojmem bezpečnostní mechanismy - jedná se o způsob, jakým jsou jednotlivé funkce systému realizovány.

Norma rozlišuje celkem 7 úrovní bezpečnosti (E0 - E6), kde E0 představuje neadekvátní ochranu. Pro splnění úrovně E1 musí existovat nějaký cíl bezpečnosti a neformální popis struktury navrženého systému. Testování funkčnosti ukáže, zda systém je schopen plnit bezpečnostní cíle.

E2 oproti E1 musí obsahovat neformální popis detailního návrhu. Systém by měl také poskytovat konfigurační nástroje a schválenou cestu šíření. U E3 se navíc provádí testování bezpečnostních mechanismů. Pro systémy úrovně E4 musí existovat formální model bezpečnostní politiky podniku, funkce zajišťující bezpečnost, návrh architektury a detailní návrh musí být proveden poloformálně.

Proti E4 musí v systémech podle E5 navíc úzce odpovídat detailní návrh finální realizaci pomocí hardware/software. V systémech podle E6 musí být návrh architektury i funkce zajišťující bezpečnost popsány formálně, v souladu s formálním modelem bezpečnostní politiky. ITSEC kritéria v aktuální podobě se používají od roku 1991 na území celé Evropské unie. Uznávání hodnocení dle těchto kritérií je možné u řady států (např. Kanada), uznávání výsledků hodnocení mimo Evropskou unii je řešeno mezistátními dohodami.

V současné době význam ITSEC pomalu, ale jistě upadá. Postupně je použití těchto kritérií totiž nahrazováno CC (Společná kritéria), které řeší problém s uznáváním certifikačního procesu bez ohledu na místo vykonání tohoto procesu.

## 5.4 Common Criteria (CC)

Common Criteria [1] tedy Společná kritéria byla vyvinuta v USA. Ke schvalování byla předána v průběhu roku 1998. Jedná se o výsledek společného snažení řady institucí zabývajících se hodnocením bezpečnosti informačních technologií.

Mezi instituce, které prosazovaly přijetí Společných kritérií patří: Communication Security Establishment (Kanada), Service Central de la Sécurité des Systémes d'Information (Francie), Bundesamt für Sicherheit in der Informationstechnik (Německo), Netherlands National Communications Security Agency (Nizozemí), Communications-Electronics Security Group (Velká Británie), National Institute of Standards and Technology (USA), National Security Agency (USA).

Oproti normám hodnocení bezpečnosti, které jsme dosud zmínili, stanovují Common Criteria pouze jakási společná kritéria, podle kterých bude možné stanovit bezpečnost bez nutnosti procházet opětovným certifikačním procesem pokaždé, kdy firma vyrábějící tento systém expanduje na nový trh.

Aby mohlo být dosaženo porovnatelnosti jednotlivých výsledků hodnocení, musí být hodnocení provedeno v rámci autorizovaného hodnotícího schématu. Toto schéma vymezuje standardy a sleduje kvalitu hodnocení, ale není jako takové předmětem zájmu CC.

Common Criteria si přitom nekladou za cíl stanovit regulační rámec pro hodnocení, ačkoliv dosažení určité míry kompatibility mezi jednotlivými hodnotitelskými autoritami je nutné. Využití společné metodologie hodnocení přispívá ověřitelnosti a objektivitě výsledků hodnocení, ale sama o sobě nestačí. Kritéria mohou být interpretována různými hodnotiteli s většími nebo menšími odchylkami, podle lidí, kteří hodnocení provádějí. Z tohoto důvodu by konečné výsledky hodnocení měly být zaslány k nezávislé inspekci v rámci certifikačního procesu.

Výsledkem tohoto procesu je udělení certifikátu.

Z hlediska hodnocení je pro nás velmi podstatné určení:

- Požadovaného profilu bezpečnosti (Protection Profile (PP))
- Bezpečnostních funkčních požadavků (Security Functional Requirements (SFR))

- Bezpečnostního cíle (Security Target (ST))

Uživatel definuje PP (profil ochrany). Tento dokument by měl obsahovat veškeré bezpečnostní požadavky na posuzovaný systém. PP profily mohou být i obecnějšího charakteru, mohou sloužit jako šablony, které organizace vyvíjející systém použije jako vodítko pro implementaci bezpečnostních funkcí, tak aby jejich systém prošel hodnocením podle tohoto nebo těchto profilů.

Bezpečnostní požadavky nutně vedou k sestavení seznamu bezpečnostních funkčních požadavků (SFR). Funkční požadavky nám obecně říkají, jak by měla daná funkce pracovat – tedy jedná se o specifikaci postupu, algoritmu práce funkce chcete-li.

Bezpečnostní cíle definují požadované bezpečnostní vlastnosti systému. Každý cíl je hodnocen v souvislosti s funkcemi (SFR), které systému mají pomoci tento cíl dosáhnout.

Výsledkem hodnocení je certifikace systému na některou úroveň Evaluation Assurance Level (EAL). Common Criteria rozlišují celkem 7 úrovní bezpečnosti. Přičemž každá úroveň přidává další bezpečnostní požadavky na systém, požadavky tak mají kumulativní charakter.

1. EAL1: funkcionálně testováno
2. EAL2: strukturálně testováno
3. EAL3: metodicky testováno a ověřeno
4. EAL4: metodicky navrženo, testováno a revidováno
5. EAL5: semi-formálně navrženo a testováno
6. EAL6: semi-formálně ověřen návrh a testováno
7. EAL7: formálně verifikovaný návrh a testováno

V rámci hodnocení se obvykle nepožaduje vyšší úroveň hodnocení než EAL4. Někdy se v rámci hodnotícího procesu požadují některá hodnocení nad rámec stanovený Common Criterii, v takovém případě se úroveň hodnocení označí symbolem + např. EAL4+.

**Rozdíly v hodnocení**
Mezi normami pro hodnocení bezpečnosti IT existují podstatné rozdíly i ve způsobu hodnocení, většina norem totiž nehodnotí skutečnou úroveň bezpečnosti systému, ale to jestli systém splňuje určité minimální bezpečnostní požadavky.
Hodnocení u většiny norem bývá také implementačně závislé (závislé na prostředí kam má být systém nasazen). Nedá se tedy říci, že systém hodnocený např. EAL4 je za všech okolností bezpečný – je bezpečný pouze v hodnoceném prostředí.

