Univerzita Jana Evangelisty Purkyně v Ústí nad Labem
Fakulta sociálně ekonomická

DIPLOMOVÁ PRÁCE

2004 **Bc. Tomáš Psika**

Univerzita Jana Evangelisty Purkyně v Ústí nad Labem
Fakulta sociálně ekonomická

Studijní program: Ekonomika a management

Studijní obor: Podniková ekonomika a management

Forma studia: prezenční

Školní rok: 2003/2004

Implementace internetového obchodování v podnikové sféře

E-Commerce Implementation in Company

Vypracoval: **Bc. Tomáš Psika**
Vedoucí diplomové práce: **Mgr. Jindřich Krous**

Místopřísežné prohlášení

Místopřísežně prohlašuji, že diplomovou práci na téma „Implementace internetového obchodování v podnikové sféře“ jsem vypracoval samostatně s použitím literatury, kterou uvádím v přiloženém Seznamu použité literatury na konci diplomové práce.

V Ústí nad Labem dne 4.dubna 2004 Podpis: . . . . . .

Resumé

Tato práce si klade za cíl poskytnout ucelený a téměř komplexní pohled na problematiku implementace internetového obchodování v podnicích orientovaných zčásti nebo zcela na získávání zákazníků prostřednictvím internetu. V první části věnované teoretickým informací se zaměřuji na aktuální souvislosti ovlivňující rozvoj elektronického obchodu a zmíněny jsou především legislativní a jiné podmínky pro vývoj elektronického obchodování v České republice. Je také popsán a zdůrazněn vliv programů Evropské unie na realizaci myšlenky informační společnosti. V dalších částech zaměřuji pozornost na shrnutí základních designérských pravidel pro realizaci úspěšného internetového obchodu a jsou popsány jeho jednotlivé součásti. Praktickou část představuje konkrétní implementace internetového obchodu a popis její funkčnosti. Cílem této části je zejména ukázat jednotlivé kroky, kterými musí tvůrce obchodu projít na cestě k vytvoření základní kostry webové aplikace. Závěrečnou část práce doplňuje pojednání o bezpečnostních problémech dnešních informačních systémů a doporučení, která by se měla při tvorbě webových aplikací dodržovat. Také zmiňuji některé popisy a příklady útoků na internetový obchod za použití standardních hackerských metod a demonstruji tak důležitost zabezpečení na všech systémových úrovních. Závěrem stručně deklaruji základní doporučení pro tvorbu jakékoliv aplikace internetového obchodu.

The main aim of this work is to give coherent and near complex view of the e-shop implementation problems in companies partly or quite orientated in acquirement of internet costumers. First theoretic part reveals circumstances and connections which incluence development of electronic commerce, above all legislative and other conditions for e-commerce growth are specified. There is also impact of EU's Action Plans described and emphasized in conjunction with realization of 'Information Society' idea. I intent on synthesis of main design rules for realization of successful internet shop in next parts of the work. All his components are then described. Practical part contains concrete e-shop implementation and description of his functionality. Objective of this part is to show particular steps forwards to creation of base web-application skeleton. Final part completes discourse about security problems of today's information systems. Then I describe some details about and examples of attacks against e-shops by using standard hacker techniques. This demonstrates the necessarity of security in all system levels. Finally I declare main recommendations for creation of every e-shop applications.

Obsah

Úvod

Úvodní slovo

I v dnešním moderním světě vyspělých technologií posledních dvou století se téměř ve všech oblastech lidské činnosti objeví čas od času krátká přelomová období, která zasáhnou a ovlivní běh světového vývoje na několik dalších desetiletí. Jedno takové období poznamenal objev elektřiny, jiné plodné období lidské inovační schopnosti podnítila druhá polovina 2. světové války a v neposlední řadě se tímto obdobím stalo posledních pár let či desetiletí, které přineslo světu dárek s názvem Internet.

Zatímco se některé dnes již téměř samozřejmé objevy rodily v bolestech a v několika okamžicích, Internetu se tento vývoj netýkal. Pokud pomineme původní účely, pro které vznikla myšlenka sítě Internetu, tak další vývoj tohoto média se odehrával v mírném tempu a teprve v posledních pár letech nabyl takové síly, s jakou dnes ovlivňuje celý svět.

Je jen velmi malá část vyspělého světa, která by internet neznala a nepoužívala ke svým účelům. Internet jako takový nikdo nevlastní, a tak se stal celosvětovým fenoménem, který je zejména v poslední době užíván i k dalšímu rozšíření pole světového obchodu. Právě tímto novým zaměřením celosvětové sítě se bude zabývat tato práce, a to převážně z praktického pohledu komerčních subjektů.

Asi bych však měl uvést důvod zvolení tohoto tématu, kterým je podle názvu této diplomové práce „implementace internetového obchodování“. Musím se přiznat, že před rozhodnutím o zvolení vhodného tématu pro práci jsem příliš nepochyboval o tom, že si zvolím oblast, o kterou se zabývám už pár posledních let, a o které si myslím, že se v ní vyznám alespoň na takové úrovni, abych mohl vyjadřovat své názory na danou problematiku. A protože tato problematika dost významně souvisí s předmětem studia na vysoké škole, kterým je ekonomie a obchod, zdálo se téměř jisté, že do práce přenesu některé poznatky i z trochu jiné oblasti a tím případné studium obohatím o část, které ještě dnes není na školách s podobným zaměřením příliš věnována pozornost.

Struktura práce

Práce se dělí na několik hlavních okruhů. První z nich je zcela věnován převážně teoretickým informacím a jejím cílem je základní uvedení do problémů, které s fenoménem internetového obchodování souvisí. Zejména jsou zmíněny podmínky pro rozvoj obchodu, a to nejen z legislativního pohledu na věc.

Další dvě části tohoto okruhu jsou věnovány už konkrétnějším prvkům internetového obchodu. Zde internetovým obchodem myslím právě tu součást elektronického obchodu, která zajišťuje obvykle obchodní styk mezi podnikem a nejčastěji zákazníkem – fyzickou osobou – prostřednictvím webové prezentace na internetu. Je tedy důležité pochopit přesné zaměření této práce, kterým v žádném případě není popisovat problematiku elektronické podnikání jako uplatnění informačních technologií v celém procesu běhu podniku, ani elektronický obchod v celkovém významu toho slova. To bylo předmětem minulé mé práce (bakalářské), na kterou navazuji je velmi stroze v teoretické části věnované změnám v legislativě. Předmět zájmu práce je tedy výrazně užší a více specializován.

Jsou zde popsány základní pravidla designu obchodu na internetu a blíže popsány nejčastěji používané prvky a součásti, které by měl každý internetový obchod obsahovat, má-li se stát úspěšným na „internetovém trhu“. Vše je vysvětleno z pohledu potenciálního zákazníka nebo tvůrce virtuální části obchodu viditelné na internetu.

V dalším okruhu jsem se snažil osvětlit nejvíce praktickou část obchodování, totiž konkrétní implementaci. To se může zdát být možná pro účely studia ekonomiky a obchodu téměř nadbytečné, neboť praxe při studiu tohoto oboru nebyla užita, ale myslím si, že je lepší o praktickém uplatnění nejen dlouze diskutovat či ho nějak popisovat, ale přímo ukázat, jak se tyto myšlenky zmiňované zejména v první okruhu práce přeměňují v realitu a praktickou upotřebitelnost. Výrazně to sice zvýšilo náročnost během tvoření této práce, doufám, že se však po přečtení práce a po nahlédnutí do příloh této práce pár lidem ujasní, o čem daná problematika skutečně je.

Poslední významnou část diplomové práce tvoří pohled na bezpečnost informačních systémů a internetového obchodu. Tato část stejně jako předešlá část věnovaná implementaci už pro dokonalé pochopení vyžaduje zčásti jiné odborné znalosti ne-ekonomické povahy. Vše je ale záměrně psáno tak, že i pro nezasvěceného člověka může být přínosem, hlavně pro pochopení skutečnosti, že cokoliv na internetu i mimo něj je ohrožováno různými útoky, kterým se dá někdy velmi těžko bránit. K napsání této části mě motivovala hlavně skutečnost, že je dnes pojem informační bezpečnosti stále více znám a už i důsledky bezpečnostních hrozeb vyspěly do podoby, která předurčuje nutnost zájmu i laické veřejnosti.

Závěrečná kapitola zmiňuje hlavní body, které by měly být naplňovány při tvorbě prezentací internetových obchodů. Všechny body a jejich náplň byly zmíněny v celé práci. Pro větší seznam takových bodů je ale vhodnější pročíst nějakou normu, ve které je v tomto ohledu výrazně více informací.

Poděkování

V neposlední řadě děkuji vedoucímu této diplomové práce – Mgr. Jindřichu Krousovi – za připomínkování a za práci, kterou musel jistě vynaložit i na pouhé přečtení celého textu, jehož rozsah nepatří zrovna k těm, které jsou u diplomovových prací běžné.

Dále také děkuji tvůrci nejstaršího a nejkvalitnějšího veřejného sázecího systému TEX, Donaldu Knuthovi, a pokračovatelům jeho práce, díky nimž vznikl způsob sázení textu CSLATEX využitý pro realizaci mého pokusu o profesionální sazbu této práce. Bez nich by totiž má práce vypadala určitě méně hezky.

Kapitola 1

Teoretický základ

1.1 Prostředí pro komerci na internetu

V posledních letech se stejně jako informační technologie vyvíjí i legislativní prostředí, které upravuje podmínky pro rozvoj a uplatnění elektronického obchodu v praxi. Internetové obchody se u nás i v Evropě zdárně vyvíjejí a podíl obchodů uzavřených prostřednictvím elektronických sítí na hrubém národním produktu se významně zvyšuje [1, Ekomerce]. Bohužel to tolik neplatí o České republice, kde je tento podíl nadále malý. Naši zákonodárci stejně jako před několika lety, nemají zcela jasno v tom, jaký postoj by měly zaujmout k této problematice a proč a jestli vůbec by se měly upravovat kvůli této oblasti obchodu různé právní normy, a tak se doplňují do zákona jen občasné a méně významné prvky, které jsou zejména nutné pro přijetí legislativy kompatibilní s legislativou Evropské Unie, do které právě vstupujeme [6, Bilakniha03]. Vše je ale provázeno bez větších veřejných diskuzí o tématice. Avšak i právní úpravy EU, krom programů vytvářené Evropskou Unií, se nezdají být příliš fundované a spíše se realizují až jako důsledek tlaku různých lobbistických skupin a obchodníků, čímž nezaručují všeobecnou přijatelnost ve všech členských zemích. Přesto lze ale říci, že pojetí a přístup k internetovému obchodování a moderní informační společnosti ze strany Evropské Unie je o moc vyspělejší než u nás.

Zejména v přístupu ke koncepci informační společnosti má naše země vůči EU dost co dohánět. Evropská Unie jako jeden z primárních faktorů pro rozvoj informační společnosti považuje internetovou penetraci v rodinách a hraje tak klíčovou roli v hodnocení informační vyspělosti jednotlivých členských zemí. Zde je opět nutné podotknout, že se stále na tomto poli v naší republice nic významného nemění. Stále se sice zvyšuje počet lidí přistupujících k internetu, ale stejně tak jde stále z větší části o zaměstnance firem, nikoliv o příslušníky domácností jako takových. Penetrace internetu ze strany domácností je stále brzděna skličující – i když

dnes už formálně konkurenční – situací na trhu telekomunikačních služeb, a slabou kupní silou domácností. Významnou roli také hraje počítačová gramotnost, o jejíž zlepšení se však stát prostřednictvím Ministerstva informatiky ČR víceméně stará celkem dobře[1], přestože je toto ministerstvo poměrně mladé.

Navíc platí víceméně asi stejný postoj, který panoval u našich právních odborníků před několika lety, kdy se docházelo k závěrům, že není třeba na národní úrovni měnit významně obchodní, občanské a jiné související předpisy v souvislosti s vývojem elektronického obchodování (e-commerce) a podnikání (e-business), neboť se dají již aplikovat ty dnešní i na tento nový způsob obchodování přes internet [2, Skochova01].

Přesto se některé věci za posledních pár let změnili a v dalších kapitolách se jimi budeme zabývat.

1.2 Postoj ČR k elektronickému obchodování

1.2.1 Historie podpory elektronického obchodování

Nejdříve si musíme ujasnit, do jaké minulosti sahá vývoj elektronického obchodu v naší zemi. Historie asi není to nejlepší slovo k pojmenování skutečnosti, že elektr. obchod se u nás vyvíjí až od poloviny 90.let (podobně jako v jiných částech světa), proto se zabývejme nejdříve otázkou, co konkrétně považujeme za elektronické obchodování.

Při konkretizaci elektronického obchodování narazíme na problém, zda se např. obchodování za použití faxů, telefonů apod. dá již považovat za „dostatečně elektronické“. Asi je potřeba vypomoci si nějakou konkrétní definicí. Elektronický obchod (e-commerce) bychom mohli nejlépe definovat jako **způsob obchodování, při kterém se využívají dostupné informační technologie zahrnující zejména elektronická média a telekomunikační sítě k provozování obchodních styků.** Tato definice vyjadřuje asi nejširší vyjádření činností spojených s e-komercí, už téměř splývá s pojmem „elektronické podnikání“ (e-business). Elektronickými médii se v této definici mohou chápat už například přenosy obchodních dat na disketách a optických discích, což byla zřejmě první forma elektronického obchodování, která se u nás uplatňovala možná už po roce 1990, nebo v primitivnějších podobách již před rokem 1989. Pod pojmem telekomunikační sítě se dají ukrýt i telefonní sítě, ale obecně se za ně považují především počítačové sítě v širším významu slova, kdy se telefonní síť může využít nanejvýš jako

[1] Prostřednictvím programu „Národní program počítačové gramotnosti“ (NPPG)

možná přenosová cesta. Mezníkem pro rozvoj elektronického obchodování na standardizované úrovni bylo využití systému EDI[2] podniky. Ten se využívá dodnes.

Co se týče specifičtější formy elektronického obchodu, internetového obchodování (jako součásti oblasti e-komerce), zde již není zvláštní definice potřeba, neboť se jím rozumí obchodování za využití Internetu (zde ve významu mezinárodní sítě založené na protokolech TCP/IP)[3]. Tato forma obchodování je nejmladší a o skutečném internetovém obchodování lze mluvit v USA až od první poloviny 90.let a u nás nejdříve kolem roku 1996[4], tedy od doby, kdy již internet v českých podmínkách přestal být pouze zájmem nadšených studentů a odborné veřejnosti a stal se více veřejným.

16.června 1999 se vláda České republiky rozhodla poprvé vyjádřit svůj postoj k elektronickému obchodu a vydala Usnesení č.604 ve formě „Návrhu opatření pro podporu elektronického obchodu v České republice“, ve kterém definovala základní cíle a k nim směřující kroky státu v oblasti aplikace principů a podpory elektronického obchodu. O rok později, 12. ledna 2000, bylo vydáno nové usnesení (Usnesení č.56), kterým bylo definováno 15 základních opatření, jak stimulovat elektronický obchod v ČR.

Po těchto víceméně formálních usneseních byl v roce 2001 vydán dokument po vzoru Evropské unie s názvem „Zelená kniha o elektronickém obchodu“, a to již v rámci odpovědnosti Úřadu pro veřejné informační systémy (dále jen ÚVIS).

Do této doby se posledním dokumentem, který již nabyl konkrétnější a obsáhlejší podoby, stala **Bílá kniha o elektronickém obchodu** [6, Bilakniha03] (dále jen Bílá kniha), jež reprezentuje závěry několika dalších dokumentů, jmenujme především *e*Europe+ 2003 a *e*Europe 2005 jako klíčové dokumenty přicházející z úřadů Evropské unie, stejně tak i různé směrnice ES vztahující se k elektronickému obchodu. Dále pak tak jako předešlá Zelená kniha vychází ze závěrů aktualizace Akčního plánu realizace státní informační politiky [8, AkplanSIP02], Národního akčního plánu *e*Europe+ 2003 pro Českou republiku přijatý Usnesením vlády č.594 z 13.června 2001 a dalších dokumentů.

1.2.2 Státní informační a komunikační politika

Dříve než se budeme zabývat v samostatné kapitole Bílou knihou, stručně se ještě zmíníme o Státní informační politice ČR [7, SIP02]. Jde o poměrně rozsáhlý dokument zastřešující

[2] Electronic Data Interchange – systém pro výměnu strukturovaných standardizovaných zpráv mezi podniky

[3] Transmission Control Protocol/Internet Protocol – protokoly síťové a transportní vrstvy využívané k realizaci elektronických datových přenosů na dlouhé vzdálenosti

[4] Za první český a dodnes největší internetový obchod se považuje Vltava.cz, vzniklý roku 1996, který má v roce 2004 něco přes 120.000 registrovaných zákazníků. Tento obchod podle `http://www.ebiz.cz` patří k nejlevnějším v českém prostředí – `http://www.vltava.cz`, `http://www.cpress.cz`

mnoho oblastí podpory vývoje informační společnosti po vzoru Evropské unie, a to včetně vyjádření finanční náročnosti v podobě rozvah. Předmětem této politiky je osm následujících oblastí:

- *Informační gramotnost*
- *Informatizovaná demokracie*
- *Rozvoj informačních systémů veřejné správy*
- *Komunikační infrastruktura*
- *Důvěryhodnost a bezpečnost informačních systémů a ochrana osobních údajů*
- *Elektronický obchod*
- *Transparentní ekonomické prostředí*
- *Informační společnost stabilní a bezpečná*

Samostatná kapitola „Elektronický obchod“ už mluví sama o sobě, významným krokem však je také plánování zavádění informačních systémů e-governmentu[5] a s tím související prosazení konceptu informatizované demokracie. Zvýšení informační gramotnosti a moderní informační společnosti je prioritou Ministerstva ČR pro informatiku. Zajímavý je také bod zabývající se důvěryhodností a bezpečnostní informačních systémů a ochrany osobních údajů, což je téma, které bude podrobněji zohledněno i v této práci ve vztahu k internetovému obchodování.

Stále ve stadiu návrhu je nová koncepce **Státní informační a komunikační politiky**, která má sjednotit nynější Státní informační politiku a Státní telekomunikační politiku. Nejde však pouze o jednoduchou konvergenci obou těchto politik, je to i reakce na tzv. lisabonský proces z roku 2000, na kterém se Rada Evropy shodla na strategickém cíli *přeměnit Evropskou unii do roku 2010 v nejkonkurenceschopnější a nejdynamičtější znalostní ekonomiku schopnou udržitelného růstu* [4, Peterka03] [5, Europa]. Mimo jiné se v tomto dokumentu také otevřeně přiznává, že se nepodařilo dle evropského programu *e*Europe+ 2003 zlepšit do konce roku 2002 dostupnost „narrowband“ služeb[6], k čemuž se Česká republika přihlásila usnesením vlády č. 405/01 z 23. dubna 2001. Zde je znění tohoto závazku:

„Dosáhnout podstatného snížení ceny za přístup na Internet posílením konkurence a/nebo regulací cen a srovnáváním na evropské úrovni.“

[5] Využívání informačních systémů ve veřejné správě
[6] Tím jsou myšleny zejména úzkopásmová připojení k internetu

Protože víme, že je tento cíl stále v nedohlednu, snaží se stát prostřednictvím dalších konceptů informační a telekomunikační politiky dosáhnout nejen těchto cílů, ale už i cílů, které vyplývají z programu *e*Europe 2005, ve kterém se považuje za nutné dosáhnout všeobecné dostupnosti „broadband“ telekomunikačních služeb, které představují v poslední době u nás nově vznikající širokopásmová internetová připojení. Je důležité si navíc uvědomit, že už od května 2004 se na nás nebudou vztahovat aktualizované programy pro přistupující země (jako *e*Europe+ 2003), ale již programy členských států. Aniž bych měl něco dopředu předjímat, je splnění tohoto cíle bez nějaké vnější pomoci nebo radikálního řešení více než nepravděpodobné vzhledem k dnešní situaci na národním telekomunikačním trhu, kdy ještě neexistuje ani všeobecně využitelné paušální „dial-up“ připojení[7] a širokopásmová připojení jsou využitelná teprve pár měsíců, zatímco v západní Evropě i USA je tomu už několik let. Situace se pomalu, ale jistě stále zlepšuje[8], obvykle ale jako důsledek donucovacích nástrojů státního aparátu vědomého si svých závazků vůči EU a také díky všeobecné a dlouholeté nespokojenosti internetové veřejnosti, v mnohých oblastech doslova tyranizované důsledky nedokonalostí na komunikačním trhu.

Návrh této politiky, vědom si nynějších nedostatků, v souvislosti s realizací těchto cílů předpokládá v blízké době vytvoření speciálního koncepčního dokumentu „Národní širokopásmová strategie“, který by měl být hotov do vstupu naší země do Evropské unie a splňuje tak základní požadavky *e*Europe 2005. V návrhu také stojí vlastní „národní“ definice broadbandových služeb:

„Za ‚širokopásmové‘ bude obecně považováno takové připojení, které svou efektivní (skutečnou) propustností neomezuje (nezpomaluje) uživatele v jeho aktivitách. Z praktických důvodů bude hranice ‚širokopásmového‘ připojení prozatím stanovena na 256 kbit/s, přičemž se předpokládá její postupné zvyšování.“

Uvidíme tedy, zda se všechny tyto odvážné cíle naplní.

Významnou část návrhu tvoří mimo jiné též oddíl věnovaný bezpečnosti, která je taktéž významnou částí této práce.