## 5.5 Certifikační proces v ČR

Česká Republika samotná nemá vlastní kritéria pro hodnocení bezpečnosti informačních systémů, předpokládá se proto, že pro hodnocení budou používána kritéria zahraniční, nejlépe taková, která již byla prověřena a jsou s nimi v zahraničí dobré zkušenosti. Z hlediska legislativy je definována povinnost certifikovat pouze u některých typů informačních systémů se specifickým určením, kde je bezpečnost kriticky důležitá. Povinnost certifikovat je tak stanovena např. pro systémy, které pracují s utajovanými skutečnostmi.

Povinnost certifikovat v tomto případě ukládá vyhláška Národního bezpečnostního úřadu 56/1999 Sb., o bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů [17].

Tato vyhláška je určena všem veřejným informačním systémům, které nějakým způsobem nakládají s utajovanými skutečnostmi. Z této vyhlášky vyplývá potřeba existence bezpečnostní politiky informačního systému jako souhrnu norem a postupů pro zajištění a udržení bezpečnosti informačního systému.

Pro vytváření politiky je dle vyhlášky možné užít některou z metod pro hodnocení bezpečnosti jako jsou např. TCSEC, ITSEC, CC a další. Nejsou tedy specifikována přesně kritéria hodnocení, která je nutné použít, není dokonce specifikována nutnost použít některá z těchto kritérií – autor informačního systému může navrhnout vlastní systém hodnocení, zajistit jeho splnění a informační systém může být úspěšně certifikován.

O samotný proces certifikace se stará nezávislá komise. Nezávislá se zde myslí ve smyslu absence zájmu na úspěšném certifikování informačního systému. V samotném procesu certifikace je informační

systém zkoumán z hlediska splnění požadavků na nakládání s utajovanými skutečnostmi, dle požadovaného stupně utajení skutečností, se kterými bude informační systém pracovat.

Výsledkem procesu hodnocení je vystavení certifikátu. Jen pro doplnění dodávám, že o certifikaci žádá organizace, která chce informační systém zavést, nikoliv samotný výrobce informačního systému. Požadavky na certifikaci jsou také obsaženy v některých dalších zákonech a vyhláškách, např. v prováděcí vyhlášce k zákonu o elektronickém podpisu a dalších. Tato vyhláška ukládá některé povinnosti poskytovatelům certifikačních služeb (PCS). Jednou z těchto povinností je nutnost vyhovět podmínkám EAL4 Společných kritérií pro šifrovací moduly certifikačních autorit – tedy modulu, který se stará o generování certifikátu.

Bezpečnostní požadavek je i v tomto případě logický, alespoň pokud stát má ručit za platnost elektronicky podepsaných dokumentů dle zákona o elektronickém podpisu.

**Kontrolní otázky**

1. Je certifikace IS v ČR povinná a proč?
2. Co je to referenční monitor?
3. Co rozumíme ochranou návěštím?
4. Podle kterých norem hodnotíme skutečnou úroveň bezpečnosti IS?

# Kapitola 6

# Informační systémy veřejné správy

**Průvodce studiem**
V této kapitole se seznámíme s koncepcí informačních systémů ve veřejné správě (ISVS).

**Po prostudování této kapitoly budete**
**Vědět**

- Jaké systémy považujeme za veřejné
- Jakým způsobem jsou ISVS sestavovány
- Jaké úlohy plní v této oblasti ministerstvo vnitra
- Co jsou to datové schránky
- Jak fungují elektronické podatelny

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

## 6.1 Stručná historie informačních systémů veřejné správy v ČR

Budování informačních systémů veřejné správy je spjato s nasazováním informačních technologií ve státní správě. Každá z institucí, která tyto systémy nasazovala tak činila proto, aby do určité míry automatizovala svou činnost a také získala jednotné úložiště, které by umožnilo sdílet data mezi pobočkami veřejných institucí.

Primárním cílem tak bylo zajistit plnění úkolů svěřených těmto institucím prostřednictvím v té době platné legislativy. To znamená, že každá instituce buduje vlastní, samostatný systém, který nepředpokládá spolupráci se systémy jiných institucí nebo dokonce sdílení dat mezi nimi.

Slabiny této koncepce si vláda uvědomila už v roce 1996, kdy vzniká zákonem 272/1996 Sb. ( [22]) Úřad pro státní informační systém (ÚSIS). Ještě téhož roku má být přijat další zákon, který tomuto úřadu měl definovat práva a povinnosti (tedy kompetence). Díky politickým turbulencím ale tento kompetenční zákon přijat nebyl a tak ÚSIS až do svého zániku zůstal „bezzubý“.

Výsledkem jeho práce tak bylo pouze několik spíše obecnějších dokumentů zabývajících se koncepcí informačních systémů ve veřejné správě.

Ke změně dochází až v roce 2000, kdy je přijat zákon 365/2000Sb. o informačních systémech veřejné správy [23], který ÚSIS ruší. Úkoly v oblasti ISVS tak přejímá nově zřízené Ministerstvo informatiky a Úřad pro veřejné informační systémy.

Úřad pro veřejné informační systémy dostává za úkol řešit především praktickou realizaci opatření v oblasti ISVS, zatímco Ministerstvo informatiky řeší oblast normalizace, vývoj legislativy apod.

Ministerstvo informatiky tak oblast řeší především návrhem standardů ISVS, které definují životní cyklus informačních systémů, jakým způsobem budou mezi nimi vyměňována data apod.

Poslední větší změna se udála v roce 2006, kdy zaniká Ministerstvo informatiky a jeho úkoly přebírá Ministerstvo vnitra. V rámci této transformace pozbývají platnost standardy ISVS, ve své původní podobě (tedy jako normy), některé z nich jsou ale přijaty ve formě vyhlášek.

## 6.2 Informační systémy veřejné správy

Informační systémy veřejné správy jsou definovány dnes zákonem 365/2000 Sb. o informačních systémech veřejné správy. Tento zákon definuje ISVS jako soubor informačních systémů, které slouží pro výkon veřejné správy. Tedy v podstatě jakýkoliv informační systém, který je využíván orgány veřejné správy. Za ISVS jsou považovány i jiné informační systémy, které této definici nepodléhají. V takových případech tyto systémy do skupiny ISVS zařazuje nějaký jiný právní předpis (např. zákon o státní statistické službě, živnostenský zákon, apod.).

Naopak u některých informačních systémů, které by výše uvedenou definici splňovaly, se o ISVS nejedná a to opět ze zákona. Jedná se především o takové systémy, které nakládají s údaji takové povahy, že okruh užití těchto údajů by měl zůstat pouze v kompetenci daného orgánu.

Mezi ISVS proto neřadíme informační systémy používané zpravodajskými službami, Policií ČR, Vězeňskou službou, orgány činnými v trestním řízení, Národním bezpečnostním úřadem. Zákonu o ISVS také nepodléhají některé činnosti Ministerstva financí (v souvislostí s finanční kriminalitou) a Ministerstva obrany (v souvislosti s obranou státu).

Zákonu také nepodléhají orgány veřejné správy nebo právnické osoby (resp. IS, které provozují), které tyto IS využívají výlučně pro účely krizového řízení dle krizového zákona (240/2000 Sb.).

Specifické je také postavení Ministerstva vnitra, do jejíž gesce ISVS spadají. Ministerstvo vnitra má:

- kontrolní a tvůrčí pravomoci v této oblasti,
- působí v akreditaci a atestaci,
- stanovuje pravidla pro sdílení informací,
- vyjadřuje se k projektům ISVS,
- vydává věstník.

Pokud mají být finanční prostředky vynaložené na rozvoj ISVS vynaloženy efektivně, musí existovat místo, kde se tyto systémy (a jejich schopnosti) budou registrovat a orgán, který bude kontrolovat, že navrhovaný systém již není realizován a používán např. nějakým jiným orgánem státní správy.

Systémy musí být také vzájemně kompatibilní, pokud si mezi sebou mají vyměňovat informace. Tato kompatibilita by přitom měla jít až na co možná nejnižší úroveň – tedy na úroveň stanovení datového typu a rozsahu a také pravidel validace správnosti vyplněného údaje. Tyto definice pak musí být veřejně dostupné tak, aby je mohly správně do svých systémů implementovat další orgány státní správy. Těmto definicím a pravidlům souhrnně říkáme referenční rozhraní.

ISVS musí také splňovat určité bezpečnostní podmínky, s tím souvisí akreditace a atestace.

Akreditací rozumíme pověření nezávislé právnické osoby prováděním atestací ISVS. Akreditaci provádí Ministerstvo vnitra a může ji udělit pouze nezávislé právnické osobě (nezávislé na posuzovaných ISVS), která je zároveň členem mezinárodních sdružení zabývajících se akreditacemi.

V rámci akreditace se prověřuje zejména existence schválených akreditačních pravidel a také to, zda daná organizace má proces atestace odborně zajištěn kvalifikovaným personálem. Atestace pak provádí akreditované atestační středisko, které nesmí mít pohledávky vůči orgánům státní správy (nesplňovalo by podmínku nezávislosti). Atestace se provádí dvojího typu:

- posuzování dlouhodobého řízení ISVS a
- způsobilost k realizaci vazeb mezi systémy ISVS

Atestace se provádí vždy podle předem stanovených atestačních podmínek. Výsledkem atestace je protokol o zkoušce. Atest se uděluje vždy na dobu určitou a to maximálně na 5 let. Atest je však možno opakovaně prodlužovat a to maximálně o 2 roky.

Své úkoly v oblasti ISVS mají taktéž orgány státní správy a to především:

- spolupracují s Ministerstvem vnitra,
- předkládají Ministerstvu vnitra návrhy na pořízení nebo změnu informačních systémů,
- zajišťují vazby na jiné informační systémy pomocí referenčního rozhraní,
- zveřejňují číselníky,

- odstraňují nedostatky zjištěné v rámci kontrol.

Jakým způsobem konkrétně se výše uvedené činnosti provádějí, definují prováděcí vyhlášky tohoto zákona.

Vyhláška 469/2006 Sb. o informačním systému o datových prvcích [10] definuje fungování informačního systému shromažďujícího informace o jednotlivých datových prvcích.

Datovým prvkem přitom rozumíme datovou položku a její popis. Účelem je, aby data vedená v informačních systémech veřejné správy vedla tato data stejně napříč systémy – a tyto systémy tak byly kompatibilní. Tento informační systém o datových prvcích je základním předpokladem pro možnost implementace referenčního rozhraní.

Předtím, než je tedy navržen nový datový prvek informačního systému, je konzultován IS o datových prvcích, zda už takový prvek neexistuje. Předem jsou už tak řešeny případné návaznosti mezi jednotlivými informačními systémy.

Vyhláška 528/2006 Sb. o informačním systému o informačních systémech veřejné správy [12] definuje náležitosti informačního systému, který bude shromažďovat informace o existujících systémech veřejné správy. Takový systém umožňuje zjišťování, zda existuje IS s požadovanými vlastnostmi včetně toho, kde je takový systém nasazen.

Účelem takového systému je vytvořit prostředí motivující k efektivním investicím do IT. Organizace pořizující nebo modifikující IS tak nemůže činit svévolně, ale až poté co prokáže, že změna je nutná (v souvislosti s legislativními požadavky) a nejsou k dispozici takové systémy, které umožňují vedení potřebné evidence.

Vyhláška 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy [13] se zabývá různými aspekty životního cyklu ISVS a zejména dat v něm obsažených. IS musí být spravován dlouhodobě – dokud bude trvat potřeba dat v něm obsažených. Z toho také vyplývá nutnost provádět plánování na pořízení nebo vytvoření informačního systému, ale také plány na udržení kvality poskytovaných služeb a bezpečnosti.

Základním dokumentem nutným k dosažení těchto cílů je informační koncepce, která se přijímá (na úrovni orgánu státní správy) na dobu určitou a tyto problémy by měla řešit.

Vyhláška 530/2006 Sb. o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS [14] stanovuje způsob, jak postupovat během atestace orgánů státní správy na jejich způsobilost dlouhodobě řídit své informační systémy. Atestace se zaměřuje především na hodnocení informační koncepce a provozní dokumentace provozovaných informačních systémů. Výsledkem atestace je certifikát s jedním z možných výsledků:

- splněno,
- splněno s výhradou,
- nesplněno.