Ústředním bezpečnostním tématem několika málo posledních let je elektronický podpis a jeho aplikace ve veřejné správě. Ačkoliv dnes ještě používání elektronického označování dokumentů není technicky a zejména ani koncepčně zvládnuto, státní legislativa není významně pozadu a v posledním návrhu zákona o elektronickém podpisu [13, Zakelektrpodpis03] se blýská na lepší časy, neboť se zákonodárci rozhodli implementovat nový institut „autentizačních dat“,

[7] Z hlediska evropské terminologie tedy zařazované do kategorie „narrowband“ služeb

[8] K 2.únoru 2004 vznikly první, převážně ale ještě výrazně omezené způsoby využití dial-up připojení placeného paušálem – vzhledem k mizivým schopnostem tohoto připojení stále jde o velké finanční částky

který má umožnit používat nástroje se stejnými účinky jako má elektronický podpis, a to automatizovaně a zároveň i pro právnické osoby a orgány státu; navíc byla konečně zahrnuta definice „časového razítka“. Také se doplňují nedodělky slaďování legislativy s EU v oblasti kvalifikovaných certifikátů.

Zejména důležitým se stává nový prvek v tomto zákoně, jímž je *časové razítko*. V souvislosti se šířením elektronických dat po počítačových sítí si praxe vynutila existenci jednoznačného určení, kdy byl určitý dokument vytvořen (tj. podepsán), zda zpráva existovala v určitém čase a také zda byla elektronicky podepsána v té době za použití platného certifikátu. Ustanovení § 2 písm. r), § 6b a § 12b tohoto návrhu se věnují tomuto nezbytnému prvku. Zavedení časového razítka klade poměrně významné nároky na obohacení PKI infrastruktury[9] jednotlivých certifikačních autorit o tento nový prvek.

Řešení bezpečnosti elektronických sítí tento návrh neřeší, výslovně uvádí, že „*nehodlá zasahovat do technické podstaty těchto řešení – ale tam, kde mají mít oporu v zákoně, hodlá závazně specifikovat jejich vlastnosti, parametry a podmínky, které musí splňovat*“. [4, Peterka03] Tímto se elegantně stát vyhýbá řešení tohoto celosvětového problému, což však určitě nelze hodnotit negativně, neboť si s ním ví rady jen málokdo. Přesto však v návrhu padá zmínka o tom, že se stát začne angažovat v této oblasti zveřejněním koncepce s názvem „Národní strategie informační bezpečnosti“, jejíž termín dokončení však není určen. Evropská unie v této oblasti vyvíjí daleko větší iniciativu, a to dotvářením úzce specializované instituce pro boj s počítačovou kriminalitou Cyber Security Task Force, která má spolupracovat s národními „task force“ týmy, jejichž zřízení je i naším národním úkolem. Poprvé tak tedy vznikne typ organizace, který již ve Spojených státech americký delší dobu funguje.

V souvislosti s tímto stát vydal v nedávné době návrh Zákona o službách informační společnosti [12][Zaksluzbyinfspol03], který je také zajímavou nově vznikající normou. V oblasti bezpečnosti definuje např. podmínky, kdy nevzniká *odpovědnost poskytovatelů zprostředkovatelských služeb* za obsah *zprostředkovaných informací*[10], dále se též zabývá *dočasným mezi-ukládáním informací* (dále jen caching nebo cachování) a stále více než aktuálním problémem nevyžádané pošty. Navíc upravuje některá ustanovení občanského zákoníku.

Zejména v oblasti „cachování“ dat (tj. mezi-ukládání dle litery zákona) jsou stanovena poměrně striktní a taxativně vyjmenovaná jasná pravidla, čímž mě tento návrh zákona poměrně mile překvapil. Účinek zákona by měl být pro každého provozovatele serveru jasně zřetelný a i když to zákon podle obsahu důvodové zprávy neměl zřejmě v úmyslu, lze tímto zákonem lépe definovat i takové přečiny (do té doby spíše morálně odsouzeníhodné a nebo upravené v jiné právní normě), jako je zneužívání dočasně uložených dat v dočasných úložištích dat (tj.

[9] Public Key Infrastructure – zázemí pro uplatnění moderní aplikace veřejné kryptografie

[10] Týká se zejména služeb typu webhosting, webhousing a serverhousing – konkrétněji § 3 a § 5 tohoto zákona

cache) serverů, porušování obchodního tajemství či neoprávněné pročítání elektronické pošty bez vědomí adresáta a odesílatele.

Ustanovení věnovaná *nevyžádané poště*[11] (dále jen spam[12]) jsou také víceméně dobře definována a nedají se vykládat několika způsoby, které by umožnili obcházení zákona. Bohužel je však oblast nevyžádané pošty definována příliš úzce a týká se pouze tzv. *nevyžádaných obchodních sdělení*, což automaticky vyřazuje velkou skupinu spamu reprezentovanou zavirovanou poštou, poštou bez jakéhokoliv smysluplného sdělení, hoaxy[13], některou další poštou bez předem určeného účelu a od neznámých lidí, a mnoho jiných typů poštovních zpráv, které v konečném důsledku zdržují uživatele e-mailu, obtěžují ho, a v podnicích snižují produktivitu práce a zvyšují náklady na jejich kontrolu, filtraci a odstraňování. Samotné pojmenování „nevyžádaná pošta“ je v návrhu zákona méně vhodné (logicky nesprávné), ale v souladu se všeobecným chápáním tohoto slova veřejností.

Na závěr je nutné také ukázat na paragrafy tohoto zákona, ve kterých se stanoví orgány dozoru a možné sankce za nedodržení těchto ustanovení. Tyto sankce jsou nezbytné a dle návrhu se počítá, že mohou být uloženy až v maximální výši 10 000 000 Kč podle závažnosti porušení (§10). To by mělo jednoznačně tomuto zákonu přidat na významu. Orgány činnými při kontrole dodržování zákona se stanoví v oblasti nevyžádané pošty Úřad pro ochranu osobních údajů, v jiných oblastech to je krajský živnostenský úřad či profesní samosprávné organizace pro regulovaná povolání dle zvláštního zákona.

1.2.3 Bílá kniha o elektronickém obchodu

Jak již bylo zmíněno, Bílá kniha o elektronickém obchodu [6, Bilakniha03] rozpracovává myšlenky předešlé Zelené knihy, jejímž cílem bylo zejména *analyzovat potenciální překážky, které by bránily rozvoji elektronického obchodu a navrhnout rámcová opatření* a snažit se právně zakotvit komunikaci *dálkovým přístupem mezi občanem nebo podnikatelem a veřejnou správou*. Také byl definován cíl započít tvorbu právě Bílé knihy.

Protože již některé výše uvedené informace jsou součástí Bílé knihy, zmíníme se zde především o principech podpory elektronického obchodu, o konkrétních výše nezmíněných opatřeních na jeho podporu, a to zejména opatřeních legislativních, a v poslední části této podkapitoly zhodnotíme přínos a závěry tohoto dokumentu.

Přestože je Bílá kniha především dokumentem zabývajícím se praktickými opatřeními pro podporu elektronického obchodu, v prvních částech dokumentuje historii elektronického ob-

[11] Mluvíme stále jen o elektronické poště, nikoliv písemné
[12] V zákoně není toto slovo definováno ani zmíněno
[13] Falešná varování před virovou nákazou

chodování a vyjmenovává konkrétní dokumenty, které Česká republika vydala. Navíc také zpočátku definuje základní rozdíl v anglicky vyjádřených pojmech „e-business“ a „e-commerce“, který jsem uznal za vhodné soustředit už do úvodní části této práce, a to hlavně z důvodů čistě sémantických.

Bílá kniha definuje několik základních principů podpory elektronického obchodu, které považuje za důležité. Zde si je pro přehlednost všechny vypíšeme v původním znění:

1. *Rozvoj elektronického obchodu by měl být stimulován především potřebami soukromého sektoru a na základě požadavků a situace trhu.*
2. *Účast na elektronickém obchodu musí být umožněna všem díky existenci volného a otevřeného trhu.*
3. *Stát musí zajistit stabilní právní prostředí a rovné podmínky pro všechny subjekty a chránit veřejný zájem.*
4. *Všechny zásahy státu by měly být jasné, průhledné, technologicky neutrální a takové, aby nediskriminovaly některé subjekty na trhu.*
5. *Elektronický obchod je ve svých principech globální a nadnárodní. Politika státu a jeho zásahy by měly být mezinárodně koordinovány, aby nebránily vzájemné spolupráci všech subjektů na trhu.*
6. *Stát může podporovat rozvoj elektronického obchodu vedle vytvoření stabilního a spravedlivého právního a regulatorního prostředí také svým aktivním chováním a modelovým užitím elektronických nástrojů ve veřejné správě, tedy zaváděním e-governmentu a využíváním vhodných služeb.*
7. *Stát by měl podporovat i aktivity vedené soukromým sektorem a vzdělávacími institucemi v oblasti ochrany spotřebitele, bezpečnosti informačních systémů a výměny informací mezi subjekty na trhu.*

Přínos těchto principů bych nechtěl nějak hodnotit, je zřejmé, že jsou značně intuitivní a obecné, proto jim nelze nic podstatného vytknout. Zajímavé snad jen je, kolikrát se v těchto bodech odráží taková slova jako „trh“, „soukromý sektor“, „spravedlivý“ apod., což evokuje pocit spíše zbožného přání jejich tvůrců, než aby konkrétně vyjadřovaly skutečné principy, které se mají při podpoře elektronického obchodování uplatňovat. Výrazněji to tak upozorňuje na dnešní často úplně jinou realitu.

V legislativních opatřeních na podporu elektronického obchodu se konstatuje ustanovení, které již bylo zmíněno na začátku této kapitoly, že:

„Právní úprava elektronického obchodu v České republice netvoří samostatné odvětví právního řádu a tuto cestu není vhodné volit ani do budoucna. Zvláštní úprava nebyla přijata, protože se elektronický obchod od jiných způsobů obchodování odlišuje v zásadě pouze médiem . . .

Vzhledem ke specifikům využívaného média je však nezbytné řešit některé otázky odlišně od obecné úpravy. . . . “

Tyto „specifické“ úpravy mají za úkol odstranit poslední prvky zákona, které vytváří překážku pro efektivní využívání a fungování elektronického obchodu.

Nastíníme pouze ty nejzákladnější legislativní opatření, která jsou součástí Bílé knihy.

Nejdříve se zaměříme na věčně diskutované úpravy související s uzavíráním **elektronických smluv**. Zde se musíme zabývat Směrnicí EU o elektronickém obchodu, ze které naše úpravy vycházely a dále pak návrhem Zákona o službách informační společnosti (dále jen Zákon o službách), který byl v minulé podkapitole podrobněji popsán a zejména z jeho ustanovení týkajících se úpravy občanského a obchodního zákoníku. Jelikož nejsem podrobněji s vývojem problematiky elektronických smluv v posledních měsících seznámen, vycházím ze znění druhého návrhu této směrnice, který se stal její konečnou podobou a z něho vyplynuvších dopadů na naší národní právní úpravu. V souvislosti s problematikou těchto smluv odkazuji na mou minulou práci z roku 2002 [17, psika02], ve které je podrobněji popsán vývoj znění příslušných ustanovení směrnice.

Směrnice ES pokryly proces uzavírání elektronických smluv institucí „invitatio ad offerendum“, ze které vznikla dvě významnější ustanovení směrnice a poté také ustanovení návrhu Zákona o službách soustředěné do jednoho paragrafu zákona.

Zde je úplně znění § 53, odst. 6) Zákona o službách, kterým se mění zákon č. 40/1964 Sb., občanský zákoník:

„Podá-li spotřebitel objednávku prostřednictvím některého prostředku komunikace na dálku, je dodavatel povinen prostřednictvím některého prostředku komunikace na dálku neprodleně potvrdit její přijetí; to neplatí při uzavírání smlouvy výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací při použití prostředků komunikace na dálku. Objednávka a potvrzení jejího přijetí jsou považovány za přijaté, pokud se s nimi strany, jimž jsou určeny, mohou seznámit. “

Nový odstavec paragrafu obsahuje často odsuzovanou konstrukci „pokud se s nimi (objednávkou a jejím potvrzením) strany, jimž jsou určeny, mohou seznámit“, která byla mnohými odborníky odsuzována [18, Hradek01]. Ustanovení o povinnosti neprodleného potvrzení přijetí

objednávky je konstruována v článku 11 evropské směrnice. Některá další ustanovení jsou upravována nebo přidávána do občanského zákoníku. Jedná se zejména o nutné náležitosti smlouvy, nezbytné informace poskytované „spotřebiteli“ a další drobnosti.

Zákon č. 227/2000 Sb., o elektronickém podpisu, zde byl již také zmíněn, a případné další podrobnosti k první podobě dnes platného zákona se můžete dočíst v mé předešlé práci. V Bílé knize lze taktéž najít odstavec věnovaný platebním systémů a zákonu č.124/2002, o platebních systémech, kde se konstatuje, že nynější podoba zákona – přestože je v souladu s evropskými požadavky – znemožňuje využití mikroplatebních systémů, které by měly zajišťovat odvody velmi malých finančních částek různým příjemcům ze strany provozovatelů serverů a „správců“ jednotlivých webových stránek, čímž by alespoň zčásti mohly vynahradit autorům jejich tvůrčí práci. Často totiž ukončují svou činnost velmi dobré internetové projekty jen proto, že nemají dostatek finančních zdrojů ani na pokrytí nezbytných poplatků jinak nevýznamných pro provoz internetových serverů či webů (hostování domén, platby za energii,...).

V dalších částech Knihy je uvedeno několik dalších zákonů a dodatků, které musí být provedeny nebo problémy, které mají být řešeny. Mezi několika z nich lze jmenovat zejména změnu zákona o účetnictví, která by měla odstranit „tradiční“ uchovávání účetní dokumentace v listinné podobě; dále změnu zákoníku práce, aby bylo možné validovat právní úkony, u nichž se vyžaduje písemná podoba, i elektronicky; v neposlední řadě taktéž změnu zákona o správním řízení (správní řád), o občanském správním řízení, o auditorech, o telekomunikacích a také i zákon o daních z příjmů a DPH.

Závěrem se konstatuje nynější situace elektronického podnikání a obchodování, která je charakteristická některými negativními aspekty, které se mají odstranit. Zdůrazňuje se stále malý podíl elektronického obchodování na hrubém domácím produktu země z důvodu malého využívání internetu malými a středními podniky, potřeba zajistit cenovou dostupnost internetu a telekomunikačních služeb, potřeba zlepšit bezpečnost informačních systémů a výměny informací mezi subjekty prostřednictvím počítačových sítí a nutnost uvědomění mezinárodního charakteru elektronického obchodu.

1.3 Evropská Unie a elektronické podnikání

Záměrně je v názvu této podkapitoly užito výrazu „elektronické podnikání“ – tedy v anglickém slova smyslu „e-business“ – neboť se budeme zabývat širší oblastí podpory tohoto fenoménu posledních let z pohledu Evropské unie. Protože to však není pro tuto práci důležité, popíšeme si jen základní součásti akčních programů EU, které významně usměrňují podporu elektronického podnikání v naší zemi.

Evropská Unie začala kromě legislativního zázemí v podobě mnoha směrnic, doporučení a jiných iniciativ, budovat v oblasti podpory elektronického podnikání i tzv. akční plány, které dostaly podobu programů *e*Europe. Prvním a také i pro nás významným byl program ***e*Europe 2002**, přijatý v roce 2000, ze kterého se vycházelo při definování speciálního programu ***e*Europe+ 2003**, který jako první a poslední měl pokrýt podporu pro informační a komunikační technologie (dále jen ICT) v přistupujících kandidátských zemích a kterým jsme se měli řídit, neboť byl tento program přijat oficiálně Českou republikou prostřednictvím tehdejšího ministerského předsedy Miloše Zemana. Duchovním otcem programů *e*Europe se stal předseda Evropské komise Romano Prodi a v jeho činnosti ho podpořili komisař EK pro informační společnost Liikanen a komisař pro připojování kandidátských zemí Günter Verheugen. Aktualizací tohoto programu vznikla nyní poslední verze s názvem **„*e*Europe 2005“**.

Iniciativa Romana Prodiho začala ale již v roce 1999, kdy otevřel diskuzi na toto téma zveřejněním textu „**eEurope ? Information Society for All**“ [20, Prodi99], ve kterém definoval deset priorit pro přechod EU k informační společnosti. O rok později tato diskuze skončila a v červnu 2000 ve Feiře byl přijat právě program *e*Europe 2002.

1.3.1 *e*Europe+ 2003

Česká republika se při tvorbě iniciativy *e*Europe+ významně a aktivně podílela, neboť měla již určité zkušenosti s podporou myšlenky informační společnosti, které například některé další přistupující země neměly. Základními cíli následného akčního plánu *e*Europe+ 2003 se staly čtyři body, z nichž jeden se nazval jako nultý, neboť byl speciálně navrhnut pro přistupující země, a další body byly společné s programem eEurope 2002 pro členské státy. Zde jsou stručně vyjmenovány všechny body včetně jednotlivých pod-částí:

0. Urychlení realizace základních stavebních prvků informační společnosti.
    - Urychlení přístupu k dostupným komunikačním službám pro všechny
    - Přijetí a implementace acquis ve vztahu k informační společnosti
1. Levnější, rychlejší, bezpečný Internet
    - Levnější a rychlejší přístup k Internetu
    - Rychlejší Internet pro výzkumníky a studenty
    - Bezpečné sítě a inteligentní čipové karty
2. Investice do lidí a znalostí

- Evropská mládež do digitálního věku
- Práce v ekonomice založené na znalostech
- Účast všech na ekonomice založené na znalostech

3. Podpora používání Internetu
   - Urychlení elektronického obchodu
   - Státní správa on-line: elektronický přístup k veřejným službám
   - Zdravotnictví on-line
   - Evropské digitální informace pro globální sítě
   - Inteligentní dopravní systémy
   - Životní prostředí on-line

Nultý bod, speciální pro kandidátské země, měl zajistit „urychlení přístupu k dostupným komunikačním službám pro všechny“ včetně zajištění kontroly plnění tohoto plánu. Měl za úkol alespoň zajistit minimální úroveň podpory informační společnosti. Jako indikátory pro kontrolu se stanovily např. ceny za připojení, procento domácností s pevnou linkou apod.

Prvním bodem, který již byl společný pro oba programy *e*Europe, bylo zajistit vytvoření dostatečné síťové infrastruktury jako základního pilíře pro informační společnost, a *vhodnými opatřeními dosáhnout podstatného snížení cen za přístup na Internet.* Tyto a jiné další úkoly měly být naplněny do konce roku 2002, pouze zavádění služeb digitální televize až do roku 2003. Jak jde vidět, služby digitální televize se „zavedly“ v ČR na poslední chvíli (rozdělení potřebných frekvencí) ke konci roku 2003, a k *podstatnému snížení* cen připojení k Internetu nedošlo vůbec, dokonce „nedošlo ani ke zlevnění, ale zdražení“. Tento nedostatek je zmíněn i v Bílé knize o elektronickém obchodu, o které jsem se zmínil v minulé kapitole. Zajímavé je, jak ani mezinárodní závazky nedokáží naše státní orgány dostatečně motivovat k jejich důraznému prosazení na našem „zkostnatělém“ telekomunikačním trhu. Ostatní cíle, např. rychlejší internet pro studenty a výzkumníky a realizace bezpečných sítí, byly do konce roku 2003 – jak stálo v plánu – z větší části splněny.

Realizace následujícího bodu týkajícího se investic do lidí a vytvoření ekonomiky založené na znalostech je značně dlouhodobější proces, ale přesto byly některé jeho důležité úkoly splněny zcela. Například zvýšení informační gramotnosti bylo cílem několika programů Ministerstva informatiky ČR. Jeden z nich, *Internet do škol*, zajistil, že je snad všem žákům základních a středních škol zajištěn přístup na Internet a zajištěna jakási minimální informační gramotnost, která si vyžádala rozsáhlé programy doplňování kvalifikace učitelů těchto škol. Ale jak už to v našich krajinách bývá, program iniciován státem byl opět jako mnoho jiných podobných

zneužit a výsledkem dnes je, že některé školy mají sice přístup na internet, ale takové kvality[14], který umožňuje současné připojení k internetu snad jen pár žákům v jednom okamžiku, a to ještě, když mají to štěstí a páteř napojené sítě není přetížena. A to podle odborníků za ceny, které by měly zajistit daleko větší kvalitu. Finanční skandál, který se s tímto programem spojuje a který zřejmě ochudil státní rozpočet mimoděk o další miliardy korun, bude mít zřejmě navíc díky našemu neobvykle svižnému soudnímu systému několikaletou dohru. Navíc se s tímto programem spojila ze stran politiků taková propagace, která ve veřejnosti musela původně vzbudit dojem, že je program výsledkem jakéhosi ušlechtilého a dobrosrdečného myšlení zákonodárců a tvůrců programu. Pokud si však uvědomíme, že je tento program nutným prostředkem k tomu, aby se dosáhlo závazků z programu *e*Europe+ 2003, už nemůžeme být tak naivní.

V jiných oblastech ICT však stát také prostřednictvím svých nástrojů a možností implementuje řešení určité problematiky až poté, co je k tomu víceméně „donucena“ externími vlivy. Kéž by se alespoň taková nouzová řešení prosadila v případě monopolu Českého Telekomu na českém telekomunikačním trhu, a to i za cenu finančních ztrát z možné privatizace tohoto „železného kolosu“. Určitě by to vedlo k daleko větší „informatizaci“ české společnosti, neboť potenciál v podobě know-how a schopností v oblasti IT máme oproti většině nejen kandidátských zemí EU větší, srovnatelný např. s Irskem v EU či Estonskem na straně přistupujících zemí. Situace v této oblasti se ale u nás také mění spíše k horšímu, skoro by se dalo říci, že se zvyšující se životní úrovní obyvatel Evropy klesá ochota čerpat informace z oblasti IT.