Vyhláška 52/2007 Sb. o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní [11] stanovuje způsob atestace způsobilosti orgánu státní správy realizovat vazby na jiné ISVS pomocí referenčního rozhraní.

Během atestace se hodnotí zejména soulad mezi implementací vazby a její soulad s dokumentací (viz. 469/2006 Sb.). Výsledkem atestace je certifikát s hodnocením splněno nebo nesplněno.

Vyhláška 53/2007 Sb. o referenčním rozhraní [15] stanovuje povinnost používat v rámci ISVS vyhlášené datové prvky. Ovlivňuje také technologii, která bude použita pro výměnu informací mezi jednotlivými ISVS – předpokládá se totiž výměna pomocí jazyka XML.

Konečně vyhláška 64/2008 Sb. o přístupnosti [16] garantuje přístupnost služeb ISVS také lidem se zdravotními postiženími.

## 6.3 Elektronické podatelny

Povinnost zřizovat elektronické podatelny je stanovena vyhláškou 496/2004 Sb. o elektronických podatelnách. Samotné zřízení elektronické podatelny se děje podle nařízení vlády 495/2004 Sb., kterým se provádí zákon č 227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů.

Uznávány jsou podané dokumenty, které splňují určité požadavky na formát zprávy (obvykle jsou podporovány formáty doc, xls, pdf a html – požadavky za formáty musí být také zveřejněny). U některých typů dokumentů je nutné pak ještě připojení elektronického podpisu, značky nebo časového razítka. Požadavky na tyto typy dokumentů jsou stanoveny samostatnými zákony a vyhláškami.

Zaslaná elektronická zpráva se na úřadu zaregistruje a je vyřízena v souladu s pravidly, která byly pro tento typ dokumentů přijaty.

Technicky se v podstatě nejedná o nic jiného než běžné schránky elektronické pošty, které přináležejí k určitému orgánu státní správy nebo samosprávy.

Elektronické podatelny se z hlediska technického i legislativního přežily a jak vyhláška 496/2004 Sb., tak nařízení vlády 495/2004 Sb. byly zrušeny zákonem 167/2012 Sb. Celá komunikace s orgány veřejné správy a samosprávy se tak děje s pomocí obecné normy - zákona o elektronickém podpisu, popřípadě prostřednictvím datových schránek.

## 6.4 Datové schránky

Datové schránky byly přijaty v roce 2008 zákony 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů a 301/2008 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona 300/2008 Sb.

Pro funkčnost datových schránek jsou velmi důležité další navazující zákony a vyhlášky, především 191/2009 Sb. o podrobnostech spisové služby, 193/2009 Sb. o stanovení podrobností provádění autorizované konverze dokumentů a 194/2009 Sb. o stanovení podrobností užívání a provozování informačního systému.

Zákon 300/2008 definuje informační systém datových schránek a jejich využití. Na rozdíl od elektronické podatelny datová schránka funguje jinak. Není založena na technologii elektronické pošty, ale na existenci státem garantovaného informačního systému, kde každý uživatel má svůj prostor a také nástroje pro komunikaci primárně s orgány státní moci, v omezené míře i dalšími uživateli datových schránek. Tímto způsobem odpadají problémy s identifikací uživatele, ale také problémy s doručovacími adresami problémy s vyzvedáváním pošty (listovních zásilek) apod.

Současným provozovatelem informačního systému datových schránek je Česká pošta.

Datové schránky mohou využívat orgány veřejné moci, právnické a fyzické osoby. Zřízení pro všechny typy uživatelů probíhá bezúplatně a to do tří dnů od podání žádosti. Použití datových schránek je přitom pro právnické osoby a orgány veřejné moci povinné a pro tyto zřízení datové schránky probíhá automaticky. Fyzické osoby mohou využít služeb datových schránek nepovinně. Pokud si ale už datovou schránku zřídí, jsou orgány státní moci povinny s uživatelem komunikovat touto formou.

Datové schránky samotné zřizuje a spravuje Ministerstvo vnitra.

Uživatel k obsahu datové schránky přistupuje přes WWW rozhraní. K provozu je však kromě nezbytného WWW prohlížeče nutné mít instalován modul 602XML filter, umožňující snadnější vyplňování formulářů, zejména ve smyslu kontroly vyplňovaných údajů z hlediska syntaktické správnosti (např. že datum je skutečně datum apod.).

Veškeré zasílané dokumenty v rámci komunikace prostřednictvím datových schránek musí být elektronicky podepsány. Pasivní užití schránek je tak sice zdarma, ale v případě, že uživatel chce využívat datovou schránku pro zasílání dokumentů (není to povinné), musí získat patřičný certifikát od poskytovatele certifikačních služeb dle zákona o elektronickém podpisu. Tyto služby jsou již zpoplatněny.

V současné době je zatím možná komunikace se státními orgány v „papírové podobě“ směrem podnik -> státní orgán, komunikace opačným směrem je však ze zákona možná pouze komunikace v elektronické podobě prostřednictvím datových schránek.

Jedinou výjimkou kdy i orgán veřejné moci může využít klasickou „papírovou“ formu je případ, kdy povaha dokumentu to neumožňuje. V současné době se tedy stále v papírové podobě přepravuje dokumentace s velkým rozsahem obrazového materiálu, apod.

Harmonogram náběhu datových schránek je následující:

1. 1.7.2009 – zahájení provozu datových schránek pro orgány státní moci, právnické osoby a dobrovolně fyzické osoby pro komunikaci s orgány státní správy a samosprávy.
2. 1.1.2010 – datové schránky je možné využívat pro komunikaci s jinými uživateli datových schránek pro doručování faktur (nebo jiných dokumentů podobného charakteru).
3. 1.7.2010 – možnost doručování jakýchkoliv dokumentů

Zasílání zpráv faktur nebo v budoucnu jiných dokumentů právnickým nebo fyzickým osobám je přitom také zpoplatněno. Po několika měsících použití se dá s jistotou říci, že zasílání faktur pomocí datových schránek není oblíbenou službou (za první 3 měsíce se poslalo okolo 300 faktur).