Bod poslední – podpora používání Internetu v různých oblastech – má snad nejvíce daleko do konstatování bezproblémového stavu. Podíváme-li se na jednotlivé pod-body tohoto programu, najdeme takové části, které snad v našich podmínkách do roku 2002 či roku 2003 nebyly ani teoreticky pochopeny nebo diskutovány. Elektronický obchod se vyvíjí sice pomalejším tempem zejména z důvodu nižších průměrných příjmů obyvatel, ale to je předpokládaný jev. Zato jiné části nejsou zvládnuty vůbec. Především realizace „životního prostřední on-line“, jehož cílem v rámci Unie *vytvořit síť specializující se na sběr, sledování a podávání kompatibilních zpráv o životním prostředí*, je zatím spíše jen podnětem k diskuzi a spíš je ochota tuto činnost provádět ze stran neziskových organizací, které však trpí silnou pod-kapitalizací.

Realizace státní správy on-line není úplně na nulovém bodě, možná je i o dost lepší než v jiných přistupujících zemích, ale z pohledu bezpečnosti – nejnutnějšího základu úspěšného fungování státní správy on-line – je nynější situace téměř ignorováním tohoto programu, který si na problematice bezpečností sítí zakládá. Naštěstí je podobná situace i v některých členských zemích, takže se nemusíme až tolik stydět, že kdejaký cracker pozměňuje obsah některých webových stránek ministerstev a jiných orgánů. Používání elektronického podpisu ve státní správě je už téměř legislativně zajištěno[15], přesto není zatím realizováno.

[14] Rozuměj při porovnání šířky linky, použitého softwaru a hardwaru

[15] Po přijetí novelizace zákona o elektronickém podpisu

Podobná situace je u „zdravotnictví on-line“, už existují teorie, jak by mohlo fungovat, neexistuje však žádná iniciativa k implementaci. Inteligentní dopravní systémy jsou také zatím spíše jen „myšlenkou“. Neúspěchy v této problematice snad může trochu zmírnit závislost prosazení těchto úkolů na členství v Evropské unii.

Je zřejmé, že po našem vstupu do Evropské unie, už může být dost pozdě s nějakým diskutováním nad problémy, které měly být už alespoň teoreticky vydiskutovány a navrhnuta případná řešení. Zvláště když se po vstupu do EU na nás bude vztahovat akční program *e*Europe 2005, o kterém si něco povíme níže.

1.3.2 *e*Europe 2005

Programem *e*Europe 2005 se zde nebudeme zabývat příliš podrobně, protože obvykle stanovuje vyšší kvalitativní cíle programu eEurope 2002. Zmíníme však některé důležité prvky, které se nás bezprostředně týkají.

Akční plán *e*Europe 2005 se považuje za příspěvek k rozvoji znalostní ekonomiky v Evropě. Pokrývá roky 2003 až 2005 a členské státy EU se na něm shodly při summitu v Seville. Česká republika se přihlásila k plnění tohoto programu v souvislosti se svým přistoupením k EU. Tento program je totiž závazný pro členské státy a náš stát jako jeho právoplatný člen od května 2004 musí jeho náležitosti plnit.

O základním cíli jsme se již zmiňovali v minulé kapitole a souvisí s rozšířením širokopásmových připojení k internetu. Jelikož zatím nemáme obecně dobrý přístup ani k úzkopásmovým připojením, lze více než doufat, že závazek, který na sebe tímto bereme, umožní velmi výrazně zlepšit situaci na našem trhu telekomunikací. Pokud si přečteme obsah tohoto programu, zjistíme, že se v něm velmi často objevuje myšlenka „multiplatformní konektivity“, kterou se rozumí schopnost připojení k internetu z různých zařízení[16], ne tedy pouze z klasických počítačů. V souvislosti s tímto cílem se Evropská unie rozhodla vytvořit panevropskou superrychlou počítačovou páteř[17], která má splňovat zvýšené požadavky na konektivitu.

Zároveň program předpokládá existenci moderních verzí e-governmentu (elektronická státní správa), e-health (systém elektronického zdravotnictví), dynamického prostředí pro e-business a také rozšíření e-learningu (elektronická výuka). Jako nutnou podmínku pro realizaci těchto cílů opět předpokládá existenci cenově dostupného širokopásmového připojení k Internetu, a to v dostatečně bezpečném prostředí. Bezpečnost mají zajišťovat speciální instituce v jednotlivých členských státech, přičemž koordinace připadne na ústřední organizaci Cyber security task force (CSTF).

[16] Těmito zařízeními se rozumí především interaktivní digitální televize, zařízení v domácnosti,...

[17] Páteří se zde rozumí páteř internetové sítě

Program definuje několik dalších podstatných cílů, některé z nich budou vyžadovat obrovské finanční částky, což se potvrzuje v poslední části akčního programu.

Program *e*Europe 2005 nově definuje další indikátory, které mají hodnotit situaci v jednotlivých členských zemích[18]. Zatímco v programu *e*Europe 2002 definoval 23 podstatných indikátorů pro hodnocení, nynější program jich definuje podstatně více a rozděluje je do tří základních skupin. Nutné je podotknout, že již první „benchmarking“ se provede už i s novými členskými zeměmi v roce 2004. Máme se tedy určitě na co těšit a myslím, že budeme v těchto oblastech hodnoceni spíše negativně.

Při popisu tohoto programu a při letmém pohledu na jeho anglický text jsem se nedovedl zbavit dojmu, že některé jeho části člověku musí připadat jako „sci-fi“. Neumím si plno věcí představit ani v evropském kontextu, natož v tom malém českém.

[18] Toto hodnocení označuje program za „benchmarking“

1.4 Design obchodu

1.4.1 Design a informační architektura

Předtím než se začneme zabývat designem internetového obchodu, je potřeba si uvědomit pravý smysl tohoto slova. Slovo „**design**“ se chápe ve dvou rovinách, které však nejsou naštěstí v přímém protikladu. Designem v užším slova smyslu chápeme vzhled, grafické provedení či barevnou kompozici. Toto chápání je však trochu povrchní. Skutečný design reprezentuje daleko širší oblast tvorby, která se zejména v našich podmínkách ještě zcela nedoceňuje. To je také důvodem, proč je v naší zemi tak málo skutečných designérů, ať už opomineme jejich odvětvové zaměření.

Co je tedy skutečný význam designu? Je jím bezesporu **vytváření čehokoliv, co má smysl.** Zpočátku takováto definice nemusí být příliš zřetelná, ale je třeba si uvědomit, že neexistuje nějaká vhodněji stanovená definice tohoto termínu, neboť jde částečně o abstraktní pojem. Design v sobě nezaujímá jen pouhou tvorbu vzhledu, ale také funkčnosti. Když kupříkladu začneme vytvářet prezentaci internetového obchodu pro jakoukoliv firmu, není úkolem designu pouze navrhnout hezkou grafickou podobu reprezentující firmu v tom nejlepším světle, ale také tzv. informační architekturu, která podmiňuje konkrétní funkčnost webové prezentace. Je to právě **informační architektura internetového obchodu,** [3, Mindzak02] která má snad největší vliv na kladné či záporné přijímání firemní prezentace na internetu. Samozřejmě se to však netýká jen firemních webových stránek. Potenciální zákazník navštěvující komerční webové stránky se dívá nejen na pouhou grafickou podobu, ale také na konkrétní způsob, jak se může dostat k informacím, které ho zajímají. Implementace vhodné informační architektury tak často rozhoduje o tom, jak bude náš zákazník vnímat naši webovou prezentaci. Je tedy nutné této oblasti věnovat zvýšenou pozornost.

Konkrétněji si vysvětlíme, co se rozumí informační architekturou a jaká je vazba na celkový design obchodu. Musíme se částečně vžít do situace návštěvníka našeho obchodu. Ten obvykle nemá předem nějaké informace o tom, jak využívat náš obchod a nezná jeho schopnosti a vlastnosti. Tento zákazník může chtít zpočátku jen získat potřebné informace o nějakém výrobku nebo naopak je už pevně rozhodnut si něco objednat. První případ je zřejmě pravděpodobnější, pomineme-li ještě, že prvotním krokem potenciálního zákazníka bude nejspíš předběžné získání informací o firmě. Tento krok však zatím ignorujeme, neboť nemá příliš moc významnou vazbu na informační architekturu obchodu. Zákazník chtějící získat informace o určitém výrobku se musí nejdříve seznámit se strukturou webové stránky a to vyžaduje určitý čas. Čím je tento čas kratší, tj. čím je informační architektura obchodu jednodušší a srozumitelnější, tím je větší pravděpodobnost, že bude tento člověk s prezentací spokojen a stane se naším zákazníkem. Informační architekturou se rozumí strukturování informací na jednotlivých webových

stránkách, které by mělo být logické a vést k co nejefektivnější práci s prezentací a v jednoduché navigaci uživatele obchodem. Zejména rozložení hypertextových odkazů na stránce, koncepce logické stavby internetového obchodu a plno dalších věcí tvoří složky informační architektury.

Podle posledních odstavců bychom mohli již odhadnout, že informační architektura webových stránek je nedílnou součástí jejich designu. Design je tedy pojem zahrnující i informační architekturu. Existuje mnoho přístupů a názorů na to, jak by měl být takový design implementován. Mezi web designéry však platí několik málo zásad, o jejichž dodržování se vůbec nepochybuje. Některé z nich zde v několika dalších odstavcích stručně zmíníme. Je ale potřeba také říci, že zejména při tvorbě designu se velmi uplatňuje tvůrčí práce a umělecké cítění, které už samo od sebe může být někdy kontraproduktivní. Je třeba se při tvorbě designu, zejména grafické úpravy webových stránek, částečně oprostit od nadbytečné kreativity, která je tak častá u některých tvůrců osobních webových stránek a stránek, které se primárně zabývají designem. Těžko náš potenciální zákazník může ocenit jeho uměleckou i jinou hodnotu, pokud design popírá hlavní účel internetového obchodu, kterým je samozřejmě prodej výrobků. Zejména pro tvorbu komerčních webových stránek je potřeba dodržovat alespoň základní pravidla, která neomezují jejich funkčnost. Osobně jsem se ale nesetkal zatím s prezentací, která by svým osobitým uměleckým designem nějak významně omezovala či znesnadňovala základní používání obchodu zákazníkem. V těchto případech by totiž často významné finanční částky investované firmou do tvorby designu nemusely přinést očekávané ovoce. Vždy je nutné držet se pevné vize firmy, která si tvorbu prezentace objednává, neboť designér nereprezentuje při implementaci designu sebe a své schopnosti, ale má za úkol prostřednictvím webových stránek reprezentovat firmu.

Protože je design naprosto strategickým prvkem pro zajištění úspěšnosti obchodu provozovaného na internetu v rámci provozu transakcí B2C[19], budeme se jím ještě v několika odstavcích zabývat. Mohly bychom se však také zmínit o elektronickém obchodování a jeho designu v oblasti B2B[20]. Zde pak můžeme říci, že design zde nehraje primární roli. Není potřeba implementovat zvlášť kvalitní design aplikací zprostředkujících obchodní a informační komunikaci mezi podniky. Je to už docela jiná oblast, která není předmětem této práce. Souvisí totiž s jinými informačními technologiemi a je vázána úzce na sofistikovanější informační systémy a jejich vzájemné vazby a rozhraní, které bývají spíše zřídka reprezentovány internetovými stránkami. Musím však říci, že implementace EDI[21] [16, Petr96] a podobných už postarších technologií jsou spíše na ústupu a webové rozhraní se prodírá i do těchto oblastí. Často využívají i jiné technologie, jako např. XML apod., které mohou, ale často spíše nemají podobu prezentace, k jejichž zobrazení používáme webový prohlížeč. Navíc se specifikace formátu XML jako prostředku pro přenos přehledných strukturovaných zpráv stále vyvíjí a nejde zatím o dokončenou

[19] Business To Customer – systém elektronického obchodování mezi podnikem a zákazníkem
[20] Business To Business – systém elektronického obchodování v rámci podniků
[21] Electronic Data Interchange – systém výměny elektronických dat po síti

specifikaci. Možnosti XML[22] se stále vyvíjejí k větší dokonalosti a všeobecné použitelnosti. Tyto přístupy jsou ale pro svou jednoduchost, kompatibilitu a snadnost použití stále oblíbenější. Zejména kladou menší nároky na kvalifikaci obsluhujícího personálu, zvyšují rychlost implementace a tak i šetří náklady a v neposlední řadě taktéž zefektivňují komunikaci. Problémem zde ale může být bezpečnost, vyšší hardwarové nároky na provoz sítí a stabilita takového systému. Je to však již jiná problematika.

1.4.2 Základní principy designu

V tomto odstavci se zmíníme o některých elementárních zásadách, které by se měly ve spojení s tvorbou komerčních prezentací dodržovat. Pak si je ještě trochu podrobněji rozčleníme v dalších částech textu o designu.

Nejdříve si můžeme trochu upřesnit základní pojmy, které nemusí každý znát. Médium nazývané dnes WWW[23] vzniklo již v roce 1989 ve švýcarských laboratořích atomových částic CERN[24] a jeho autorem je Tim Berners-Lee. V souvislosti s tímto médiem vznikl hypertextový jazyk HTML[25], prostřednictvím něhož se vytvářejí webové stránky s hypertextovými odkazy tak jak je známe dnes. K zobrazení HTML stránek se používají internetové prohlížeče, tzv. **browsery.**

V době psaní tohoto textu je nejpoužívanějším browserem Internet Explorer firmy Microsoft, dále se často používají prohlížeče Opera, Mozilla, Galeon, Netscape Navigator, Thunderbird, Amaya, Links apod. V jejich zobrazovacích schopnostech a jiných funkcích nejsou příliš velké rozdíly, přesto však existují odlišnosti pramenící z odlišné interpretace internetových standardů či dokonce implementace nestandardních rozšíření, které obvykle implementace ostatních prohlížečů úspěšně ignorují. Je také dnes zvykem, že se dnešní **prohlížeče** poněkud nepřesně rozlišují na **standardní** (do této kategorie se řadí hádejme proč snad jen Internet Explorer firmy Microsoft) a tzv. **alternativní.** Často však alternativní prohlížeče nejsou nijak podřadné kvality (je tomu často naopak), snaží se však poskytovat jen ty funkce, které jsou mezinárodně schváleny konsorciem W3C, které je obecně přijímáno za tvůrce internetových standardů, které se snaží různé firmy ve svých prohlížečích implementovat. Z takto definovaných odlišností pak pro web designéra pramení určité povinnosti, jejichž cílem je umožnit prohlížení webových stránek obchodu pod různými prohlížeči ve víceméně stejné podobě. To může být často velmi

[22] eXtended Markup Language – moderní značkovací jazyk, formát pro výměnu dat mající dalekosáhlé použití

[23] World Wide Web

[24] fr. Conseil Européen pour la Recherche Nucléaire – Evropské sdružení pro jaderný výzkum se sídlem v Ženevě, založeno 1952

[25] HyperText Markup Language – známý značkovací jazyk vzniklý zjednodušením SGML – Standard Generalized Markup Language

obtížné, proto se tvůrce webového rozhraní musí řídit **mezinárodními internetovými standardy,** které v dnešní době vydává konsorcium W3C. To je tedy první princip, kterým by se měl každý implementátor řídit. Nedodržování těchto pravidel totiž často vyúsťuje v nepoužitelnost obchodu potenciálními zákazníky využívajících jiné platformy, operační systémy a dnes zvané „alternativní“ prohlížeče. Pokud prohlížeč neumí porozumět standardu a zobrazit webovou stránku správně, není to chyba tvůrce internetového obchodu, pokud dodržuje standardy. Ze zkušenosti bych řekl, že dnes si je většina kvalitních internetových obchodů této věci vědoma a již plně respektují tyto standardy. Bohužel to ale neplatí o většině osobních stránek či dokonce i některých větších projektech, např. internetového bankovnictví některých komerčních bank. Poměrně významná část státních institucí, škol apod. tyto principy však již dodržují. Např. e-government by v tomto ohledu měl být vzorem. Z pohledu podniku se nedodržování standardů projevu zvýšeným množstvím stížnosti a dotazů potenciálních zákazníků na nefunkčnost či nepřehlednost obchodu. Vždy je cílem správců webu zjistit příčinu těchto trápení a co nejdříve chyby a opomenutí napravit. To se netýká jen dodržování internetových standardů, ale také konkrétní funkčnosti webové aplikace. Každá firma přeci chce mít spokojené zákazníky. V souvislosti s uplatňováním této zásady je třeba pro firmu ještě zajímavou otázkou, zda náklady vynaložené na opravu již existujícího internetového obchodu nepřeváží nad přínosem v podobě přilákání nových zákazníků a zvýšení jejich spokojenosti s obchodem. To je již čistě manažerské rozhodnutí, neboť IT odborníci stojí hodně peněz a každé firmě se tyto peníze nemusejí vrátit v podobě dodatečných zisků z tržeb.

Další zásada také vyplývá ze schopností browserů a také operačních systémů uživatelů. Mluvíme teď o **barvách.** Je třeba často zohledňovat barevné schopnosti většiny operačních systémů a také počítačových monitorů. V některých operačních systémech (např. MaC OS X) se některé barvy zobrazují jinak, např. jsou světlejší, tmavší apod. Lze se tomu vyhnout různými technikami, kterými se zde ale nebudeme zabývat. Také monochromatické monitory musíme brát v úvahu (např. u mobilních zařízení), pak je třeba dávat si pozor na kontrast jednotlivých barev po převodu na černobílou verzi. Některé barvy se v operačním systému uživatele nezobrazí nebo jsou nahrazeny barvou jinou, která nemusí odpovídat našemu cíli. Nebo se různé barevné přechody na stránce zobrazí ve velmi špatné kvalitě na systémech s méně barvami a méně vybavenou barevnou paletou. Jistě by bylo možné nalézt další problémy s barvami. Hlavním řešením je vystříhat se při tvorbě komerčních webových stránek nestandardních barev či minimalizovat množství používaných barev v grafických prvcích stránek. Protože většina takových omezení částečně omezuje schopnosti vytvořit kvalitní grafický design a schopnosti dnešních prohlížečů, operačních systémů a hardwarových komponent jsou již velmi kvalitní, neřídí se těmito pravidly příliš tvůrců webu. Osobně si myslím, že není potřeba výrazně optimalizovat barevnou kompozici webových stránek právě z těchto důvodů. Určitý ohled se musí brát pouze, vytváří-li se odlehčená verze internetového obchodu pro prohlížeče v mobilních zařízeních, tj. v mobilních telefonech, handheldech apod. Pro tyto aplikace se ale obecně používají trochu více

modifikované principy.

Zásadní je pro každou internetovou stránku **rozlišení,** ve kterém se má zobrazit na monitoru počítače. Potenciálního zákazníka vlastnící dnes již zastaralý monitor s maximálním rozlišením dejme tomu 800*600 pixelů asi příliš neuspokojí webová stránka konstruovaná na daleko vyšší rozlišení nebo větší monitor. Uživatel je totiž v takovém případě nucen posunovat postranními jezdci v okně prohlížeče, protože nevidí stránku v celé své podobě, pouze její část. A posunování jezdců v okně je velmi nepříjemná a zbytečná činnost, která zbytečně prodlužuje čas nutný k prohlížení. Proto se dnes používá při tvorbě konstantně velikých stránek jako vzor rozlišení 800*600, nejvýše však 1024*768 pixelů. Daleko lepším řešením je také vytvoření webového obsahu s dynamickou velikostí, která se přizpůsobuje velikosti okna prohlížeče. V souvislosti s rozlišením monitoru by se měl brát ohled též na proporcionální velikost písma, která musí zaručit čitelnost obsahu. Ale o písmu se zde ještě zmíníme.

Ač se to může zdát být nepodstatné, i **volba** konkrétního typu obrázku a **množství grafického obsahu** na stránce, jsou důležité a podstatné vlastnosti každé webové stránky. Není nic horšího, než když se při modemovém připojení k internetu grafikou zcela vyplněná stránka zobrazuje uživateli déle než minutu (např. http://www.mobilmania.cz). Pak je vždy na místě vhodná optimalizace velikosti jednotlivých obrázků nebo zestřízlivění celého grafického designu stránek. Velmi mnoho uživatelů obtěžuje tato datová náročnost některých stránek a určitě se po určité delší době natahování webové stránky mohou rozhodnout, že už to nevydrží a proces zobrazování našeho internetového obchodu na stránce svého prohlížeče prostě přeruší. A protože je v naší zemi kvalitní internetové připojení z mnoha nepochopitelných příčin stále jakýmsi nadstandardem, je těchto potenciálních zákazníků stále velké množství. Jako příklad lze například uvést, že podle organizace Zona Research ztratili v roce 1999 on-line obchodníci ve Spojených státech 4 mld. dolarů v důsledku pomalého natahování webových stránek[25, Frolik00]. Pokud se přeci jen ale rozhodneme pro přemíru grafiky ve webové prezentaci firmy (což je v tomto případě vždy kontraproduktivní), snažíme se alespoň minimalizovat velikost jednotlivých obrázků. K tomu lze doporučit mnoho postupů spočívající zejména v používání komprimovaných obrázků, komprimování veškerého obsahu webové stránky (příliš se neužívá) či volby úsporných grafických formátů a dalších optimalizačních technik, např. interlacingu (GIF, PNG) a progressingu (JPEG), kdy se obrázky načítají v několika krocích, což se projevuje tak, že se uživateli vykreslí jen hrubá podoba obrázku a v průběhu načítání stránky se tento obrázek vykresluje do větších detailů. Opět je zde ale nutné zabývat se tím, zda tyto a jiné techniky zvládá každý běžný prohlížeč.

Jako poslední nutnost při tvorbě našeho internetového obchodu je nutné se zabývat použitými **písmy** ve webové prezentaci firmy. Je nutné zajistit, aby se náš web zobrazil s čitelným písmem, které lze najít i v jiných operačních systémech. Někdy totiž může dojít k tomu, že

určité písmo v systému uživatele neexistuje a pak se např. nahradí jiným písmem, které už nemusí plnit původně myšlené typografické funkce, tj. čitelnost a nenáročnost čtení textu. Tímto se ještě budeme stručně zabývat v následujících krátkých kapitolách.