Pro zasílané zprávy je vždy vytvořena tzv. obálka s identifikačními údaji zprávy (tzv. metainformace o datové zprávě). Tato obálka se zasílá spolu se samotným souborem zprávy. Po uplynutí 10

dní, se zpráva automaticky považuje za přečtenou, se všemi právními důsledky, které to má. Uživatel datové schránky pak má možnost zprávu přečíst dalších 90 dni. Po uplynutí této doby je zpráva ze systému smazaná (pokud si uživatel nezaplatil dodatečnou službu nazvanou Datový trezor, která je však již zpoplatněna). V systému zůstane zachována pouze obálka datové schránky obsahující

1. Kdo zprávu poslal
2. Komu ji poslal
3. Kdy ji poslal
4. Informaci zda a kdy byla přečtena
5. Název zprávy
6. Haš samotné zprávy

Pokud, tedy příjemce zprávy potřebuje zprávu zachovat pro pozdější použití, musí použít buď zpoplatněnou službu – tato služba ovšem neřeší expiraci certifikátu a tedy možnost ověření pravosti zaslaného dokumentu – nebo musí použít služeb tzv. autorizované konverze dokumentů.

Autorizovanou konverzi je možné provést na CzechPOINTu. Sestává se z ověření datové zprávy z hlediska validity elektronického podpisu (elektronické značky, popř. časového razítka), následného tisku a zkontrolování souladu s původní zprávou. O celém procesu se vytvoří ověřovací doložka, která je uložena do centrálního úložiště. Celý proces tak připomíná proces standardního úředního ověřování dokumentů a jako takový je také zpoplatněn.

**Platnost elektronického podpisu**
Ověření dokumentu/datové zprávy je možné pouze po dobu platnosti certifikátu, který byl použit pro podepsání dokumentu. Po uplynutí platnosti nebo revokaci certifikátu dokument/zprávu není možné ověřit bez ohledu na zákonné lhůty pro doručování zpráv do datové schránky a 90 denní ochranné lhůty pro archivaci zpráv. Takové zprávy již není možné ani autorizovaně konvertovat do listinné podoby. Pokud si nejste jistí mechanismem fungování elektronického podpisu, konzultujte své poznámky/skripta z předmětu Bezpečnostní informatika 1.

Do budoucna se uvažuje s možností dlouhodobého ověřování platnosti dokumentů uskladněných v datových schránkách. Předpokládá se přitom použití kombinace časového razítka a elektronického podpisu. Časové razítko umožní ukotvit dokument v čase a zkoumat, zdali v okamžiku zaslání zprávy byl certifikát použitý k podepsání zprávy v platnosti nebo ne.

Bohužel ani časové razítko nezajistí schopnost ověřování pro situace, kdy došlo k prolomení bezpečnosti použitého schématu elektronického podpisu, které by umožnilo padělání těchto dokumentů. Z tohoto důvodu se uvažuje o použití různých tzv. „solí“, které znesnadňují útoky, ale ani tento mechanismus nezaručuje dlouhodobou bezpečnost – zejména s uvážením možnosti úniku mechanismu generování soli.

Na ověřování dokumentů z datových schránek ale existuje ještě jeden pohled, který je v přímém rozporu s výše uvedeným názorem. Alternativní pohled pracuje s pojmem vyvratitelná domněnka pravosti, podle zákona 499/2004 Sb., o archivnictví a spisové službě [24]. Domněnka pravosti totiž zjednodušeně říká, že dokument se považuje za pravý, pokud byl podepsán a není prokázáno, že by pravý nebyl.

Tento pohled se vůbec nezabývá platností certifikátů (ať už použitých pro podpisové operace nebo operace časového razítka) – dokument může platit věčně. To znamená, že na zájemci o zneplatnění dokumentu je důkazní břemeno prokázání toho, že dokument není pravý.

Tento pohled byl jednu dobu pohledem preferovaným státní správy. Dnes se spíše přikláníme k nutnosti pečlivého udržování řetězce důvěry nutného pro technické zajištění zaručení pravosti elektronických dokumentů.

**Elektronický podpis a datové schránky, zajímavosti a podrobnosti**
Celá problematika elektronického podpisu a datových schránek je velmi zajímavá, bohužel však také velmi složitá a dynamicky se vyvíjející.
Pro zájemce proto doporučuji studium z dalších zdrojů. Začít doporučuji s podnětnými články Jiřího Peterky na lupa.cz [6].
Pozornost věnujte především článkům s nálepkou e-government, datové schránky a e-podpis (ačkoliv i ostatní články jsou nepochybně zajímavé).

## 6.5 Základní registry

V roce 2009 byl přijat zákon 111/2009 Sb. o základních registrech [21], která definuje soubor základních registrů s informacemi o občanech. Základními registry ve smyslu tohoto zákona jsou:

1. Registr obyvatel
2. registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob)
3. registr územní identifikace, adres a nemovitostí (registr územní identifikace)
4. registr agend orgánů veřejné moci a některých práv a povinností (registr práv a povinností)

Tyto registry jsou určeny pro sdílení údajů mezi základními registry a mezi agendovými informačními systémy tak, aby tyto údaje byly udržovány pouze na jediném místě. Ostatní IS, které s těmito údaji pracují, jejich správnost dále nezkoumají.

Základní registry společně tvoří Informační systém základních registrů (ISZR). K těmto registrům přistupují Agendové informační systémy (AIS), v rámci kterých jsou zpracovávány jednotlivé agendy orgánů státní správy a samosprávy.

Zajímavé je také to, že fyzické osoby, o kterých se agenda vede, jsou identifikovány pomocí neveřejného identifikátoru, který je navržen tak, že z něj nelze odvodit žádné osobní nebo jiné údaje vztahující se k dané osobě.

Informace o fyzických osobách registr obyvatel (ROB). Mezi evidované informace patří:

- jméno a příjmení
- adresa/místo pobytu
- datum, místo o okres narození (+ stát u cizinců)
- datum, místo a okres úmrtí
- státní občanství
- čísla elektronicky čitelných identifikačních dokladů
- záznam o zpřístupnění datové schránky

Správce registru obyvatel je Ministerstvo vnitra.

Informace o právnických osobách eviduje registr osob (ROS). Mezi evidované informace patří:

- obchodní jméno/jméno a příjmení u fyzických osob
- agendou identifikátor osoby
- datum vzniku/zápisu do evidence
- datum zániku/výmazu z evidence
- právní forma
- informace o zpřístupnění datové schránky
- statutární orgán
- právní stav
- adresa sídla
- datum zahájení/ukončení činnosti v provozovně
- adresa místa provozovny
- adresa místa pobytu

Správcem registru osob je Český statistický úřad.