1.4.3 Navigační systémy

V tomto oddíle se stručně zmíníme, jak by měla vypadat navigační struktura našeho obchodu na internetu. Jak jsme se již zmínili, navigační systém je součástí celkové informační architektury prezentace obchodu a předurčuje tak částečně funkční schopnost celého obchodu. Navigace společně s implementovanými funkcemi a grafickým provedením rozhoduje nejvíce o tom, zda se k nám potenciální zákazník bude vracet opakovaně a nakupovat naše zboží, služby či výrobky.

Navigace by měla být co nejvíce přehledná a snadno pochopitelná. Jejím úkolem je zajistit zákazníkovi co nejlehčí a naprosto bezproblémový přístup k informacím, které hledá. Čas a trpělivost zákazníka u počítače zde hraje limitující faktor. Čím déle se náš potenciální zákazník snaží vyznat se ve struktuře naší stránky a čím déle se mu to nedaří, tím je větší pravděpodobnost, že se naším skutečným zákazníkem nikdy nestane.

Způsobů, kterých se užívá při tvorbě navigace je hned několik. Dávno přežitým způsobem je **navigace v nezávislém rámci**, kdy se veškeré důležité odkazy realizují v jednom či více rámcích a vlastní stránka je také částí jiného rámce. Tento způsob byl ještě před několika lety velmi používaným, neboť existovaly především statické webové stránky, které již dnes nejsou vhodné pro realizaci internetových obchodů. Stále se však používají, zejména při tvorbě jednoduchých webových stránek. Daleko častějším způsobem realizace navigace je **klasická navigace**, tj. bez použití rámců. Navigační prvky jsou součástí každé jednotlivé stránky, obvykle se nalézá v horní či levé části stránky. Díky vývoji informačních technologií a rozšíření dynamicky generovaných stránek se tento styl navigace v posledních letech rozšířil nejvíce. Pro tvorbu dnešních internetových obchodů a obecně i jiných profesionálních stránek se užívá tzv. „tabulková grafika“, kdy celý obsah stránky tvoří jedna či více velkých tabulek, v jejichž jednotlivých polích se objevují odkazy, vnořené tabulky a vlastní obsah. Tento styl zobrazení umožňuje zachovat kvalitní design a také umožňuje realizovat sofistikovanější navigační systém.

Existují dva přístupy ke tvorbě navigačních prvků. Jeden z nich používá jednoduchou, tzv. **textovou navigaci**, při které není potřeba tvořit téměř žádnou grafiku. Tento přístup se používá zejména tehdy, pokud se snažíme zrychlit přístup na stránky pro pomalá modemová připojení, ale nejen tehdy. I pomocí jednoduchých textových odkazů a tabulek za použití stylových jazyků (např. CSS[26]) lze poměrně dobře vytvořit vynikající design. Také proto se často

[26]Cascading Style Sheets – stylový jazyk rozšiřující omezené možnosti jiných značkovacích jazyků

používá. Častěji používaným přístupem však je realizace **grafické navigace** s obrázky. Ta dává každému designérovi víceméně volnou ruku a lze tak realizovat téměř každé přání firmy. Jazykem dnešních internetových technologií se takováto navigace realizuje zejména prostřednictvím klikacích map, grafických odkazů, grafických tlačítek a prvků s „roll-over“ efektem a dalšími způsoby. Grafická navigace však přesto přináší jednu podstatnou nevýhodu. V důsledku velké datové náročnosti obrázkové grafiky si někteří uživatelé prohlížečů vypínají načítání obrázků, což pak klade na designéra další požadavky. Webová stránka s nezobrazenými obrázky musí být i přesto potenciálním zákazníkem použitelná. Realizuje se to tím, že se HTML kód webové stránky doplní o doplňující atributy obrázků, které způsobí, že místo obrázku se v okně prohlížeče zobrazí pouze text.

Ať už použijeme jakýkoliv přístup k tvorbě navigačního systému, musí se vždy brát ohled na jeho základní cíle. Konkrétní implementace a schopnosti a zkušenosti web designéra hrají klíčovou roli pro následné kladné či záporné přijetí výsledného internetového obchodu zákazníkem.

1.4.4 Typografický design, písmo

Veškerý obsah stránek je obvykle v textové podobě, proto tedy nepochybně záleží na úpravě textu a na tom, jak se tento text jeví přehledným a zda se snadno čte. I nevhodným výběrem rodiny písma, jeho velikostí, řezy apod. lze vzhled webové prezentace značně znehodnotit. Ačkoliv se to nemusí na první pohled zdát, existuje plno pravidel, převážně typografických, kterými by se měl designér určitě zabývat.

Obecně rozdělujeme písma používaná na webech na patková, bezpatková a monospace. Patková písma jsou charakteristická linkou na začátku a konci každého písmene, zejména ve spodní části písmene. Tato písma jsou čitelná a ulehčují orientaci v souvislosti řádku. Nejpoužívanějším představitelem tohoto písma je rodina Times New Roman na systémech s Windows a Times Roman na unixových systémech a na MACu. Bezpatková písma naproti tomu jsou méně užívaná při tisku knih a časopisů, pro webový obsah jsou však vhodnější, neboť jsou jednoduchá a velmi čitelná. Čtení textu vysázeném patkovým písmem je totiž se zvyšujícím se objemem textu stále více náročné na orientaci a soustředění. To je také hlavní důvod, proč se častěji používají bezpatková písma. Nejznámějším představitelem rodiny bezpatkových písem je Sans-Serif. Posledním používaným typem písem na webu je monospace písmo, která má vždy stejnou mezeru mezi jednotlivými písmeny. Nejznámějším písmem tohoto typu je Courier. Pro webový obsah však písma monospace nejsou příliš vhodná, neboť neúměrně zabírají místo, kterého je na obrazovce monitoru vždy málo.

Primární značkovací jazyk HTML používaný při tvorbě internetových stránek nemá vhodné nástroje pro rozšířenou práci s jednotlivými fonty, proto se často používají rozšiřující možnosti poskytované stylovým jazykem CSS. Ten umožňuje definovat pevnou velikost písma. Názory na to, zda by měly mít písma na stránkách fixní velikost nebo zda-li by mělo být umožněno uživateli velikost dynamicky měnit, se různí. Dle mého názoru již dnes každý lepší a inteligentní prohlížeč webových stránek umí zvětšovat velikost celkové stránky beze změny písem, které, jsou-li definovány fixně, nemění vzhled a design webové stránky. Není tak tedy potřeba ještě navíc umožňovat uživateli měnit vzhled písem.

Pro webovou prezentaci internetového obchodu je vhodné použít jen jednu, nejvýše dvě rodiny písma, raději bezpatkových rodin. Platí zlaté typografické pravidlo „**čím méně, tím lépe**“. Doporučuje se použít i více řezů písma podle objemu textu na webové stránce, nejvýše však pět až osm, odstupňované například podle důležitosti v textu (nadpisy, citace, . . .).

Vždy bychom měli používat taková písma, která jsou obecně dostupná pro všechny platformy. Takových je velmi málo, lze jmenovat zejména rodiny Times Roman a Helvetica (Arial). Také je potřeba počítat s tím, že i stejná písma se na různých systémech mohou zobrazovat v jiné velikosti.

Problém s neexistencí některých písem na různých platformách je dlouhodobě přetrvávající a už roky je snaha tento problém nějak inteligentně řešit. Vzniklo tak několik technologií, z nichž nejvýznamnější se jeví tzv. „font embedding“, kdy se odkaz na konkrétní užité písmo stává součástí webové stránky, čímž by se měly vyřešit problémy s mezi-platformními rozdíly. Zástupci těchto technologií (True Doc, OpenType) se však ještě asi zdaleka tak rychle nestanou standardními nástroji na internetu..

1.4.5 Barevná kompozice

Teď se budeme krátce věnovat barevné sladěnosti našich webových stránek internetového obchodu. Kompozice barev na webové stránce je totiž to nejdůležitější, co vytváří první dojem pro návštěvníka. Je tedy velmi důležité se tímto tématem také zabývat. Hlavním úkolem designéra by mělo být vytvořit takovou barevnou kompozici, která jasně vystihuje charakter prezentace, a zároveň se držet základních principů, které zajistí, že bude stránka snadno čitelná a bude pozitivně působit na uživatele. Není totiž nic horšího, než když někdo vytvoří stránku např. s červených písmem na modrém pozadí nebo když použije takovou barvu písma a pozadí, která způsobí, že je velmi obtížné takový text číst.

Určitě patří správná volba barev na webu mezi nejobtížnější úkoly designéra. Nejdříve si něco povíme o základních typech barev a vztahu mezi nimi. Primárně se barvy, tak jak téměř

každý ví, dělí na **studené** a **teplé barvy**. Mezi studené a obvykle příjemné barvy lze zařadit zejména modré odstíny, mezi teplé a někdy agresivní například červené odstíny barev. Každá barva s sebou přináší určitou „náladu“. Například sytá červená barva provokuje a působí velmi dráždivě, zatímco např. některé modré a zelené odstíny působí velmi klidným dojmem. Pro prezentace internetových obchodů a firemních prezentací je vhodné používat příjemné a spíše chladné barvy. Doporučuje se standardní bílé pozadí webových stránek, zejména z důvodu čitelnosti. Není to však podmínka, často se dají za nezmenšení čitelnosti použít i světlé odstíny žluté či zelené barvy. Obvykle je nutné vytvářet poměrně kontrastní variaci barev, aby byla prezentace více čitelná.

Webová prezentace obchodu však jen málokdy bývá vyplněna pouze dvěma či třemi barvami. Často je nutné zejména z důvodu odlišení určitých částí stránek, hierarchických úrovní a odstavců v textu využít většího množství barev. Zde je pak nutné řídit se barevným spektrem barev a určit, zda se určité kombinace barev dají zařadit mezi barvy analogické, komplementární či zda se dají považovat za jednoduché monochromatické schéma.

Můžeme se tedy řídit tzv. kruhovým barevným spektrem, které poprvé použil Isaac Newton v roce 1666. V něm se **barvy**, které leží vedle sebe označují za **analogické**. Tyto barvy spolu tzv. „ladí“, stejně tak jako barvy **komplementární**, které se také označují jako opozitní. Ty leží v kruhovém spektru naproti sobě. Vždy je třeba rozhodnout se pro použití jen jednoho typu barev, popř. je doplnit nanejvýše jednou méně agresivní barvou, např. určenou pro zvýraznění textu či částí stránky. Na internetu lze najít velké množství webových stránek, které v důsledku řízení se tímto postupem vypadají naprosto perfektně a vytvářejí velmi vynikající dojem. Abychom vše ještě doplnili o jeden postup, musíme se zmínit o použití **monochromatického schématu**, které je tvořeno bílou a černou barvou s jedním odstínem jiné barvy s různými stupni světlosti a sytosti. Tyto barevné kombinace jsou také velmi často používané.

Není od věci zde zmínit, že poměrně značná část populace nevnímá všechny barvy stejně, někteří lidé jsou slabě barvoslepí a vnímání nekontrastních barevných schémat jim může činit velké potíže. Když už najdeme optimální barevnou kompozici, měli bychom si vyzkoušet kontrastnost a přehlednost tohoto schématu převedením stránky na černobílou monochromatickou variantu a zde pak hodnotit kontrastní vlastnosti. Pokud je i poté obsah prezentace čitelný, máme vyhráno a barvy jsou nejspíš dobře zvoleny.

Posledním problémem se může stát zobrazení barev na počítači uživatele. Už jsme se o tomto problému zde zmínili, některý hardware (monitor, palmtop, ...) některé barvy nezobrazí správně, např. je nahradí jinou barvou z dostupné palety, problémy mohou nastat i v důsledku použití méně schopného operačního systému, který mění např. gamma profil zobrazované grafiky, v důsledku čehož se některé obrázky na webové stránce mohou jevit světlejší či tmavší než na jiném systému. Dnes již ale existují grafické formáty, které tyto nedokonalosti

dokáží překlenout (např. formát PNG). Krátce se o tom zmíníme v následující podkapitole věnované grafickým formátů používaným na webu. Opět je potřeba brát ohled na to, zda vytváříme webovou prezentaci pro zobrazení na počítači či na mobilním zařízení typu mobilu.

1.4.6 Grafické prvky a jejich formáty

Pokud se rozhodneme zejména z estetických důvodů použít v naší prezentaci větší množství grafiky (přestože to není zrovna vhodná volba, jak jsme se již zmínili), vyvstává otázka, v jakém formátu tuto grafiku vytvořit. K dispozici dnes máme několik možností, z nichž pro účely webové grafiky se stávají nejvhodnějšími alternativami formáty PNG, GIF a JPEG. Každý z těchto formátů může plnit různé účely a není problém kombinovat jejich použití na webové stránce. Velmi stručně se zmíníme o některých vlastnostech těchto formátů a o příkladech jejich užití.

Nejdříve se začneme zabývat zřejmě stále ještě nejrozšířenějším formátem, kterým je GIF[27]. Jako jediný z webových formátů umí implementovat animace[28], díky čemuž se hojně používá při tvorbě reklamní grafiky, tzv. bannerů. Má však některá další omezení. Interně lze použít v obrázku nejvýše 256 barev, což automaticky vyřazuje použití tohoto formátu pro detailnější grafiku, která vyžaduje přinejmenším alespoň 16-bitovou barevnou hloubku. Další nevýhodou je stále ještě někde patentovaný mechanismus komprese LZW, který neumožňuje rozsáhlé používání animací v nástrojích pro tvorbu grafiky. K výhodám GIF-u lze přičíst postupné natahování obrázku (tzv. interlacing) a jednostupňovou transparentnost, díky čemuž je možné vytvářet i obrázky s průhledným pozadím. Tento formát je tedy více než vhodný pro použití grafiky s malým počtem barev a pro obohacení grafické stránky webu o dynamické animace a o transparentnost. Navíc téměř všechny webové browsery implementují zcela specifikaci GIF-u.

Nevýhodu spočívající v použití malého množství barev odstraňuje formát JFIF/JPEG[29] (dále jen JPEG). Tento formát se složitou specifikací umožňuje použití 24-bitové barevné hloubky[30] a navíc velmi významně zmenšuje datovou velikost souborů, což je hlavní důvod, proč je tento typ grafiky tak hojně používaným. Malé přenosy grafických dat umožňují přenášet data rychleji i na pomalých internetových linkách, avšak na úkor ztrátovosti grafických informací. Postupné natahování souborů je realizováno podobně jako u GIF-u, tzv. metodou progressingu, který podporuje též většina internetových browserů. Bohužel tento formát zase neumí realizovat průhlednost.

[27] Graphics Interchange Format
[28] Konkrétně formát GIF89a, starší formát GIF87a nemá tuto možnost
[29] Joint Photographic Expert Group (JPEG) File Interchange Format
[30] Bohužel však jen této barevné hloubky, která představuje použití přibližně 16 5 mil. barev

Třetím a zároveň nejnovějším webovým formátem grafických souborů se stává formát PNG[31]. Úkolem tohoto typu obrázků je nahradit oba předešlé, neboť oproti JPEG realizuje bezztrátovou kompresi dat a navíc implementuje novou schopnost, a to 256stupňovou transparentnost, která odstraňuje tzv. halo efekt u průhledného GIF-u[32]. Bohužel PNG neumožňuje zobrazit animace tak jako GIF a velikosti PNG souborů jsou také o dost větší než u GIF-u nebo formátu JPEG[33]. Podpora PNG v internetových prohlížečích není stále ještě úplná.

Asi by bylo správné zmínit ještě o formátu MNG a JPEG2000, které se možná v budoucnosti více rozšíří i na webových stránkách.

V posledních letech se kromě obyčejných obrázků, které tvoří webovou grafiku v prezentacích firem, objevují i nové technologie, které úplně nebo zčásti zatracují tradiční HTML model webových stránek a poskytují nové uživatelské rozhraní. Problémem těchto technologií je zatím nepříliš velká podpora na klientských počítačích.

To se už téměř netýká formátu Macromedia Shockwave Flash, který se už možná za pár let stane všeobecně přijímanou technologií pro alternativní zobrazování webového obsahu. Tato technologie umožňuje přinášet do webu dynamické a graficky velmi dobře obohacené prvky. Zatím se použití této technologie prosazuje jen na určitých operačních systémech, lze však v budoucnu očekávat i rozšíření na jiné platformy, čímž by se mohl formát stát webovým standardem.

Paralelně s technologií Flash se vyvíjí už roky i ActiveX komponentní technologie firmy Microsoft, která však asi nikdy nemůže být všeobecně použitelná ve webových prezentacích, a to především z důvodu zaměření se jen na operační systémy Microsoft Windows a také proto, že nerespektuje často ani ty nejzákladnější bezpečnostní prvky, což má za následek velmi časté zneužívání ActiveX k napadání systémů Windows nebo ke ztrátě důvěrných dat uživatele. ActiveX umožňuje kromě napadání těchto systémů i velmi kvalitní vzájemnou spolupráci při vytváření dynamických prvků webových stránek, díky čemuž lze dosáhnout velmi pozoruhodných grafických efektů.

Možnosti obohacení webových stránek o grafický obsah tímto nejsou zdaleka vyčerpány, ale kromě DHTML technologií už plní více specializované funkce, které se při implementaci internetového obchodu stěží využijí.

[31] Portable Network Graphics

[32] Efekt, který vzniká při jednostupňové průhlednosti, kdy se okraje průhledného obrázku někdy vyplňují pixely jiné barvy

[33] Přestože implementuje i rozšířenou kompresi dat

1.4.7 Vazba na propagační prvky organizace

Asi posledními úkoly designéra je při realizaci designu internetového obchodu využít firemních znaků, symbolů a barevných schémat, které budou jednoznačně spjaty s podnikem, jeho marketingovou koncepcí a propagačními prvky. Tyto prvky pak na stránce zosobňují podnikové znaky a působí i jako reklama.

Jako příklad využití podnikového barevného schématu v internetové aplikaci lze demonstrovat internetový obchod a prezentaci české firmy LOSAN, s.r.o.[34]

1.4.8 Design – konečný výsledek

Pokud se při vývoji designu obchodu řídíme všemi dříve zmíněnými pravidly a tipy, je úspěšná tvorba designu obchodu již téměř zajištěna. Vytvoření celkového vzhledu webové aplikace, informační architektury a veškerých dalších funkčních rozšíření není jednoduchá záležitost, proto ji nemůže dělat kdokoliv. Klade na tvůrce velké nároky, a proto je tak obtížné na internetu najít dobře zvládnutý internetový obchod či jinou webovou prezentaci. Každý web má své klady a také zápory a při podrobném a profesionálnějším pohledu na jakýkoliv z nich lze najít alespoň několik nedostatků, začínajících obvykle od drobných chyb v grafické úpravě či nedostatkům ve funkčnosti až k naprosto špatně napsanému kódu, který zdaleka neprojde žádným validátorem kódu[35] a je tedy nevhodný pro zobrazení ve všech běžných prohlížečích, či je dokonce určený pro zobrazení jen na jednom typu webového prohlížeče.

Implementátor internetového obchodu, má-li dostatek času, by se měl zabývat alespoň trochu o takové oblasti, jako je výtvarné umění, typografie, programování, či o design jako takový a všímat si věcí okolo sebe, které ho mohou při tvorbě designu inspirovat. Zejména tím myslím reklamu, ve které jsou prvky designu také velmi důležité a rozhodují o obrovských či malých příjmech podniků. Podaří-li se takovému tvůrci sladit všechny prvky dokonalého designu, vytvoří internetový obchod, který bude daleko úspěšnější než u konkurence. A to je přeci cílem každého podniku.

[34] `http://www.losan.cz`
[35] Program, který kontroluje správnost kódu webové stránky

1.5 Náležitosti internetového obchodu

V této krátké kapitole nastíním základní prvky, které by při realizaci internetového obchodu neměli chybět. Samozřejmě se zde ale budu hlavně zabývat prezentační a implementační stránkou věci, tj. tou, kterou vnímají zákazníci. Podnikové a jiné zázemí pro správnou funkci internetového obchodu je ve velké míře v režii daného podniku a je tedy v praxi velmi různé a navíc není účelem této práce se jím zabývat. Přesto toto „zázemí“ značně ovlivňuje výslednou podobu internetového obchodu, neboť každý podnik má zájem mít internetový obchod podle svých představ.

1.5.1 Unifikace ?

Nejdříve si však musíme říci, že do dnešní doby neexistuje žádná konkrétní a standardizovaná koncepce pro implementaci internetových obchodů, kterou by všichni respektovaly. Je to částečně způsobeno tím, že je internetové obchodování stále ještě nový fenomén a částečně také kvůli různým požadavkům a představám podniků o jeho podobě. V konečném důsledku tak neexistuje ani žádný unifikovaný systém hodnocení a z toho vyplývá i uplatňování značně subjektivního hodnocení kvality a funkčnosti internetových obchodů. Situace je natolik špatná, že je celkem běžné na internetu pozorovat, jak tuto funkci přejímají ostatní, ve velké míře naprosto neerudovaní a ještě dokonce anonymní lidé.

Je-li vyžadována nutnost určité standardizace, existují normy a standardy, které lze zejména za účelem zabezpečení aplikace splňovat. Tyto normy podrobněji zmíníme v kapitole věnované bezpečnosti internetového obchodu.

Je potřeba také navíc zmínit, že určitá pravidla již určují naše dnes platné zákony, zejména Občanský a Obchodní zákoník, dále pak Zákon na ochranu osobních údajů, Zákon o elektronickém podpisu a další právní normy. Navíc jak již bylo zmíněno, existují návrhy zákonů, které budou ještě více upravovat a přidávat nezbytné náležitosti a povinnosti.

Přestože existují organizace, které se i tímto hodnocením, popř. unifikací zabývají, nejsou obvykle respektovány tak jako například normy ISO 9000. A je k tomu určitě důvod, neboť počet těchto organizací je zejména ve Spojených státech příliš velký, což vede k situaci, že se internetové stránky obchodů plní různými certifikáty kvality, v lepším případě málo známých organizací, což pak působí značně nepřehledně, i když to zřejmě plní svůj účel – tedy uměle zvýšit hodnotu a kvalitu obchodu v očích zákazníka. V konečném důsledku se tak plní internetové stránky těchto organizací pomyslnými žebříčky nejlepších obchodů, což až nápadně připomíná situaci v moderním boxu, kdy se každoročně vyhlašují desítky „mistrů světa“ ve stejné váze.

Tato situace je zřejmě delší dobu nemožná, protože opět – stejně jako mnoho jiných faktorů – snižuje důvěryhodnost v internetové obchodování, která je velmi křehká.

V našich podmínkách není zatím situace ještě natolik nepřehledná jako ve Spojených státech, ve skutečnosti se počet takových organizací u nás dá spočítat na prstech jedné nebo obou ruk. Nejvýznamnější a trochu známou organizací, která vydává pro české internetové obchody osvědčení (certifikáty) kvality, je **Asociace pro elektronickou komerci APEK** [22, APEK], která byla založena za tímto účelem v roce 1999. Organizace vydává certifikáty označené souslovím „Nákup bez obav“. Hlavním účelem této organizace je certifikovat obchody, které lze považovat za „bezrizikové“ pro zákazníka a hlavní moto je více než vystihující podstatu věci:

„Míra rizika při nakupování by neměla být nikdy větší, než míra ochoty nakupovat!“

Při hodnocení kvality obchodu budu i já v této práci částečně vycházet z certifikačních pravidel této organizace.

1.5.2 Informace o podniku

Největší výhodou při podnikání na internetu je víceméně dost výrazná anonymita. Ačkoliv se to může zdát v případě internetového obchodu jako zcela nevhodná a přinejmenším zákonu odporující vlastnost, stále ještě existuje. Internet byl před vznikem prvních internetových obchodů jen jakási džungle, kde nikdo nikoho nevidí a nemůže nikoho kontrolovat. Dnešní skutečnost je poněkud jiná, ale nejvíce je to patrné právě v oblasti internetového obchodování. Nejenže je technicky možné za vyložení různého úsilí vyhledat téměř kohokoliv na Internetu, navíc je tu legislativa, která takové chování v případě internetových obchodů považuje za porušení zákona.

Mělo by být naprostým pravidlem **ignorovat internetové obchody, které** o svých aktivitách, sídle a jiných údajích **nepodávají** žádné, strohé, neúplné či mylné **informace**. Zákazník si nemůže být jist, zda mu pak objednaný výrobek vůbec někdy přijde, zda při dobírce na poště nezaplatí nehoráznou finanční sumu za prázdný nebo nekvalitní obsah balíku, zda má provozovatel internetového obchodu způsobilost k právním úkonům, zda má živnostenský list nebo jiné podnikatelské oprávnění atd. Může se tak snadno stát, že vás okrade třeba i 16ti-letý kluk, který kromě každodenního vysedávání u počítače pilně studuje učební obor „zámečník“. Je potřeba při nakupování na internetu – stejně jako v jiných případech – především používat mozek, čímž se dá vyhnout mnoha problémům.

Pokud jsme zmínili Návrh zákona o službách informační společnosti, tak ten taxativně definuje nově náležitosti, které o sobě podnik *prostřednictvím některého prostředku komunikace na dálku* musí poskytnout před uzavřením kupní smlouvy.

Zde je zestručněný a neúplný výčet těch informací o podniku, které se netýkají konkrétního výrobku nebo služby:

- Obchodní jméno, identifikační číslo, sídlo právnické osoby, bydliště v případě fyzické osoby
- Údaj o zápisu do obch. rejstříku nebo jiné evidenci
- Údaje o kontrolním orgánu v některých případech
- Název profesního sdružení v některých případech
- Zajištění trvalého přístupu k těmto informacím

Není potřeba nijak zvlášť zdůrazňovat, že většina internetových obchodů dnes nenaplňuje všechny tyto budoucí požadavky včetně těch, které jsem zde záměrně pro stručnost neuvedl. Většina lepších obchodů však již splňuje požadavky platné nyní podle občanského zákoníku a jiných právních norem, ostatní údaje se stanou nutností až po případném uvedení zákona v platnost.

Mělo by být však slušností a také určitým marketingovým nástrojem poskytnout nejen tyto povinné, ale také jiné informace o podniku. Zejména jde o zmínění vedlejších aktivit společnosti (podniku), výčet referencí a spolupracujících firem, základní cíle a směřování podniku a podobné informace, které mohou značně vylepšit mínění potenciálního zákazníka o daném podniku. Samozřejmě jiné informace bude poskytovat prezentace výrobního, a jiné podniku orientovaného na obchod. V žádném případě se nevyžadují citlivé nebo dokonce informace podléhající obchodnímu tajemství podle zákona.

Množství informací o podniku zveřejňovaných na konkrétní webové stránce má být malé, aby příliš nezatěžovalo čtenáře. Toho obyčejně při čtení těchto informací nezajímají v tu chvíli marginální informace o dodacích podmínkách a jiných konkrétních záležitostech, které mají být soustředěny na jiném místě, a navíc mu stačí pár řádek nebo pár desítek řádek textu, nikoliv několik desítek kB pro něj už naprosto zbytečných dat. Je zajímavé, ale snadno vysvětlitelné, že většina prezentací výrobních podniků tento postup uplatňuje a kolik i významnějších internetových obchodů své zákazníky otravuje balastem nedůležitých a na daném místě nezajímavých dat, které vedou čtenáře k tomu, že radši tyto informace přestanou číst, i když o ně měli původně zájem. Těžko je to záměr provozovatele kvalitního internetového obchodu.

Účelem poskytnutí těchto informací je zvýšit důvěryhodnost a prestiž internetového obchodu, která má přímo strategickou důležitost. Nejsou-li tyto informace, zákazník už hodnotí pouze vzhled a funkčnost obchodu a jiné věci, podle kterých se rozhodne, zda danému obchodu

důvěřovat nebo ne. Jak jsem již zmínil, takovému obchodu je podle mého názoru lépe se vyhnout, a pokud existuje podezření z nekalé činnosti provozovatele webové prezentace, je lépe upozornit na to příslušné orgány. Protože však zatím tyto orgány nemají nástroje a vůli se tímto příliš zabývat, nezbývá než si počkat na potřebnou aktivitu těchto orgánů až do doby, kdy to možné bude, což v rámci povinností po našem vstupu do Evropské unie bude snad poměrně brzy.

1.5.3 Kontaktní informace

Kontaktní informace uváděné na webových stránkách internetového obchodu mohou nabývat několika podob, od textových v podobě korespondenčních adres, faxových či telefonních čísel na jedné straně uváděných společně s informacemi o podniku až k pokročilým a např. interaktivním CRM[36] systémům u podniků kladoucích důraz na marketingovou činnost.

Nejčastějším způsobem uvádění kontaktních informací je prosté uvedení adresy sídla podniku či bydliště podnikatele doplněné např. o emailovou adresu pro případné dotazy. Pro velkou většinu internetových obchodů s malým obratem je to dostačující. Stačí tak pro odpovídání na dotazy zákazníků, vyřizování a potvrzování objednávek a pro jinou podporu zákazníkům vyčlenit jen jednoho či několik zaměstnanců, kteří přijímají a odpovídají na emaily, a k tomu je obyčejně nutné vytvořit alespoň jednoduchý způsob obsluhy objednávek pomocí webového nebo jiného aplikačního rozhraní. Tito zaměstnanci pak předávají k vyřízení závazné objednávky jiným zaměstnancům podniku.

V souvislosti s udáváním emailových adres je zajímavé zmínit, že se dodnes nijak neupravuje skutečnost, kdy se pro jednotlivá pojmenování emailových kontaktů používají často jména a příjmení zaměstnanců. Někdo to považuje za nemorální, závadné nebo v rozporu se zákony, zatímco jiní proti tomu nic nemají. Toto se týká nejen internetových obchodů, ale i státní správy on-line. V některých místech světa je toto názvosloví poštovních schránek zakázáno a jména či příjmení zaměstnanců se nesmí v kontaktních emailových adresách objevovat.

Kromě jednoduchých emailových adres je časté používání webových formulářů pro zasílání připomínek zákazníků a v neposlední řadě se používají i modernější způsoby interaktivní komunikace zejména prostřednictvím klientů sítí ICQ, IRC, AOL, Yahoo, MSN, Jabber, Talk a jiných, čímž se už značně přibližují způsobům užívaných při realizaci pokročilých CRM systémů, které nalézají uplatnění pouze ve velikých marketingově orientovaných firmách.

[36] Customer Relationship Management – systém řízení vztahů se zákazníky, někdy označované za zákaznické systémy či věrnostní systémy

1.5.4 Registrace a přihlašování klientů

Na rozdíl od kamenného obchodu, ve kterém se zákazník nemusí představovat prodávajícímu, je „představení se“ v internetovém obchodě nutností, aby mohla být korektně uzavřena smlouva o koupi věci nebo služby. Tato nutnost vyplývá z neexistence osobního kontaktu při uzavírání smlouvy na dálku. Webová aplikace zastřešující internetový obchod a dynamicky reagující na jednání zákazníka za počítačem musí mít určité minimální rozlišovací údaje, aby mohla jednoho anonymního zákazníka odlišit od jiného. K tomu slouží zejména zadání uživatelského jména a hesla.

Mechanismů, kterými je možné se přihlásit k internetového obchodu je několik[37], přesto se používá ten nejméně zabezpečený, tj. prostřednictvím webového formuláře, do kterého uživatel napíše své uživatelské jméno a heslo a pošle ho často v nezašifrované nebo dokonce i nekódované podobě.

Ačkoliv neexistuje zatím alternativa k tomuto procesu objednávání zboží, považuji ho za značně nedokonalý. Pokud totiž člověk navštěvuje více obchodů najednou, musí si za optimálních a bezpečných podmínek zapamatovat takové údaje jako je přihlašovací jméno a heslo, popř. další údaje, pokud to webová aplikace vyžaduje a nejsou tyto údaje pro danou osobu vždy stejné. To klade na zákazníka zbytečně velké požadavky a odrazuje ho v registraci ve více obchodech. V horším případě se takový zákazník začne chovat tak, že se na všech místech registruje pod stejným uživatelským jménem a heslem a nebo či zároveň si dokonce zaznamenává citlivá data na místa, ke kterým má někdo jiný přístup, což je z bezpečnostního hlediska naprosto nevyhovující. Při vyzrazení hesla je tak možno danému člověku uškodit v daleko vyšší míře, pokud je to účelem potenciálního útočníka. A to například tím, že si při zaregistrování jeho jménem můžeme objednávat na jeho účet desítky výrobků a oprávněnému uživateli tak můžeme přinést potíže nebo dokonce i výraznou škodu. Konkrétněji a podrobněji toto téma rozebereme v kapitole věnované bezpečnosti. Už nyní ale řeknu, že možností jak řešit tento problém je velmi málo a problém jako takový nelze vyřešit zcela.

1.5.5 Katalog výrobků

Katalog výrobků tvoří zřejmě nejdůležitější součást internetového obchodu. Jeho úroveň a funkční možnosti vnímá zákazník jako nejvýznamnější při celkovém hodnocení daného obchodu.

[37] Basic Authentication, Digest Authentication, Integrated Windows (NTLM Authorization), Negotiate, Kerberos, SSL, Microsoft Passport

Každý internetový katalog by měl obsahovat sortiment rozdělený do jednotlivých kategorií pro lepší navigaci zákazníka. Další funkcí by měla být možnost náhledu vlastností jednotlivého výrobku tak, aby zákazník měl o výrobku nezbytné a úplné údaje. Těmito náležitostmi by měly být zejména:

- Název a základní charakteristiky zboží nebo služeb
- Cena zboží nebo služeb včetně všech daní a poplatků, jsou-li k ceně připočítávány
- Náklady na dodání
- Doba, po kterou zůstává nabídka nebo cena v platnosti
- Záruční doby, pokud se odlišují od zákonné lhůty
- Na co se záruka vztahuje, případně nevztahuje

Zejména v oblasti uvádění rozsahu záruky je potřeba významnější implementace funkční stránky e-shopu. V případě větších obchodů tyto náležitosti lze obtížně uvádět u každého výrobku nebo služby a vyžaduje to větší množství práce personálu.

Z katalogu nebo z místa náhledu charakteristik by měl vést přímý odkaz na přidání do nákupního košíku, pokud není funkcionalita řešena jiným způsobem.

1.5.6 Nákupní košík

Stejně jako v případě běžného obchodu je nutné nakupované zboží[38] soustředit do nákupního košíku. V případě virtuálního e-obchodu je toto nutné zejména z důvodu čistě implementačních, nikoliv jako v případě kamenného obchodu, kde má funkci usnadňující přenos zboží k pokladně.

Význam virtuálního košíku je tedy trochu odlišný od běžného, má za účel soustředit informace o nakupovaném zboží, o jeho množství, popř. dalších náležitostech nutných pro nákup v daném obchodě. Zákazníkovi by měla být určitě umožněna možnost prohlížet obsah nákupního košíku, který by kromě údajů o výrobcích a jejich množstvích měl obsahovat i plné ceny. Konečně by měla implementace košíku vypočítávat konečnou souhrnnou cenu k zaplacení.

Vysypání obsahu košíku by mělo být taktéž nezbytnou součástí, aby zákazník nemusel odstraňovat výrobky z košíku jednotlivě. Stejně jako v případě katalogu výrobků by měl vést přímý odkaz ze stránky zobrazující nákupní košík na následující krok, čímž je konečná objednávka.

[38] V případě internetového obchodu i služeb

1.5.7 Realizace objednávek

Závazné objednání výrobků obsažených v nákupním košíku je posledním nutným krokem k uzavření obchodu mezi námi a internetovým obchodem. Musí mít své náležitosti, které byly zmíněny výše. Má obvykle podobnou strukturu jako znázornění nákupního košíku. Kromě těch zmíněných náležitostí jsou potřeba i další náležitosti, které nám určuje zákon (jeho návrh) a s objednávkou zboží nebo služeb souvisí. Zejména musí být uvedeny tyto náležitosti:

- Způsob platby, dodání nebo plnění
- Poučení o právu na odstoupení (s určitými výjimkami)
- Náklady na použití komunikačních prostředků na dálku

V době realizace objednávky musí být uživateli jasno, jakým způsobem bude zboží doručeno, znát plnou cenu za výrobky včetně daní a poplatků, znát možnosti reklamace, podmínky uplatnění záruky, metody plateb, problematiku stornování dodávky, výše poštovného a jiných poplatků a další nezbytné údaje. Na tyto údaje[39] by podle certifikace organizace APEK měly vést viditelné odkazy hned z úvodní stránky obchodu. Také by mělo být zmíněno[40] při realizaci objednávky nebo na jiném místě webové aplikace, že údaje poskytnuté obchodu budou sloužit jen pro účely obchodu a že nebudou poskytnuty třetím osobám či jinak použity v rozporu se zákonem. Konkrétní právní normou pro posuzování této problematiky je poměrně nový Zákon o ochraně osobních údajů.

Tímto však ještě povinnosti obchodu nekončí. Zboží poslané např. poštou musí splňovat další věci, mezi kterými je hlavní existence daňového dokladu u zásilky, dále pak dodací a popřípadě záruční list.

V praxi je splnění těchto a i dalších zde nezmíněných kritérií poměrně obtížné a jen málokterý internetový obchod je schopen je zaručit. Důvodem je zejména snaha minimalizovat náklady na provoz obchodu, což je jedním z hlavních stimulů pro vývoj elektronické komerce.

Na jedné straně je tak v ekonomickém prostředí internetu cítit snaha o rozvoj internetového podnikání, ale na druhé straně je brzděna některými novými povinnostmi, které internetové obchodování staví do pozice stále méně výnosnějšího podnikání. Cílem je prosadit stejné nebo velmi podobné podmínky pro internetové zákazníky, které požívají v pozici zákazníka v běžném kamenném obchodě.

[39] Jde o tzv. nákupní řád
[40] A bude to zřejmě zanedlouho i zákonnou povinností

1.5.8 Internetově orientované platební systémy

Jestli existuje nějaká výrazná bariéra bránící výraznějšímu vývoji internetového obchodování, elektronického bankovnictví a jiných moderních přístupů využívajících počítačové sítě a moderní informační technologie, pak je soustředěna zejména v oblasti zabezpečování finančních plateb na dálku.

Obecně se dá říci, že zákazník ze své podstaty nedůvěřuje moderním systémům plateb přes Internet. Důvodů není mnoho, ale ten jeden hlavní je nejdůležitější. **Zákazník** neví, jakým způsobem je platba zajišťována, a ze strachu vyplývajícího z neznalosti a z negativních zkušeností poškozených zákazníků **si** tak **není jist bezpečností takové platby**.

Situace by se dala srovnat s rozmachem bankovního sektoru. V dobách, kdy se neuplatňovala žádná měnová politika a bank bylo velmi málo a poskytovaly jen základní služby, nebyl majetný člověk příliš motivován[41] k úschově svých disponibilních zdrojů do banky, což vedlo k velké tezauraci finančních prostředků. S postupem doby však zjistil, že mu to obvykle přinese výhody v podobě snížení transakčních nákladů a postupem času se projevilo i zmenšení rizika ztráty takto vloženého kapitálu.

Dnes je situace podobná. Zákazníci drží své peníze v běžných komerčních bankách a cítí se, že je mají obvykle v bezpečí. Uplatnění informačních platebních systémů jim taktéž přinese snížení transakčních nákladů a v neposlední řadě i ušetří čas nutný k návštěvě bankovní přepážky. Jako příklad lze uvést rozšíření uplatňování bankomatů, které značně ulehčili obyvatelům život. V případě internetových a jiných elektronických plateb je však nedostatečná bezpečnost příliš demotivujícím faktorem.

Důvěryhodnost bank je pro banku strategická a pečlivě se o ní banka stará. V případě elektronických plateb však potenciální zákazník neví a v mnoha ohledech ani nemůže vědět, zda je tato platba bezpečná, neboť Internet nebyl v dobách svého vzniku a ani v několika dalších desetiletích určen k provozování zabezpečené komunikace a zákazník nemá dostatek informací k tomu, aby dokázal posoudit rizika. Na Internetu jsou tisícovky lidí, kteří mají nekalé úmysly a jsou vyzbrojeny často obrovským technologickým know-how, které jim umožňuje nalézat slabiny v informačních systémech a počítačových sítích. Při odhalení nějakého bezpečnostního nedostatku jsou schopny velmi brzy tohoto svého poznatku využít ve svůj prospěch, který obvykle vede v neprospěch zákazníků důvěřujících těmto pro něj „Black-box“ platebním systémům.

Důsledkem je, že se velmi často při platbě za zboží v internetových obchodech využívá standardních a bezpečnějších prostředků. Těmi jsou poštovní dobírka či platba poštovní složenkou či platba příkazem k úhradě u bankovní přepážky. U těchto plateb je totiž provozovatelem

[41] A nebyl ani přesvědčen o smyslu takového jednání

zajištěna záruka doručení platby a případné vyhovující reklamační řízení při problémech s platbou. V případě platby přes Internet je tato záruka velmi diskutabilní právě z důvodu vlastností počítačových sítí. Případná chyba či manipulace při přenosu elektronických dat potvrzujících finanční transakci vede často i ke ztrátě informací důležitých pro reklamaci.

Situace se výrazně zlepšuje s tím, jak se vyvíjejí zabezpečující technologie. Už není možné tak jako ještě před pár lety poslat nezabezpečený email s příkazem k úhradě bance. Dnes již existuje informační infrastruktura určená k přenosu zabezpečených dat a jsou vyvíjeny sofistikované platební systémy a jejich aplikace, které mají útokům zvenčí zabraňovat. Nakolik jsou úspěšné a přesvědčivé se dá usoudit z rozšířenosti jejich použití, z množství jejich prolomení a finančních ztrát, které však banky a další instituce z důvodu ztráty své důvěryhodnosti neuveřejňují.

Co se týče konkrétní implementace určitého platebního systému do funkční struktury internetového obchodu, je vlastní implementace velmi obtížná, a proto se spíše využívají provozovatelem systému vytvořená aplikační rozhraní, pokud existují. Nejčastěji využívaným systémem elektronické platby prostřednictvím platební karty je zřejmě systém založený na **protokolu SET**[42]. Platba platební kartou za zboží v internetovém obchodě je u nás velmi málo rozšířena a mikroplatební systémy ze zákona zakázány. Ostatní možnosti plateb jsou méně zabezpečené a méně standardizované, což je automaticky vyřazuje z běžného používání. Mezi tyto systémy obyčejně patří plno implementací plateb virtuálními penězi a jiné hybridní systémy vycházejících z elektronického bankovnictví.

1.5.9 Doprovodné služby a možnosti rozšíření funkcionality

Kromě zde zmíněných a víceméně nezbytných součástí internetového obchodu se snaží provozovatel takového obchodu poskytovat i jiné služby, které mají zejména ulehčit zákazníkův život a také rozšířit prosté zajištění obchodu o další funkcionalitu, která se dá obchodníkem využít k lepší propagaci.

Zapomenutí přístupového hesla, bezpečnostní problém

Při dnešním množství webových stránek, které vyžadují autentifikaci, se nemůžeme divit, že je těžké pro potenciálního zákazníka našeho obchodu zapamatovat si své přístupové údaje do našeho obchodu. Realizací služby změny hesla nebo zaslání hesla elektronickou poštou lze odstranit případné emailové žádosti o zjištění hesla a uživatelského jména zákazníka směrované našemu podniku, které totiž vyžadují větší pracovní nasazení obsluhujícího personálu.