Údaje o území, ale také o jednotlivých objektech na daném území obsahuje registr územní identifikace, adres a nemovitostí (RUIAN). O území samotném jsou vedeny následující informace:

1. území státu,
2. území regionu soudržnosti
3. území vyššího územního samosprávného celku
4. území kraje
5. území okresu
6. správní obvod obce s rozšířenou působností
7. správní obvod obce s pověřeným obecním úřadem
8. území obce
9. území vojenského újezdu
10. správní obvod v hlavním městě Praze
11. území městského obvodu v hlavním městě Praze
12. území městské části v hlavním městě Praze
13. území městského obvodu a městské části územně členěného statutárního města
14. katastrální území

15. území základní sídelní jednotky
16. stavební objekt
17. adresní místo
18. pozemek v podobě parcely

O samotných objektech se pak shromažďují tyto informace:

1. měsíc a rok dokončení,
2. počet bytů u stavebního objektu s byty,
3. zastavěná plocha v $m^2$,
4. obestavěný prostor v $m^3$,
5. podlahová plocha v $m^2$,
6. počet nadzemních a podzemních podlaží,
7. druh svislé nosné konstrukce,
8. připojení na vodovod,
9. připojení na kanalizační síť,
10. připojení na rozvod plynu,
11. připojení na rozvod elektrické energie,
12. způsob vytápění a
13. vybavení výtahem.

Funkci editora vykonává obec, městský obvod nebo městská část územně členěného statutárního města, městská část hlavního města Prahy a kraj v přenesené působnosti.

Z hlediska bezpečnosti citlivých informací evidovaných v základních registech je důležité, aby přístup k těmto údajům měly pouze ty orgány (a jejich úředníci), kteří k nim přístup mít mají na základě legislativou stanovených povinností. Tuto úlohu plní Registr práv a povinností (RPP). RPP si lze představit jako matici obsahující na jedné straně jednotlivé úřady a na straně druhé seznam registrů se stanovenými přístupovými právy. Správce registru je opět Ministerstvo vnitra.

V souvislosti s registry je zajímavé jedno datum a to konkrétně *1. 7. 2012*. Od tohoto data totiž vstupují v platnost všechna ustanovení zákona o základních registrech v platnost. V praxi by to mělo znamenat, že úředník při komunikaci s občanem již nebude moci přímo od občana zjistit danou informaci, pokud je již obsažena v některém z registrů.

Myšlenka je to krásná, její praktická realizace však poněkud kulhá. Zdá se totiž že přechod na plnohodnotné využívání registrů nebude nijak snadný, neboť většina ISVS není připravena automatizovanou komunikaci s těmito registry. Připravilo se proto přechodné období, kdy informace ze základních registrů budou předávány poloautomatizovaně prostřednictvím datových schránek.

Předání bude vypadat tak, že úředník jeden krát denně vypíše formulář požadující informace a ty pak následně odešle na místo určení prostřednictvím datových schránek. Žádost o informace bude vyřízena a informace se pošle žádajícímu úředníkovi zpět, opět prostřednictvím datové schránky.

**Kontrolní otázky**

1. Jaké IS užívané státními orgány nepovažujeme za veřejné a proč?
2. Co je to referenční rozhraní?
3. Jak funguje elektronická podatelna?
4. Jaký je rozdíl mezi datovou schránkou a elektronickou poštou?

# Kapitola 7

# Přehled dalších předpisů týkajících se počítačové bezpečnosti

**Průvodce studiem**
Cílem této kapitoly je, aby si čtenář vytvořil pokud možno ucelený obrázek o oblastech formální úpravy bezpečnosti informačních technologií.

**Čas nutný pro studium**
Pro prostudování této kapitoly budete potřebovat přibližně 45 minut.

Na závěr těchto skript jsem si dovolil připravit přehled předpisů zabývajících se bezpečnostními aspekty nasazování informačních technologií. V žádném případě se nejedná o úplný výčet všech existujících předpisů. Záměrně jsem zvolil pouze předpisy vydávané NIST, zejména z toho důvodu, že je možné se k nim dostat zadarmo prostřednictvím sítě Internet – což je pro Vás jako studenty nepochybně výhoda.

## 7.1 NIST – řada 800 (800 series)

Jedná se o celou řadu publikací, které nemají charakter předpisu nebo normy, ale spíše odborné publikace, které jsou zaměřeny na určitou oblast. Jednotlivé publikace pak slouží jako výklad nebo pomůcka pro implementaci technologií, opatření apod. vyplývajících z nějakého předpisu.

Celá řada je tedy čistě podpůrného charakteru. Přehled aktuálně platných publikací naleznete: http://csrc.nist.gov/publications/nistpubs/index.html.

*SP 800-12 - An Introduction to Computer Security: The NIST Handbook* (říjen 1995) – Úvod do počítačové bezpečnosti: Příručka NIST.

Příručka podává přehled základních úvah, důležitých konceptů, vzájemné vazby různých prvků týkajících se zabezpečení výpočetní techniky (hardware, software a informace).

Účelem je, aby čtenář pochopil potřebnost bezpečnosti IT a získal přístup k výběru základních bezpečnostních mechanismů, pomocí kterých lze bezpečnosti IT dosáhnout.

*SP 800-13 - Telecommunications Security Guidelines for Telecommunications Management Network.* (říjen 1995) – Průvodce telekomunikační bezpečnosti pro telekomunikační řízené sítě. Definují rámec a poskytují vodítka pro návrh bezpečných telekomunikačních sítí. Bezpečností se zde myslí

především procedurální, logická a fyzická opatření, která umožňují předejít, detekovat popř. napravit určité činnosti nebo hrozby, které mohou kompromitovat integritu, dostupnost a důvěrnost informací a služeb.

*SP 800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems* (září 1996) – Obecně přijímané principy a postupy pro zabezpečení IT systémů.

Poskytuje základní vodítka pro organizace, vedení, auditory, uživatele o základních požadavcích na bezpečnost, které by měl splňovat každý systém.

*SP 800-15 - Minimum Interoperability Specification for PKI Components (MISPC), Version 1* (září 1997) – Minimální požadavky na interoperabilitu komponent PKI

Zajišťuje společnou bázi pro spolupráci mezi infrastrukturami veřejného klíče (PKI) jednotlivých výrobců.

*SP 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model* (duben 1998) – Požadavky na školení o bezpečnosti informačních technologií: Model založený na rolích a model založený na výkonnosti.

Zajištění ochrany integrity, důvěrnosti a dostupnosti informací v dnešním vysoce zasíťovaném prostředí není možné bez toho, aby každá osoba chápala svou roli a povinnosti a byla adekvátním způsobem proškolena k jejich vykonávání. SP 800-16 byl vyvinut, aby poskytl vodítka pro návrh takového školení.

*SP 800-17 - Modes of Operation Validation System (MOVS): Requirements and Procedures* (únor 1998) – Módy činnosti ověřovacích systémů.

Specifikuje procedury týkající se ověření implementace DES algoritmu, Skipjack algoritmu a ESS algoritmu. MOVS navržen za účelem provádění automatických testů implementace výše uvedených algoritmů.

*SP 800-18 - Guide for Developing Security Plans for Information Technology Systems* (prosinec 1998) – Průvodce pro vývoj bezpečnostních plánů IT systémů.

IT prostředí se stále prudce mění – to s sebou nese nutnost přijmout alespoň minimální kontrolu řízení za účelem ochrany zdrojů IT. Dokument poskytuje vodítka pro vývoj bezpečnostních plánů, které popisují management, technické a operativní nástroje pro federální (USA) automatizované informační systémy.

*SP 800-19 - Mobile Agent Security* (říjen 1999) – Bezpečnost mobilních agentů.

Technologie mobilních agentů představuje nové paradigma informatiky, ve kterém programy ve formě softwarového agenta mohou přerušit činnost, přenést se na jiný hostitelský systém a pokračovat ve své činnosti.

Dokument poskytuje přehled hrozeb, kterým musí čelit návrháři platforem agentů a aplikací založených na agentech. V dokumentu jsou také identifikovány základní bezpečnostní cíle a opatření pro anulování identifikovaných hrozeb.

*SP 800-20 - Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures* (duben 2000).

Viz. SP 800-17 pouze pro algoritmus Triple DES

*SP 800-21 - Guideline for Implementing Cryptography in the Federal Government* (listopad 1999) – Průvodce implementací kryptografie ve federální vládě.

*SP 800-22 - A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (říjen 2000) – Statistický testovací nástroj pro náhodné a pseudonáhodné číselné generátory určené pro kryptografické operace.

A další publikace. Poslední konečnou verzí publikace řady 800 je SP 800-72 – Průvodce forenzní analýzou PDA zařízení z listopadu 2004. Řada publikací 800-66 až 800-77 jsou ve stadiu návrhu a jsou volně dostupné na Internetu pro připomínkování širokou veřejností.

## 7.2 FIPS

Zkratka FIPS znamená Federal Information Processing Standards, tady Standardy pro zpracování informací na federální úrovni. Jedná se o dokumenty normativního charakteru. Jsou závazné pro subjekty státní správy a samosprávy a tedy i jejich dodavatele IT (dodávaná řešení IT musí splňovat požadavky stanovené ve standardu).

Ostatní subjekty se mohou řídit standardy dle vlastního uvážení.

*FIPS 31 - Guidelines for Automatic Data Processing Physical Security and Risk Management* (červen 1974) – Vodítka pro fyzickou bezpečnost a řízení rizika automatického zpracování údajů.

*FIPS 46-3 - Data Encryption Standard (DES)* (říjen 1999) – Standard pro šifrování dat.
Specifikuje užití algoritmů DES a Triple DES pro šifrování.
*FIPS 48 - Guidelines on Evaluation of Techniques for Automated Personal Identification* (duben 1977) – Vodítka pro hodnocení technik automatické identifikace osob
*FIPS 73 - Guidelines for Security of Computer Applications* (červen 1980) – Vodítka pro bezpečnost počítačových aplikací.
*FIPS 81 – DES Modes of Operation* (prosinec 1980) – Módy činnosti DES
*FIPS 102 - Guidelines for Computer Security Certification and Accreditation* (září 1983) – Vodítka pro certifikaci a akreditaci počítačové bezpečnosti.
*FIPS 112 – Password usage* (květen 1985) - Užití hesel
*FIPS 140-1 - Security Requirements for Cryptographic Modules* (leden 1994) – Bezpečnostní požadavky na kryptografický modul.
*FIPS 180-2 - Secure Hash Standard (SHS)* – Standard pro bezpečné hashovací funkce.
A další. Aktuální přehled platných FIPS publikací je možné získat:
http://csrc.nist.gov/publications/fips/index.html
Českou obdobou FIPS dokumentů jsou standardy vydávané Ministerstvem informatiky. Pro přehled platných standardů v oblasti IT viz [39].

## 7.3 Věstníky

Věstníky slouží k informování široké veřejnosti o změnách vyhlášek, norem, standardů apod. Jsou tedy vyloženě informativního charakteru.

NIST za tímto účelem vydává v měsíčních intervalech ITL Security Bulletin [40]. Ministerstvo informatiky v ČR vydávalo vlastní věstník, vzhledem k zániku tohoto ministerstva jsou tyto věstníky dostupné jen v archivní sekce Ministerstva vnitra [18]. Ministerstvo vnitra vydává vlastní věstník, v rámci kterého uveřejňuje

- metodické pokyny,
- seznam atestačních středisek,
- udělení osvědčení o akreditaci,
- udělení atestů,
- další dokumenty vztahující se k informačním systémům veřejné správy,
- seznam určených mezinárodních sdružení zabývajících se akreditací,
- rozhodnutí o pověření akreditující osoby k provádění akreditace,
- rozhodnutí o odnětí pověření k provádění akreditace,
- provozní řád pro dodávání datových zpráv orgánu veřejné moci prostřednictvím portálu veřejné správy.

Tento věstník je možné nalézt na následující adrese: http://www.mvcr.cz/clanek/vestnik-ministerstva-vnitra-vestnik-ministerstva-vnitra.aspx [19].

# Literatura


[1] Common criteria.

[2] Csirt.cz.

[3] Enisa.

[4] First - forum for incident response and security teams).

[5] Gem.

[6] Jiří peterka.

[7] SugarCRM homepage.

[8] TERENA.