[42] Secure Electronic Transactions

Způsobů, jak tento problém vyřešit k úplné spokojenosti zákazníka je mnoho. Zde si uvedeme ta nejčastěji využívaná a podíváme se ně také z pohledu bezpečnosti obchodu. Je totiž nutné si uvědomit, že je zde obchod nejzranitelnější. Stačí potenciálnímu útočníkovi zjistit heslo a přihlašovací jméno našeho zákazníka a na jeho účet objednávat zboží či provádět změny v uživatelském nastavení, popř. zjistit, co si daný uživatel kdy objednal a za jaké peníze.

Způsob, který spočívá v jednoduchém zobrazení hesla ve webovém prohlížeči při správné odpovědi na určitou otázku[43], je naprosto nepřijatelným, přesto ještě někde používaným mechanismem. Absolutně nerespektuje bezpečnost a takové heslo je obvykle možné velmi snadno odhalit, jsou-li navíc údaje požadované webovou aplikací veřejně dostupné nebo známé. Navíc jde takové heslo fyzicky odpozorovat i z monitoru počítače.

Druhým, dnes už méně využívaným způsobem, je prosté zaslání hesla v nezašifrované podobě prostřednictvím elektronické pošty na adresu, kterou zákazník při registraci v obchodě musel uvést. A na tuto adresu je mu zaslán email s jeho heslem. Každému je jistě jasné, že tento způsob je velmi nebezpečný a rozhodně je velmi snadno zneužitelný, neboť se emailová zpráva prostřednictvím poštovních serverů a jiných aplikací na Internetu šíří obvykle v nekódované podobě přes neznámé počítače a síťová zařízení. Je-li alespoň jeden z nich napaden útočníkem, může toto heslo útočník odposlechnout na síti. Stačí obvykle na napadeném stroji, kudy chodí pošta, nainstalovat trojského koně[44], který bude například v přenášených emailových zprávách vyhledávat slova "pass", "password" či jejich ekvivalenty v mnoha jazycích a hned je možné toto heslo zneužít k neoprávněnému přístupu do obchodu.

Další způsob využívá při požadavku zákazníka na změnu či obnovu hesla generování jedinečného URL[45] odkazu, obvykle platného jen pár hodin či minut, který je přenášen také nezašifrovaně poštovní zprávou. Pokud se v jedinečném odkazu zakomponovává např. některý údaj, který útočník odposlouchávající provoz nemůže znát (např. IP adresu), pak klademe útočníkovi daleko větší překážku k prozrazení hesla. Zákazník kliknutím na internetový odkaz v emailové zprávě dostane speciální stránku určenou pro obnovení či změnu hesla daného uživatele. Samozřejmě není tento systém také neprolomitelný, při útočníkově dokonalé kontrole nad počítačem provozovatele obchodu nebo jeho poskytovatele webového prostoru je možné i tento způsob obvykle prolomit. Je to jen o moc obtížnější a také často časově náročnější. Tento způsob je použit v mé implementaci internetového obchodu. Opět je třeba říci, že nesmí být v žádném případě heslo zobrazeno v okně webového prohlížeče, neboť by se dalo kupříkladu zjistit v cache proxy serveru nebo by mohlo být odposlechnuto na síti v reálném čase.

Asi nejméně užívaným a nejvíce zabezpečeným způsobem je poslání kódované či šifrované emailové zprávy, ve které je umístěn jedinečný (tedy i kódovaný) odkaz na webovou stránku,

[43] Například na rodné číslo nebo den narození zákazníka
[44] Počítačový program provádějící před uživatelem počítače skrytou činnost
[45] Uniform Resource Locator – adresa sloužící k odkazování na dokumenty na internetu

na které se zákazníka ptáme na kontrolní otázky, které uvedl na webové stránce při registraci z bezpečnostních důvodů. Tento způsob je sice útočníkem při dodržení určitých dalších principů na straně serveru, téměř neprolomitelný, nejvíce však „obtěžuje“ zákazníka. Obvykle se tento mechanismus používá v souvislosti s registrací elektronického podpisu (certifikátu) prostřednictvím internetu.

Paralelně s těmito způsoby zabezpečení nevyzrazení hesla komukoliv se využívá šifrovaného zabezpečeného připojení SSL/TLS[46] pro přístup k internetové stránce. To by dnes mělo být standardní opatření. Opět však zde neplatí, že se i tento způsob nedá zneužít k útokům. Navíc dnes ještě není tento způsob zabezpečení dostatečně implementován u poskytovatelů webhostingových služeb.

Rozesílání bulletinů

Služba pravidelného rozesílání bulletinů může být pro internetový obchod poměrně významným způsobem, jak zákazníkovi připomenout jeho existenci a popřípadě jak upozornit na novinky v obchodě. Toto rozesílání by ale mělo být potvrzeno zákazníkem např. během registrace, nemělo by být rozesíláno nevyžádaně a v každém případě by mělo být zákazníkovi umožněno zrušit jeho zasílání do své emailové schránky.

Bulletiny a jiné podobné dokumenty by neměly mít velký informační obsah, jejich účelem je pouze objasnit novinky a služby, které může zákazník u našeho obchodu využít a neměly by plnit další funkce, které jsou náplní reklamy na výrobky.

Upozorňovací emaily, reklama, spam

Kategorie emailů upozorňujících na slevy výrobků a služeb a na nové výrobky se řadí velmi často do tzv. **nevyžádané pošty** (dále jen spam). Pokud si tímto způsobem obchod zajišťuje reklamu, mělo by to být vždy v přiměřené míře, aby to neobtěžovalo zákazníky. Zřejmě tedy tři emaily denně s reklamou na nové CD od Britney Spears asi nebude to správné množství. Není pro člověka nic horšího než když se denně musí probírat desítkou zavirovaných emailových zpráv určených pro napadení operačního systému počítače a desítkou nevyžádaných zpráv od neznámých odesílatelů s obsahem, se kterým nechce mít nic společného.

Opět jako v případě jiné – často nevyžádané – elektronické pošty, musíme dbát o našeho zákazníka a nezatěžovat ho věcmi, o které nemá žádný zájem. To je však velký problém, pokud

[46] Secure Sockets Layer/Transport Layer Security protocol

jeho preference neznáme. Musíme mu umožnit si případné zasílání reklamy z našeho obchodu zakázat, a pak toto jeho rozhodnutí respektovat.

Je potřeba si navíc uvědomit, že spolu s naší reklamou může náš zákazník denně dostávat další nezjištěné množství nevyžádané pošty, což může vést k tomu, že si naší reklamy ani nevšimne. V těchto případech je naše reklama úplně zbytečná. Také nevíme, zda náš zákazník nemá aktivován na svém počítači či u jeho poskytovatele emailových služeb filtr pro spam. Pak se k němu tato pošta ani nemusí dostat. Určitě tedy není reklama prostřednictvím elektronických zpráv tolik účinná jako v případě reklamy v masmédiích, novinách, časopisech atd. Snadnost rozesílání takové reklamy a téměř zanedbatelné náklady s tím spojené určitě nejsou důvodem, proč svého zákazníka odrazovat.

Ankety, uplatnění data-miningu

Ankety na stránkách internetového obchodu plní velmi významnou funkci v získávání informací, které se jinak složitě zjišťují přes dotazníkové nebo jiné výběrové metody. Vhodně zvolenou otázkou v anketě se můžeme dozvědět konkrétní požadavky velké skupiny našich zákazníků. Nevýhodou však naopak bývá zjevná statisticky pojatá vychýlenost odhadu zákaznických názorů, protože není zajištěno, že v naší anketě budou odpovídat „průměrní“ zákazníci.

Ačkoliv v této práci bude později ještě zmíněno téma dolování dat (data-mining) podrobněji, řekneme už teď, že plno nových prvků webových aplikací, mezi něž lze zařadit částečně i ankety, blogy a jiné, jsou významným a nevyčerpatelným zdrojem informací a základem pro uplatnění moderních přístupů a metodologií užívaných při dolování dat[47], které mají široké využití v obchodě, zejména v marketingu. Ostatně každý CRM systém lze také k těmto účelům využít.

Princip dolování dat je poměrně novým interdisciplinárním přístupem použitelným k mnoha účelům a spočívá v *procesu netriviálního získávání implicitní, dříve neznámé a potencionálně užitečné informace z dat* [26, Sarmanova02]. Dolování dat může být velmi zajímavým přístupem, jak z obrovského množství dat o návštěvnosti stránek internetového obchodu konkrétněji zjistit konkrétní preference zákazníků, dobu návštěvy určitých oblastí webové aplikace a další zajímavé informace, pokud je webová aplikace k tomu uzpůsobena a soustřeďuje v databázovém systému potřebné údaje. Ve spojení s některými dalšími systémy modelování zahrnujícími např. využití technologie neuronových sítí, shlukových analýz, Kohonenových sítí a jiných metodologií[48] se mohou u velkých internetových společností využít nejen pro marketingové účely.

[47] V některé české literatuře se používá synonymum vytěžování dat

[48] Například souvisejících s teoriemi inženýrské psychologie a s přístupy dříve označovanými za „kybernetické aplikace“, které v posledních desetiletích díky rozvoji informačních technologií a výkonu hardwaru počítačů obohatily statistické, ekonomické, matematické i jiné vědy

Pokročilý CRM a vazba na informační systém

CRM[49] systém, tedy **systém řízení vztahů se zákazníky**, je nutnou a často integrální součástí celého informačního systému ve větších firmách orientujících se na prodej přes internet. Jeho úkolem je zejména přijímání požadavků a stížností od zákazníků, vyřizování reklamací a poskytování dalších informací zákazníkům, a často je vše doplněno o prvek groupwarového systému, který umožňuje okamžitou komunikaci mezi zaměstnanci při vyřizování dotazů.

V praxi není nutné používat vždy nějakou implementaci CRM systému. Je docela dobře možné, že stačí pro provoz internetového obchodu na straně firmy vyčlenit pouze jednu osobu, která přijímá emaily od zákazníků a jejich vyřizování spravuje sama nebo je přesměrovává na jiné spolupracovníky. Ve skutečnosti je tento způsob také reálný, se zvyšující se zátěží však vzrůstá potřeba personálních pomocných sil a klesá produktivita práce a schopnost rychlé odezvy, která je zákazníkem velmi citlivě hodnocena.

V posledních letech tak vznikly i sofistikované systémy, které lze obvykle dobře upravit pro potřeby zaměstnavatele a které se dokáží prostřednictvím zefektivnění práce vyrovnat i s většími požadavky ze strany zákazníků. Od tohoto bodu již obvykle můžeme způsob řešení označit za CRM systém, přestože je definice tohoto systému velmi neurčitá a subjektivní a s časem se mění hranice, kdy lze určitý systém považovat jen za rozšíření dosavadních standardních postupů a kdy jde již o samostatný systém splňující aktuální požadavky kladené na systém.

V případě většího množství zákazníků lze libovolně upravit systém tak, aby byl prostřednictvím poštovního serveru nebo i systému on-line komunikace (např. ICQ) použitelný i pro obsluhu většího množství požadavků více zaměstnanci. To bývá prvním bodem při konstrukci CRM systému. Dalším bodem je vyřešení způsobu, jak se bude toto prostředí monitorovat, což je zaměstnavateli také vyžadováno. V případě rozsáhlejších CRM systémů, u kterých se vyžaduje vazba na celý informační systém, je nutné vyřešit i problematiku této návaznosti na IS podniku, a to zejména pro účely archivace a následného procesu analýzy trhu či jiných marketingových činností za využití odborníků a popř. moderních metodologií heuristické analýzy.

Přestože jsou tyto přístupy k řešení procesu komunikace se zákazníkem internetového obchodu na vysoké úrovni, nejsou vhodné pro naprostou většinu firem provozujících internetový obchod. Důvodem je zejména malý důraz na význam internetového obchodování v podniku směřujícího své aktivity zejména k běžnému prodeji mimo internet nebo omezující velikost malého podniku, kterému se tento systém nevyplatí ani implementovat, natož za něj vydávat někdy i vysoké finanční prostředky.

[49] Costumer Relationship Management

1.5.10 Administrace

Posledním prvkem, kterému musí být v souvislosti se správným fungováním internetového obchodu věnována dostatečná pozornost, je soustředěna na administraci obchodu. Konkrétně se tím rozumí takové činnosti, které mají personálu zajistit možnost přidávat a odebírat jednotlivé druhy zboží ze sortimentu obchodu, upravovat popis jejich vlastností a také upravovat některé další vlastnosti obchodu.

Administrace obchodu je obvykle součástí samotné implementace webové aplikace ve formě webového rozhraní, ke kterému se přistupuje prostřednictvím webového prohlížeče, v některých případech tomu tak není, pokud se administrace obchodu týká pouze úpravy sortimentu obchodu. V takových případech existuje důvod, proč tuto administraci řešit mimo vlastní aplikaci např. vlastními silami vytvořeným softwarem či použitím jiného prostředku, který umí dostatečně dobře spravovat používaný databázový systém, bez kterého se každý běžný internetový obchod sotva obejde.

Administrační rozhraní webové aplikace je obvykle nutné velmi dobře zabezpečit, neboť při jeho eventuální kompromitaci útočník získává téměř neomezenou moc nad obchodem a zejména i databázovým systémem.

1.5.11 Prostředky nutné pro provoz internetového obchodu

V této poslední podkapitole zmíním základní prostředky, které musí být použity pro zprovoznění a udržování internetového obchodu. To velmi záleží na způsobu, který si daná firma zvolí při rozhodování o způsobu investování do jeho výstavby. Dnes již existuje několik možností, jak určitý internetový obchod provozovat.

Ještě před pár lety existoval jediný způsob, jak vytvořit internetový obchod, a ten spočíval ve **zprovoznění vlastního webového serveru**, tedy počítače s nainstalovaným softwarem zajišťujícím možnost komunikace protokolem HTTP mezi počítačem zákazníka a počítačem v místě firmy přes internetovou síť. Tento způsob je dodnes zřejmě nejlepším a pro větší firmy určitě nejvýhodnějším. Výhodou tohoto řešení je jednoznačně plná fyzická kontrola nad obsahem svého internetového obchodu. Veškeré technické činnosti, které provoz obchodu případně vyžaduje, jsou prováděny na místě a odborným personálem. Jeho nevýhody však spočívají právě ve vyšších nákladech na tento personál, který nejen spravuje webový server, ale obvykle má na starosti i správu sítě, popř. poštovního serveru. Často to s sebou přináší nutnost takový personál vyškolit na pracovišti.Je-li tento personál velmi dobře vzdělaný v oblastech IT a zkušený zároveň, může navíc plnit funkce bezpečnostní. Mzdové náklady na takový personál jsou nemalé

a obvykle ve střednědobém období – pokud jsou zaměstnáni na plný úvazek – mohou výrazně překračovat náklady na pořízení hardwaru, popř. softwaru nutného pro provoz internetové prezentace.

Nedostatky předcházejícího přístupu se snaží odstranit malý podnik zejména prostřednictvím využití **webhostingových služeb**. Tyto služby poskytuje dnes již dostatek podniků a spočívají v pronajmutí webového prostoru na jejich hardwarovém a softwarovém vybavení. Podniku tedy stačí obvykle pouze zadat zakázku na vytvoření funkční webové prezentace obchodu[50] a tu pak přenést na server poskytovatele webhostingových služeb. Není těžké uhádnout, jaké to přináší výhody či nevýhody. Největší výhodou bývají nízké náklady na vznik a provoz obchodu, což je hlavní stimul pro malé podniky. Teoreticky je možné zprovoznit obchod téměř bez jakýchkoliv finančních nákladů a platit pouze za webhostingové služby. Výhodou je také možnost nezaměstnávat žádného IT specialistu, což také snižuje náklady a obvykle stačí personál velmi krátce seznámit s administrací a interakcí s webovou aplikací, což zabere nejvýše pár desítek minut či hodin. Určitou nevýhodou však může být absence kontroly nad webovým serverem a počítači, kterých se provoz našeho obchodu týká. To může v konečném důsledku vést až ke ztrátě jakékoliv bezpečnosti internetového obchodu, pokud je provozovatel webhostingových služeb podnikem ledabyle vybrán a zaměstnanci tohoto podniku méně či vůbec neseznámeni s problematikou bezpečnosti jejich počítačů.

V souvislosti s provozováním webhostingových služeb existují odvozené služby **webhousingu**, které nevýhody webhostingu částečně omezují. Při využití této služby si podnik svůj webserver nainstaluje a zprovozní ho až na místě provozovatele webhousingu, který mu případně zajišťuje další doplňkové služby nesouvisející obvykle s vlastním provozem webserveru. Tento přístup je jakýmsi kompromisem mezi ztrátou kontroly nad vlastním internetovým obchodem v případě webhostingu a na druhé straně vysoké finanční náročnosti při použití vlastního řešení v podniku.

1.5.12 Manažerské rozhodování o volbě řešení

Tato poslední krátká podkapitola je věnována volbě řešení. Vždy je nutné zvolit pro tvorbu internetového obchodu tu správnou osobu nebo podnik, který webovou aplikaci vytvoří. Lze využít buď vlastních personálních zdrojů, lze též využít služeb firmy specializující se na vývoj webových aplikací či jednotlivců nebo skupin jednotlivců – programátorů. Toto je velmi těžké rozhodování a ve velké míře rozhoduje o úspěšnosti internetového obchodu.

[50] Existuje tu i možnost zprovoznit i předem vytvořenou internetovou prezentaci, což už se dnes podnikům také mnoho firem snaží nabízet. Navíc existuje možnost zprovoznění nějaké dostupné webové aplikace poskytované zdarma.

Každý přístup s sebou nese určitá rizika a konkrétní volba řešení je značně závislá na cílech podniku na poli internetového trhu, na odvaze investovat do nejistého výsledku a také na kapitálové náročnosti. Je to čistě manažerské rozhodování.

Protože je oblast vývoje IT řešení v tomto oboru velmi mladá, můžeme se v ní setkat s mnoha způsoby a v neposlední řadě i s různými extrémy.

Při nejmenších požadavcích, které spočívají v tvorbě obchodu vytvořeného ze statických stránek, lze primárně využít jakýkoliv služeb, neboť tvorba takového obchodu je jen otázkou pár hodin práce a jsou tedy nejlevnější, ať je vytváří kdokoliv.

Zřejmě nejčastěji jsou využívány **služby individuálních programátorů** specializujících se na vývoj dynamických webových aplikací. Schopnosti těchto individualit jsou však často absolutně neodhadnutelné a výsledek využití jejich schopností nemusí končit zdárně. Nebývá to však častým jevem. Dnešním paradoxem však bývá, že konkrétní služby v této oblasti nabízí prostřednictvím svých osobních webových stránek občas i velmi mladí lidé, kteří buď nemají evidentně žádné zkušenosti a po přečtení pár knížek se často cítí být „IT odborníky“ a navíc zřejmě velmi často ani nemohou uzavřít např. smlouvu o dílo apod. Příčinou je především velká dynamika vývoje IT technologií, ve které je však mladá generace schopna se velmi dobře pohybovat. Je tedy možné celkem pravděpodobně nalézt i teenagery, jejichž schopnosti mohou i velmi výrazně překračovat schopnosti daleko starších a „zkušených“ programátorů. Podnik či manažer tak čelí značné nejistotě při volbě vhodného jedince/jedinců, což často vede ke zvolení jiného řešení.

Pokud pro podnik není případná tvorba internetového obchodu prioritou, lze často využít i **vlastní zaměstnance**, kupříkladu síťové správce apod. Tito lidé obvykle nemají svůj pracovní čas v podniku vyplněn zcela a obvykle jejich zájmy zasahují i do oblasti informačních technologií. Často to může být nejlevnější řešení a někdy i velmi vhodné. Mezi tyto levnější řešení lze zařadit i pro tento účel víceméně náhodné **zvolení „kamaráda“ nebo „známého, co se zajímá o počítače“**. Kvalita konečného výsledku je ale opět velmi těžko předpověditelná. Toto řešení je ale zejména pro malé firmy velmi lákavé.

Dnes již existuje i u nás dostatek firem – často s zahraničním kapitálem – které vznikají obvykle sestavením specializovaných vývojových týmů. Tyto společnosti poskytují různá řešení pro různé typy podniků vyžadujících zřízení internetového obchodu a stejně tak jako v případě jednoho či více programátorů, je i zde nutné posoudit kvalitu poskytovaných služeb. Tyto firmy si časem vyvíjejí své vlastní implementace, které pak stačí jen do-upravit pro konečného provozovatele nebo je prostě „překopírují“ na server zákazníka. Cenová náročnost je velmi rozdílná. Prosté „překopírování“ již vytvořené implementace je dnes obvykle otázkou investice v řádu mála desítek tisíc korun, do-vyladění aplikace pro potřeby zákazníka samozřejmě představuje

pár tisíc či desítek tisíc korun navíc. Úzce specializovaná řešení nebo vývoj zcela nové rozsáhlé aplikace stojí nejvíce, řádově stovky tisíc, dokonce i miliony korun. Pro představu lze uvést, že při takové práci není výjimkou, když si firma za hodinu práce web-designéra účtuje i více jak 1000 Kč/h, práci tvůrce skriptů na více jak 800 Kč/h apod. Je tedy zřejmé, že se to nehodí pro každý podnik, protože některé podniky by tyto náklady ekonomicky položily už před dokončením implementace. Dražší řešení lze najít snad jen při zadávání zakázek ze strany státu, zde je možné – jak jsem se doslechl – pro účely tvorby i docela jednoduchých a i nezabezpečených webových aplikací vynaložit až téměř půl miliardy korun. Protože se v této oblasti trochu vyznám, tak je mi hned jasné, že takový obchod rozhodně není „košér“ a je obvykle možné jej označit za podezřelý.

Obecně však při jakékoliv volbě řešení platí, že rychlost vývoje webové aplikace je velmi důležitým faktorem. Často se totiž projeví platnost přísloví „práce kvapná, málo platná“, pokud se vývoj obchodu „uspěchá“. To platí obecně téměř vždy při vývoji jakéhokoliv proprietárního softwaru.