[9] Uznesenie vlády slovenskej republiky č. 479/2009 k návrhu organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (csirt.sk) v sr.

[10] Vyhláška 469/2006 sb. o informačním systému o datových prvcích.

[11] Vyhláška 52/2007 sb. o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb isvs prostřednictvím referenčního rozhraní.

[12] Vyhláška 528/2006 sb. o informačním systému o informačních systémech veřejné správy.

[13] Vyhláška 529/2006 sb. o dlouhodobém řízení informačních systémů veřejné správy.

[14] Vyhláška 530/2006 sb. o postupech atestačních středisek při posuzování dlouhodobého řízení isvs.

[15] Vyhláška 53/2007 sb. o referenčním rozhraní.

[16] Vyhláška 64/2008 sb. o přístupnosti.

[17] vyhláška národního bezpečnostního úřadu 56/1999 sb., o bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů.

[18] Věstník ministerstva informatiky.

[19] Věstník ministerstva vnitra.

[20] Welcome to CERT.

[21] zákon 111/2009 sb. o základních registrech.

[22] zákon 272/1996 sb. kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy České republiky a kterým se mění a doplňuje zákon České národní rady č. 2/1969 sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, a mění a doplňuje zákon č. 97/1993 sb., o působnosti správy státních hmotných rezerv.

[23] Zákon 365/2000 sb. o informačních systémech veřejné správy.

[24] Zákon 499/2004 sb., o archivnictví a spisové službě.

[25] Čsn iso 9735 elektronická výměna dat pro správu, obchod a dopravu (edifact).

[26] Itsec, 1991.

[27] *Kritéria hodnocení zabezpečených počítačových systémů.* Ben, Praha, 1994.

[28] nařízení vlády č. 432/2010 sb. o kritériích pro určení prvku kritické infrastruktury, 2010.

[29] CERT.GOV.PL. Arakis agregacja, analiza i klasifikacja incidentów sieciowych.

[30] CSIRT.CZ. Incident handling statistics.

[31] CSIRT.CZ. Novinky.

[32] DHS. National terrorism advisory system.

[33] DHS. *National Strategy for the Physical Protection of Critical Infrastructure.* 2003.

[34] DHS. *National Strategy to Secure Cyberspace.* White House, 2003.

[35] DHS. *National strategy for Homeland Security.* White House, 2007.

[36] E. E. Flahavin and P. R. Toth. Concept paper: An overview of the proposed trust technology assesment program.

[37] G. L. Kovacich. *Průvodce bezpečnostního pracovníka informačních systémů.* UNIS Publishing, Brno, 2000.

[38] Medium Soft. Podpora krizového a havarijního plánování – C3M.

[39] MI. Standard ISVS pro náležitosti životního cyklu informačního systému – 005/02.01, 2002.

[40] NIST. Itl security bulletin.

[41] T-Soft. EmOff – emergency office.

[42] A. Toffler. *The Third Wave.* Bantam Books, Washington (USA), 1984.

[43] US-CERT. National cyber awareness system.

[44] US-CERT. Us-cert - domácí stránky.

[45] P. Šenovský. *Bezpečnostní informatika 1.* VŠB - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 5. edition, 2010.

[46] P. Šenovský. *Bezpečnostní informatika 3.* VŠB - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Ostrava, 2. edition, 2010.

# Slovník

**AIS** Agendové informační systémy.

**B2B** Busines to Bosines.

**B2C** Busimes to Customer.

**BI** Bezpečnostní informatika.

**BP** bezpečnostní politika.

**BYOD** Bring Your Own Device.

**CAD** Computer Aided Design.

**CAM** Computer Aided Manufacture.

**CC** Common Criteria.

**CERT** Computer Emmergency Response Team.

**CIM** Computer Integrated Manufacture.

**CRM** Customer Relationship Management.

**CSIRT** Computer Security Incident Response Team.

**CSS** Cascading Style Sheets.

**DoD** Department of Defense.

**DTP** desktop publishing.

**EAL** Evaluation Assurance Level.

**ENISA** European Network and Information Security Agency.

**EPL** Entrusted Product List.

**ERP** Enterprise Resource Planning (plánování zdrojů podniku).

**ES** Evropská společenství (předchůdce EU).

**EU** Evropská unie.

**FBI** Fakulta bezpečnostního inženýrství.

**FIPS** Federal Information Processing Standard.

**FIRST** Forum for Incident Response and Security Teams.

**HSAS** Homeland Security Advisory System.

**HTML** Hypertext Markup Language.

**IS** informační systém.

**ISP** Internet Service Provider.

**ISVS** informační systémy veřejné správy.

**ISZR** Informační systém základních registrů.

**IT** Informační technologie.

**ITSEC** Information Technology Security Evaluation Criteria.

**JIT** Just in Time.

**JSP** Java Servlet Pages.

**KI** Kritická infrastruktura.

**MI** Ministerstvo informatiky ČR.

**MRPII** Management and Resource Planning.

**MS** Microsoft.

**MV** Ministerstvo vnitra ČR.

**NBS** National Bureau of Standards.

**NIST** National Institute for Standards and Technology.

**NSA** National Security Agency.

**NTAS** National Terrorist Advisory System.

**PCS** Poskytovatel Certifikačních služeb.

**PP** Protection Profile.

**PPS** Produkcionsplanung und Produkcionssterung.

**RFID** Radio Frequency Identification (identifikace na rádiové frekvenci).

**ROB** registr obyvatel.

**ROS** registr osob.

**RPP** Registr práv a povinností.

**RUIAN** registr územní identifikace, adres a nemovitostí.

**SCADA** Supervisory Control and Data Acquisition - Dispečerské řízení a sběr dat.

**SCM** Supply chain management (řízení odběratelsko-dodavatelských řetězců).

**SFR** Security Functional Requirements.

**SQL** Structured Query Language.

**SRN** Spolková Republika Německo.

**ST** Security Target.

**TCSEC** Trusted Computer System Evaluation Criteria.

**TEF** TTAP Evaluation Facility.

**TERENA** The Trans European Research and Education Networking.

**TPEP** Trusted Product Evaluation Program.

**TTAP** Trust Technology Assesment Program.

**USA** United States of America (Spojené Státy Americké).

**USIS** Úřad pro státní informační systém.

**WWW** World Wide Web.

# Rejstřík