Pokud bych měl vyslovit svůj názor, tak nejvhodnějším řešením pro malé podniky je využití služeb některých nabízených hotových řešení specializovaných firem nebo zaměstnání schopného jednotlivce s průměrnými nároky na zhodnocení své práce. Investice tak představují maximálně desítky tisíc korun. Při větších požadavcích je nutné velmi dobře posoudit finanční stránku věci. Při dostatku prostředků je možné zvolit opět specializovanou firmu a řešení, které stojí několik set tisíc až milionů korun, nebo zvolit velmi obětavého programátora nebo jejich menší skupinu, která obvykle za mnohem menší peníze vytvoří obvykle také velmi kvalitní produkt. Volba vhodných zaměstnanců je však podle některých zkušeností často hádáním z křišťálové koule.

Kapitola 2

Implementace

V této kapitole, věnované pouze praktické stránce tvorby funkčního internetového obchodu, se budu snažit vysvětlit podrobněji kroky, kterými musí každý tvůrce internetového obchodu projít, pokud má úspěšně vytvořit webovou prezentaci splňující požadavky podniku.

Pro tento účel jsem vytvořil vlastní implementaci takovéhoto obchodu, která se snaží být velmi jednoduchá a pozadí fungování pochopitelné i pro člověka, který problematice nemůže často rozumět. A protože obvykle 95% práce – bez ohledu na počet jiných osob často se podílejících na jeho tvorbě – leží téměř vždy na programátorovi dané webové aplikace, budeme se zčásti zabývat právě pohledem takovéhoto člověka. Zároveň bude však vše osvětleno tak, aby čtenář nemusel být seznámen s problematikou programovacích jazyků, která by byla nutná pro důkladnější pochopení problematiky zmíněné v této a také zčásti v další kapitole této práce.

Hned zpočátku bych měl upozornit, že tato implementace si neklade za cíl být nějakým komplexním řešením a také není vytvořena tak, aby byla dlouhodobě využitelná v podobě, která je součástí této práce. Tvorba mého řešení také není speciálně upravena a ošetřena proti bezpečnostním hrozbám, které představují útoky crackerů[1], přestože byl na tento aspekt kladen důraz.

Pracovně jsem projekt nazval **Xinerama** a uzpůsobil jsem mu veškeré nutné náležitosti v názvech databáze, textech apod.

[1] Slovem „cracker“ se označuje obyčejně člověk provádějící útoky na počítačové systémy za účelem jejich kompromitace a zneužití výsledků pro svou potřebu a k páchání trestné činnosti. Prosím neplést se slovem „hacker“, který má poněkud jiný význam, laickou veřejností mylně ztotožňován nebo chápán ve stejném významu slova „cracker“.

2.1 Použité prostředky

Nejdříve si vysvětlíme základní pojmy, které je potřeba znát pro pochopení funkčnosti webové aplikace jako takové. Aplikace internetového obchodu je vytvořena prostřednictvím jakéhokoliv skriptovacího nebo programovacího jazyka. K využití této aplikace je potřeba minimálně jednoho počítače s pevnou IP adresou, na kterém se spustí tzv. webový server a obvykle i databázový systém, který obhospodařuje požadavky klientů, které zajišťují jejich internetové prohlížeče. Díky několika dalším službám pak může kdokoliv při zadání naší domény do okna prohlížeče navštívit náš internetový obchod.

Teď něco ke konkrétním prostředkům. Pro vývoj internetového obchodu byl použit skriptovací jazyk PHP, který je velmi jednoduchý a rozšířený, pro účely tvorby dynamických aplikací určených pro internet zřejmě nejvhodnější pro svou velkou flexibilitu, která se projeví zejména při tvorbě a provozu rozsáhlejších projektů. Pro uchovávání dat, které je obyčejně nejdůležitějším prvkem všech dynamických internetových prezentací, byl záměrně zvolen méně komplexní, zato pro účely webových aplikací nejvíce vhodný, databázový systém MySQL, který je taktéž velmi používaným zejména z důvodu vysoké výkonnosti, která dnes nemá téměř konkurenci.

Pro vývoj a testování webové aplikace byl použit operační systém Mandrake*L*inux 9.1+9.2 GPL set za použití těchto prostředků: VIM 6.2 (editor), Apache 2 (webserver), PHP 4.3 (skriptovací engine), MySQL server 4.0 (databázový systém), PHPMyAdmin 2.5 (webové rozhraní pro přístup k databázi) a Quanta Plus 3.1 (HTML editor). Všechny tyto prostředky jsou přístupné zdarma pod licencemi GNU/GPL a podobnými. Toto tzv. **řešení LAMP**[2] je dnes nejvyužívanějším prostředkem pro provoz dynamických webových aplikací, jen těsně před technologiemi svázanými s komerčním systémem Microsoft Windows. Důvodem je především bezpečnost, která v případě serveru Apache mluví sama za sebe. Ve verzi Apache 1.3 nebyla do dnešní doby zjištěna podstatná vada, která by vedla k jeho kompromitaci[3].

Při realizaci a provozu internetového obchodu se dnes dá využít mnoha prostředků, stručně některé nejpoužívanější z nich pro úplnost jmenujme.

Kromě zde již zmíněného řešení LAMP se často využívají řešení firmy Microsoft, které zahrnují webový server Microsoft IIS[4] a skriptovací jazyk ASP[5], popř. některé další doprovodné rozšiřující služby. Pro vývoj webového kódu se často používá Microsoft Frontpage či jiné WYSIWYG[6] editory (např. Macromedia Dreamweaver), nebo pokročilé HTML editory

[2] LAMP = **L**inux & **A**pache & **M**ySQL & **P**HP

[3] Myslím tím jádro tohoto webserveru, ne jednotlivé přídavné moduly, které jsou často dílem jiných autorů

[4] Microsoft Internet Information Server

[5] Active Server Pages

[6] **W**hat **Y**ou **S**ee **I**s **W**hat **Y**ou **G**et – mechanismus tvorby, při kterém konečný výsledek vidíme již při tvorbě aplikace, není obyčejně potřeba znát pozadí technologií, což obyčejně upoutává začátečníky v oboru IT nebo klasické uživatele

(např. Homesite). Řešení založená na webserveru IIS jsou rozšířená zřejmě pouze v důsledku rozšíření platformy Windows, z hlediska použití je toto řešení bezpečnostně méně vhodné, což blíže vysvětlíme v kapitole věnované bezpečnosti. Velkou nevýhodou tohoto řešení je také závislost na operačním systému a velké finanční náklady na pořízení softwaru. Toto už dnes úplně neplatí, protože i bez jakékoliv aktivity firmy Microsoft jsou vyvíjeny projekty, které mají tyto nedostatky odstranit[7]. Výhodou je obvykle jednoduchá konfigurace v grafickém prostředí.

Méně používaná řešení představují webservery Novell Enterprise Server, iPlanet Web Server, Novell Groupwise, RealServer, Lotus Domino a v poslední době také dost používaná řešení servletových serverů BEA Weblogic, Apache Tomcat a dalších, založených na platformě Java (J2EE).

Podle mého názoru jsou nejlepší ta řešení, která jsou lety používání řádně ověřena z mnoha hledisek a která zejména při tvorbě projektů s většími požadavky na bezpečnost, flexibilitu, interoperabilitu a multiplatformitu dosahují nejlepších výsledků. Právě tyto parametry jsou vyzdvihovány i v programech Evropské Unie pro rozvoj informační společnosti. Taková řešení podle mého názoru zahrnují zejména použití serveru Apache nebo servletového webserveru a doprovodných jazyků jako je Perl, PHP, Java či Python a (X|HT)ML ve funkci značkovacího jazyka. Částečně lze za specifických podmínek a jen v některých případech asi doporučit dnes i použití technologie .NET, která se snad stane za pár let multiplatformně nezávislým řešením.

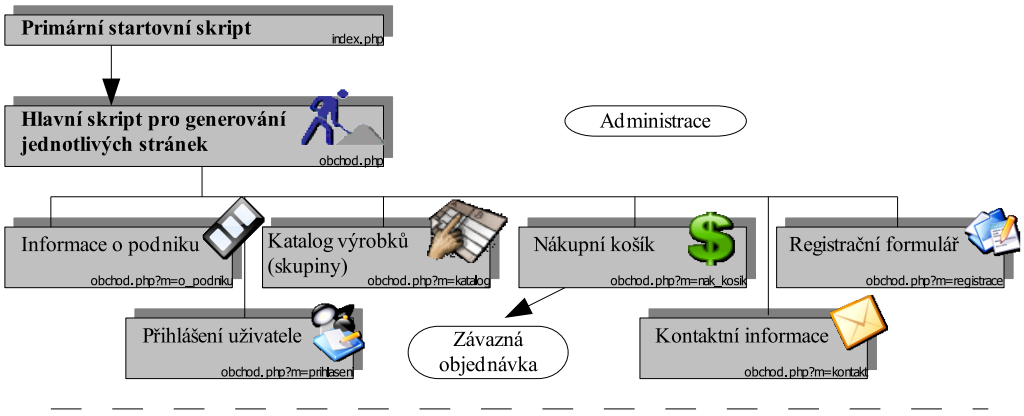
2.2 Návrh a struktura obchodu

Předně musím říci, že ačkoliv by to mělo být za jiných okolností zvykem, návrh této aplikace nebyl dopředu podrobněji promyšlen, a to zejména z důvodu své poměrně menší složitosti, která si vůbec nezadá např. s implementací rozsáhlých portálů či specializovaných webových aplikací. Struktura je tedy jednoduchá, zejména při pohledu na webové stránky takto působí. Konkrétní podoba obslužných skriptů už tuto jednoduchost trochu narušuje, právě kvůli předem málo promyšlené koncepci. Jednoduchost jazyka PHP však činí přehled o funkčnosti kódu částečně jasným i pro neodborníka. Při realizaci skutečně kvalitního internetového obchodu by mohly a často měly být uplatněny myšlenky softwarového inženýrství či jiného obdobného přístupu, který nemusí být často náplní vlastní práce programátora.

Textový obsah samotného kódu webové aplikace má rozsah asi 2,5 tis. řádek, což je poměrně malé množství. Samotná práce na projektu stejného rozsahu představuje odhadem 3 až 4 týdny při započetí práce „na zelené louce“. Vše je součástí přílohy č.2 k této práci zveřejněno pod licencí GNU/GPL k volnému použití.

[7] Jedním takovým projektem je využití ASP jako modulu Apache serveru

Obrázek 2.1: Struktura obchodu



Konkrétní zjednodušenou strukturu obchodu zobrazuje obrázek 2.1 na straně 51. Podrobnosti týkající se struktury budou dále zmíněny.

Primární skript, který se nahrává vždy při návštěvě dané domény, je soustředěn do souboru `index.php`. Tento skript jednoduše předává práci hlavnímu skriptu, který provádí generaci všech ostatních stránek obchodu (`obchod.php`).

Úkolem hlavního skriptu je zejména definování základních globálních proměnných platných všude během běhu skriptu (např. informace o podniku) a připojení k databázi, která soustředí důležité informace. Pokud se připojení k databázi nepovede, je zobrazeno uživateli, že není možné pokračovat v prohlížení webových stránek.

Hlavní skript dále kontroluje obsah URL a podle kontroly dat v databázové tabulce popisující jednotlivé stránky obchodu, se rozhodne, zda zobrazit danou stránku. Tento přístup je vhodný, protože zaručuje, že skript nebude hlásit případné nečekané chyby, pokud bude URL uživatelem špatně zadána. V tom případě se mu zobrazí krátké hlášení, že požadovaná stránka neexistuje. Nebo lze v případě potřeby přesměrovat uživatele na hlavní stránku. To vše má svůj bezpečnostní význam, který zmíníme později.

Kromě jiného je při každém načtení webové stránky zvýšeno počítadlo přístupů do našeho obchodu (individuálně podle počtu uživatelů i v celkovém souhrnu) a jsou načteny, popř. upraveny základní informace o uživateli a podstránce, která se má zobrazit. To vše se provádí při načtení jakékoliv podstránky obchodu, což je u dynamických aplikací zvykem.

Celkovou strukturu popsanou prostřednictvím jednotlivých skriptů zobrazuje tabulka 2.1 na straně 52. Kromě těchto souborů jsou součástí projektu i grafické soubory ve formátech XCF, JPEG a PNG.

Tabulka 2.1: Jednotlivé implementační soubory internetového obchodu

Název souboru	**Funkce**
`admin_ace.php`	Administrace obchodu
`databaze.sql`	SQL skript (struktura databáze)
`db.php`	Zajistí připojení a odpojení od databáze
`dph.php`	Informace o dani z přidané hodnoty
`chyba.php`	Obsluhování chybových stavů
`index.php`	Doporučený skript pro prvotní načtení webové prezentace
`_in_katalog_vyrobku.php`	Katalog výrobků
`_in_kontakt.php`	Kontaktní informace
`_in_nakupni_kosik.php`	Implementace nákupního košíku
`_in_objednavka.php`	Obsluha závazné objednávky
`_in_odhlaseni.php`	Odhlášení přihlášeného uživatele
`_in_o_podniku.php`	Informace o podniku
`_prihlaseni.php`	Přihlášení uživatele do obchodu
`_registrace.php`	Registrace nového uživatele nebo úprava registračních údajů
`_in_standardni_zahlavi.php`	Záhlaví stránky
`_in_standardni_zapati.php`	Zápatí stránky
`_in_uvodni_stranka.php`	Přivítání do obchodu
`lib.php`	Některé pomocné funkce
`obchod.php`	Hlavní obslužný skript
`opravneni.sql`	SQL skript (oprávnění)
`pausaly.php`	Paušální poplatky
`podnikove_udaje.php`	Některé vybrané údaje o podniku
`service.js`	Zdroj Javascriptu
`stranka.php`	Objekt spravující zobrazení požadované stránky
`uzivatel.php`	Objekt reprezentující návštěvníka obchodu
`vyrobek.php`	Objekt reprezentující konkrétní výrobek
`styl.css`	Kaskádový styl CSS

Části kódu zodpovědné za zobrazení konkrétního obsahu požadovaného uživatelem jsou rozděleny záměrně do několika souborů, zejména kvůli přehlednosti. Samozřejmě je možné vše soustředit do jednoho velkého souboru, ale značně to pak snižuje jeho přehlednost a v neposlední řadě se musí takový soubor dlouze načítat při každém vstupu na webové stránky, což zbytečně zatěžuje server a může při velkém zatížení snižovat dobu odezvy. Při tomto rozložení se načítají jen ty části, které jsou nutné pro zobrazení určité stránky. Načtení stránky je tak při pominutí zpoždění na straně uživatele a přenosové rychlosti sítě otázkou malého zlomku vteřiny (např. 0,1 s).

2.3 Databáze dat

Databázový systém je v případě dynamických webových aplikací – jakou je i náš internetový obchod – velmi nepostradatelnou částí, neboť se v ní ukládají informace, které jsou nutné pro provoz obchodu. Alternativním postupem k tomuto řešení je přímé ukládání informací do jednotlivých souborů, což s sebou však přináší mnoho nevýhod. Lze využít i jiné přístupy, ale obvykle je ukládání na databázovém serveru tím nejvhodnějším a v případě MySQL také nejrychlejším způsobem.

Při vytvoření databáze na serveru je vhodné použít nějaký prostředek, který nám práci při vytváření databáze ulehčí. Jedním takovým je webové rozhraní PHPMyAdmin. Pokud jste zkušenější, stačí vám konzolový přístup.

Obsahem souboru `opravneni.sql` je skript, který se při spuštění s dostatečnými právy na serveru pokusí vytvořit databázi 'xinerama' a uživatele 'tomas' s přístupovým heslem 'hezkeheslo', který bude mít oprávnění k veškeré práci s touto databází, ale pouze při přístupu z lokálního počítače. To je vhodné kvůli bezpečnosti. Např. přidělení práv uživateli 'tomas' se může v konzoli zapsat takto[8]:

```
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,INDEX,ALTER,
CREATE TEMPORARY TABLES ON ‘xinerama‘ . * TO "tomas"@"localhost";
```

Jde vidět, že přestože může být syntaxe i přehledná, není lepšího řešení než je použití grafického rozhraní PHPMyAdmina, se kterým je práce daleko rychlejší (pokud nejste databázový guru).

Teď si popíšeme stručně funkci tabulek, které jsou součástí databáze. Jejich konkrétnější funkce zde nebudu vysvětlovat, dají se zjistit ze zdrojového kódu PHP.

[8] Znaky '\\' záměrně odděluji text, který by měl být na stejném řádku, bude používáno i dalším textu

```
mysql> show tables;
+--------------------+
| Tables_in_xinerama |
+--------------------+
| data               |
| kosiky             |
| objednavky         |
| pocitadla          |
| skupiny            |
| stranky            |
| uzivatele          |
| vyrobky            |
+--------------------+
8 rows in set (0.02 sec)
```

Funkci některé z tabulek není potřeba nijak zvlášť popisovat, jejich funkce je zřejmá a jejich struktura je obsažena v souboru `databaze.sql`, který navíc obsahuje i některá ilustrativní data. V tabulce `data` se navíc soustředí informace o tom, zda není náhodou stránka mimo provoz, a také se zde archivuje čas posledního přístupu na web, což se dá použít např. k archivaci denních statistických údajů o návštěvnosti stránek. V tabulce `kosiky` se soustředí v jednotlivých položkách údaje o obsazích nákupních košíků uživatelů. Ke zjištění kompletního obsahu neprázdného košíku daného uživatele se využívá nejméně jedna položka v této tabulce. Tabulka `skupiny` obsahuje kategorie výrobků, čímž je možné po určitých úpravách vytvořit hierarchii sortimentu a rozšířit možnosti chování aplikace při prohlížení katalogu.

V tabulce `uzivatele` se soustředí jen data registrovaných uživatelů, neregistrovaní nebo nepřihlášení návštěvníci nejsou kontrolováni. Zejména se v této tabulce uchovávají tyto údaje:

- uživatelské přihlašovací jméno
- jméno a příjmení zákazníka
- heslo šifrovaně
- počítadlo přihlášení do obchodu
- emailová adresa
- adresa
- telefon

Obrázek 2.2: Design

. . . a další údaje jako jsou identifikátor sezení (session ID[9]), čas posledního přístupu, datum registrace apod.

Údaji o výrobcích v tabulce `vyrobky` se rozumí zejména jejich cena, zařazení do skupiny v sortimentu, stručný popis, informace o tom, zda je výrobek na skladě a také případný odkaz na fotografii nebo obrázek výrobku.

Co se týče tabulky `stranky`, ta v sobě soustředí data o všech podstránkách, které lze obsloužit. Obsahuje tedy zejména odkaz na soubor skriptu, který se má spustit při jejich zobrazení na webové stránce. Navíc také slouží k zobrazení daného titulku v okně prohlížeče a v neposlední řadě zaznamenává i počítadlo přístupů.

2.4 Design

V této práci byla problematika designu rozebrána do poměrně velké hloubky, ale pro mou implementaci internetového obchodu to byl ten nejposlednější prvek, neboť nebyl původně určen pro konkrétní nasazení ve firmě. Proto jsem zvolil velmi střízlivý design, přesto ale nikoliv nepříjemný, jak lze snad vidět na obrázku 2.2 (str. 55).

Při vytváření designu bylo použito „tabulkové grafiky“, která je dnes nejvyužívanějším přístupem k tvorbě webu.

[9]Tento 32ti-znakový řetězec zajišťuje udržení relace mezi webovou stránkou a daným uživatelem. Odstraňuje se tak „beze-stavovost“ protokolu HTTP/1.1, který neumožňuje udržovat tuto relaci svými prostředky.

Hlavní částí webové stránky je úvodní logo „Xinerama“, které je zapuštěno do grafického rámu jako hlavního záhlaví webu, a ve spodní části záhlaví jsou zobrazeny nejpoužívanější odkazy, které mění barvu při pohybu myši nad nimi[10]. Pak následuje vlastní obsah stránky a vše je zakončeno krátkým zápatím s copyrightem. Na podobných místech je často vhodnější zobrazovat aktuální datum či jiné údaje. Bohužel velmi často se podobná místa zneužívají i ke sdělení, že webmaster „nebyl schopen“ vytvořit webovou stránku podle standardů, a tak je webová stránka dobře čitelná pouze v určitém prohlížeči, což však málokoho zajímá natolik, aby to bylo integrální součástí každé webové stránky. A v případě internetového obchodu je to navíc krajně nevhodné.

Jako barevné schéma bylo použito jednoduchých odstínů modré a zelené barvy (tj. analogických barev) společně s červenou komplementární barvou. Toto schéma má jistě daleko do dokonalosti, přesto alespoň zčásti plní některá základní designérská pravidla.

Pro textový obsah bylo zvoleno standardní písmo, které by mělo být snadno dostupné nebo nahraditelné na jakékoliv platformě.

2.5 Registrační a přihlašovací mechanismus

Registrace a přihlašování je integrální součástí každého internetového obchodu a práce na něm je obvykle jedna z nejsložitějších, pokud má být slušně zabezpečeno.

Registrace je v mé podobě internetového obchodu povinná pokud si chce zákazník něco objednat nebo přidat do košíku. Toto řešení samozřejmě není jediné a nejštastnější, velmi často vidím, že je možné si u většiny obchodů přidávat zboží do košíku a teprve potom se zaregistrovat, aniž by člověk ztratil obsah košíku. Vidím to jako lepší řešení přestože není použito v mém obchodu. Vyžaduje to totiž sledovat chování každého zákazníka, tedy nejen registrovaného a přihlášeného. Malými úpravami kódu lze samozřejmě internetový obchod o toto chování doplnit. Zde to nebylo důležité.

Registrace je velmi jednoduchá. Stačí na úvodní stránce kliknout na odkaz pro registraci, vyplnit jednoduchý formulář[11] a po potvrzení těchto údajů se uživatel může ihned přihlásit do obchodu, což je otázka pár vteřin.

Registrační a přihlašovací mechanismus jsem se snažil vyřešit tak, aby byl co nejvíce přehledný pro potenciálního zákazníka. Už nemůže být jednodušší. Je prováděna pouze kontrola,

[10] Takzvaný „roll-over“ efekt

[11] Ve formuláři se musí povinně vyplnit přihlašovací jméno a heslo, ostatní údaje jsou nepovinné, ale s omezením, že nebude zákazník moci objednat zboží pokud chybí adresa, kam poslat dobírku, či emailová adresa pro informování zákazníka o stavu vyřizování objednávky

zda nebyly zadány při registraci nebo přihlašování nepřípustné znaky nebo nepřípustně velké řetězce a zda byly zadány alespoň povinné údaje[12]. Pokud něco nesouhlasí, je o tom uživatel okamžitě srozuměn a může svou chybu opravit, a to jak kliknutím na tlačítko „Zpět“ v prohlížeči, tak po kliknutí na nabízený odkaz.

Vše je navíc implementováno tak, že je možné i během relace přihlášeného uživatele registrovat jiného potenciálního zákazníka. To nebývá obvykle v internetových obchodech povoleno, obyčejně se vyžaduje nejdříve odhlášení aktuálního uživatele.

Pokud je zákazník přihlášen a chce si např. změnit heslo či jiné přístupové údaje[13], automaticky se mu nabídne odkaz, kde je toto možné. Opět jde z uživatelského hlediska o triviální věc. Pro přehlednost se mu v závorkách za jednotlivými poli zobrazují dříve zadané údaje. Zásadně se heslo nezobrazuje, ba dokonce ani nemůže, protože je v databázi uloženo v šifrované podobě, takže zjištění původního hesla je „téměř“ nemožné[14].

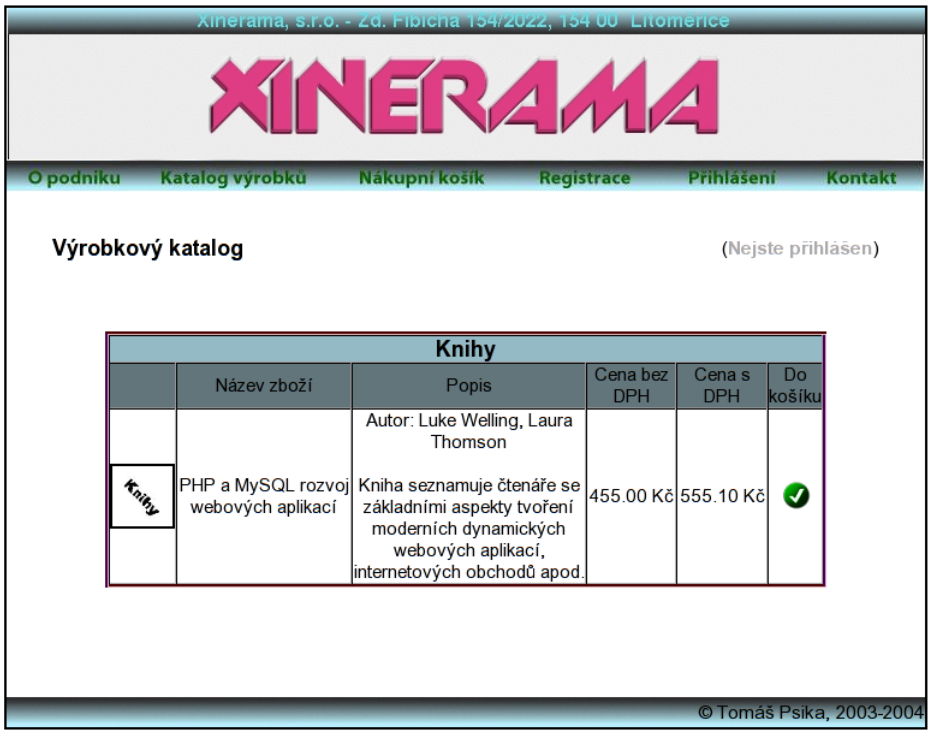
Případné odhlášení uživatele je možné na tom samém místě, kde se uživatel přihlásil. Je na to upozorněn. Je možné odkaz na tuto stránku umístit na vhodnější místo, je-li potřeba.

S vlastní registrací je spojena určitá bezpečnostní hrozba plynoucí z použití útoku přehráním (bude zmíněno později) za určitých specifických podmínek. Toto ohrožení však nevede zřejmě k narušení činnosti této podoby obchodu.

Jako doplňková služba je implementována funkce obnovení registračních údajů pokud uživatel zapomene své přihlašovací heslo. Postup není složitý. Na stránce určené k přihlašování uživatelů je defaultně umístěn odkaz pro zapomětlivce. Po jeho aktivaci je na emailovou adresu uvedenou při registraci zaslán unikátní URL odkaz, po jehož následování se zobrazí stránka obchodu a zákazník je ve stavu „přihlášen“, což ho opravňuje ke změně registračních údajů. Tento mechanismus byl odladěn za lokálních i síťových podmínek a měl by být ihned funkční, pokud je správně nastaven poštovní server. Unikátní odkaz na stránky našeho obchodu v emailu v sobě zahrnuje uživatelské jméno, zvláštní řetězec a aktuální datum. Vše je šifrováno jednocestnou hashovací funkcí, takže rozšifrování je velmi obtížné až dnes téměř nemožné. Při návštěvě stránky skript vytvoří stejný hash a ten porovná s tím, který je obsažen v URL, a v případě shody umožní uživatele přihlásit. Podobný mechanismus se používá při odesílání digitálně podepsané emailové zprávy.

[12] Je zakázáno zaregistrovat se napodruhé pod stejným uživatelským jménem!
[13] Chce-li zákazník např. doplnit adresu, aby mu mohlo být zboží zasláno na dobírku
[14] Je-li to opravdu nutné, lze toto heslo obvykle zjistit, ale vyžaduje to často nadmíru velké úsilí

Obrázek 2.3: Katalog výrobků



2.6 Výrobkový katalog

Vytvořený katalog výrobků je také implementován jednoduchým způsobem, přestože by bylo vhodné pro reálné nasazení doplnit provedení o nějaké rozšiřující možnosti. Při kliknutí na odkaz „Katalog výrobků“ je zobrazen seznam kategorií zboží. Po vybrání kategorie se zobrazí veškerý seznam zboží v dané kategorii.

V daném seznamu zboží určité kategorie se zobrazí všechny potřebné údaje o výrobcích, jako je cena bez a s daní z přidané hodnoty, obrázkový náhled[15], stručný popis a odkaz sloužící k přidání do nákupního košíku (obr.2.3, str.58. Kliknutím na náhled obrázku by se měla zobrazit zvětšenina náhledu a také bližší informace[16]. V těchto informacích by se měly objevit i informace o záruce a jiné údaje, o kterých jsme se zmínili v předcházejících kapitolách.

Z této stránky vedou individuální odkazy sloužící k přidání výrobku do košíku. Vkládá se do košíku vždy jen jeden výrobek daného druhu. Případná změna množství se dá upravit až při náhledu obsahu nákupního košíku. Pokud byl již daný druh zboží do košíku vložen předtím, není na to uživatel upozorněn a je upraveno množství daného výrobku na jeden kus, protože

[15] Je-li tento obrázek k dispozici, jinak se použije obrázek označující skupinu, ve které se zboží nalézá
[16] Není zatím implementováno v nynější verzi

předpokládám, že většina uživatelů si při přidání daného zboží do košíku zřejmě neuvědomí, že už toto zboží dříve do něj přidala (v jakémkoliv množství). Případnou dodatečnou změnu množství daného výrobku lze měnit průběžně a kdykoliv. Samozřejmě je možné využít i jiného postupu, ale mě se tento zdál pro jednodušší implementaci vhodnější.

Po přidání daného zboží do košíku je zákazník přesměrován na stránku, kde se mu zobrazí obsah košíku a je mu vypočítána aktuální celková cena. Zároveň se mu zobrazují i podrobné cenové údaje včetně souhrnných částek za jednotlivé výrobky, které jsou zvýrazněny v tabulce žlutým pozadím. Má tak tedy dokonalou kontrolu nad informacemi o cenách, které jsou pro většinu zákazníků naprosto rozhodující.

Je samozřejmě možné zvolit také metodu, kdy obchod uživatele jen informuje o přidání zboží do košíku a pak mu následně zobrazí např. skupinu zboží, kterou si objednal. Popř. je možné ho přesměrovat na podobný druh zboží apod. Možnosti jsou v tomto ohledu neomezené a je na konkrétních požadavcích podniku, jakou strategii zvolí. Téměř vše lze nějakým způsobem implementovat. Lze přitom využít i metod, prostřednictvím kterých se obchod „učí“ podle předešlých chování jiných spotřebitelů. Je to však spíše využitelné v případě více marketingově orientovaných a především velkých podniků, které mají dostatek finančních prostředků na investování do vývoje či nákup nějakého specializovaného softwaru v této oblasti[17]. Jednodušším řešením je zobrazení výrobků, které si předešlí zákazníci, kteří nakoupili dané zboží, nakoupili zároveň s ním. Toto řešení je méně nákladné a také většinou splňuje tento účel.

2.7 Nákupní košík

O možnostech nákupního košíku zde již byla většina informací zmíněna výše. Pro doplnění lze uvést, že jsou implementovány některé základní funkce, jako je vysypání celého obsahu košíku a změna množství jednotlivých druhů výrobků.

Změna množství je realizována tak, že zákazník klepne myší na odkaz, který uvádí počet kusů zboží. Poté se načte obsah košíku a objeví se editovatelné a červeným šrafováním orámované pole, ve kterém stačí vyplnit požadované číslo. Po odeslání dat se mu načte aktualizovaný obsah košíku se změněnými informacemi o cenách.

Na stránce se zobrazeným obsahem nákupního košíku je v dolní části umístěn odkaz, kterým se realizuje objednávka. A jako dodatek je také uváděno množství vyřizovaných předešlých objednávek.

[17] Opět zde můžu zmínit metody dolování dat a využití nejnovějších přístupů za využití „umělé inteligence“

2.8 Objednávkový systém

Odkaz vedoucí zákazníka k objednávce je umístěn pouze na stránce, kde se zobrazuje obsah košíku, což je ostatně dost intuitivní.

V mé implementaci je objednávkový systém trochu zjednodušen, avšak na úkor intuice. Protože jsou na stránce zobrazující nákupní košík uvedeny veškeré důležité údaje[18], kliknutím na odkaz pro objednání je již objednávka zároveň potvrzena. To nebývá obvyklé, často se používají v internetových obchodech postupy, kdy jsou nejprve zobrazeny některé další údaje na další stránce, popř. následuje ještě několik kroků před vlastním potvrzením objednávky ze strany zákazníka. V mé verzi je vše pro jednoduchost slito do jednoho kroku. Bylo by nejspíš vhodné pro reálné nasazení přidat alespoň jeden krok, ve kterém si zákazník zkontroluje údaje ještě jednou a pak teprve objednávku potvrdí.

Objednání je z pohledu běhu aplikace realizováno tak, že jsou údaje o obsahu nákupním košíku uložené v databázi ukládány pro účely objednávky do jiné tabulky ve standardizovaném formátu, který se může dál zpracovávat přes administrativní rozhraní přes personál.

Konečný výsledek z pohledu zákazníka vidíte na obr. 2.4, str. 61.

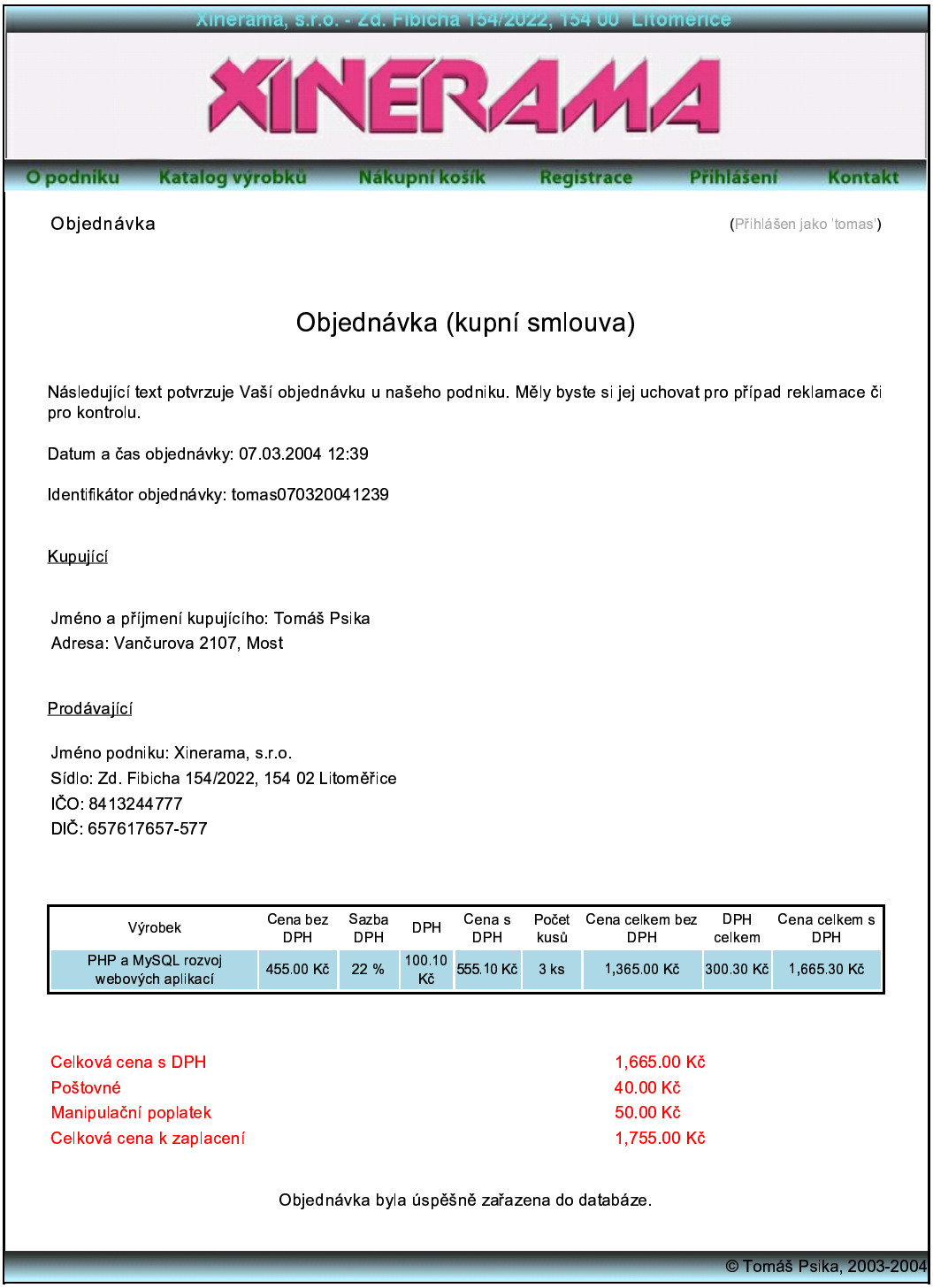
Jak vidíte, na stránce s objednávkou je poměrně málo informací, rozhodně obsahově jich je méně než by mělo být v reálném nasazení. Pro naše účely je to však dostačující.

2.9 Ostatní služby a administrace obchodu

Internetový obchod lze obohatit o mnoho dalších služeb, jimž byla věnována předešlá kapitola a které mají zejména ulehčit práci personálu firmy nebo poskytnout další funkce zákazníkovi. Vždy je velmi dobré pro firmu provozující internetový obchod vymyslet nějaké rozšiřující funkční rozšíření, které je vítáno. Pak takový obchod získá větší renomé. Je to způsob, jak se odlišit od konkurence a získat tak větší podíl na trhu. Často však tyto možnosti nejsou příliš poskytovány, zejména tehdy, pokud se nejedná o perspektivní firmu, která nemá cíl ovládnout určitý segment internetového trhu. Většina podniků totiž případnou realizaci internetového obchodu nechává formou zakázky na bedrech i celkem neprověřených IT firem nebo konkrétních programátorů a velmi často je podnikem vyžadován zejména rychlý vývoj webové aplikace, který s sebou přináší často více problémů než je nezbytně nutné.

[18] Tedy v konečné implementaci by popř. být uvedeny měly

Obrázek 2.4: Objednávka v obchodě



Má implementace neobsahuje žádné významné rozšiřující funkce z pohledu zákazníka, protože jsou obvykle velmi závislé na požadavcích konkrétního podniku a je zbytečné je dopředu implementovat. Stejně tak se to týká vzhledu a funkcionality administračního rozhraní, a to včetně případné vazby na informační systém. Tato součást nebyla vyvinuta právě z těchto důvodů.

Přesto však obchod jako takový obsahuje několik administračních prvků, které lze využít pro stavbu administračního webového či jiného rozhraní.

Kupříkladu je zajištěna možnost odstavení internetového obchodu, např. z důvodu přerušení činnosti či z nějakého jiného důvodu. Tato možnost je aplikovatelná změnou hodnoty řádku v tabulce `data` s hodnotou `server_on`. Prostou změnou této hodnoty na číslo `0` se docílí, že se při návštěvě obchodu zobrazí tato jednoduchá zpráva:

Obchod je přechodně uzavřen. Omlouváme se a doufáme, že nás v nejbližší době znovu navštívíte.

Samozřejmě je vhodnější udělat v této oblasti více při reálném nasazení. V každém případě by však měl být potenciální návštěvník srozuměn s tím, že obchod je momentálně mimo provoz, hodí se také informovat zhruba o příčině problémů a také by neměla chybět informace o době, po kterou bude obchod nefunkční. Lze kupříkladu i nastavit zobrazení určité webové stránky při vzniku chyby, ať je na na straně webového serveru nebo jinde. Všechny moderní servery již tyto funkce mají implementovány.

Dále jsou v našem řešení začleněny prvky primitivního sledování statistik návštěvnosti. V databázové tabulce `pocitadla` jsou umístěny informace o počtu přístupů (tj. kliknutí) na stránky v celkovém souhrnu a k aktuálnímu dni, a dále pak informace o počtu přihlášení registrovaných uživatelů, taktéž jako denní a souhrnná statistika. Kromě toho jsou soustředěny i informace o návštěvnosti jednotlivých stránek. Ty se objevují v tabulce `stranky` ve sloupci `pocitadlo`. Pro reálné nasazení je vhodné sledování statistik rozšířit, aby bylo možné např. sledovat počty kliknutí za účelem zobrazení podrobností k jednotlivým výrobkům.

Aby toho nebylo málo, pro účely administrace se sledují i některé údaje o registrovaných uživatelích. Těmi jsou zejména počet přihlášení, datum registrace a také čas posledního přístupu včetně aktuálního stavu, tedy zda-li je zákazník aktuálně přihlášen apod.

U jednotlivých výrobků se může sledovat informace o tom, zda je daný výrobek na skladě nebo zda je možné ho zákazníkům zajistit. Tyto informace jsou zřejmě nezbytné pro případnou tvorbu administrativního rozhraní a pro interakci s obsluhujícím personálem.

Uvedená implementace nemá za cíl být konečným řešením, další vývoj obchodu odvozeného z tohoto kódu, který je obsahem přílohy č.1, je však při jeho použití značně ulehčen.

Reálné nasazení však vyžaduje drobné zásahy do kódu, které internetový obchod učiní odolným vůči možným útokům.

Pokud se někdo náhodou bude snažit tuto mou implementaci použít pro odstartování vývoje složitější aplikace, zejména může využít již definované třídy (objekty) a rozšířit jejich funkčnost, popř. zapouzdřit i ostatní části kódu do jednotlivých tříd (např. se to týká objednávání zboží). Ostatní části kódu jsou uzpůsobeny pro konkrétní webovou prezentaci, tj. nejsou nezávislé. Profesionální tvorba kvalitního internetového obchodu by určitě vyžadovala daleko pečlivější implementaci, má implementace může tak najít uplatnění zejména v menších firmách s menšími nároky.

Kapitola 3

Bezpečnost

V této poslední kapitole se zmíním o jednom z nejdůležitějších aspektů moderního věku informačních technologií. Se vzrůstajícími nároky na internetová řešení také vzrůstají požadavky na jejich vyšší úroveň zabezpečení. V případě uzavírání elektronických smluv na dálku, tzv. distančních smluv, při provozu elektronického bankovnictví, elektronického obchodu či jiných obchodních aktivit na poli internetu se bezpečnost těchto služeb stává strategickým prvkem. Anonymita a vysoká entropie internetového prostředí je hlavním důvodem, proč se bezpečnost IT služeb dostává do popředí zejména v posledních letech, kdy se možností internetu využívá ke komerčním účelům.

Internet nebyl totiž původně vytvořen za účelem poskytování bezpečného základu pro vývoj komerčních aktivit a jako takový tuto funkci neplní ani dnes. Původním cílem této celosvětové sítě bylo poskytnutí prostředků pro vzájemnou komunikaci na dálku v případě jaderného ohrožení světa za studené války. Během dalšího vývoje se však Internet stal významným pomocníkem pro akademický svět a kromě vojenských účelů našel uplatnění i ve vědecké komunitě. Až teprve s vývojem PC se Internet začal stávat více veřejným prostorem a začal se formovat do podoby, kterou známe dnes po přelomu tisíciletí. Internet dnes představuje virtuální prostor, který je méně regulován dogmaty a omezeními fyzického světa, a jako takový je využitelný pro velký rozsah činností, čemuž odpovídá také obrovský počet lidí připojujících se každodenně do této mezinárodní počítačové sítě.

Se vzrůstajícím využitím Internetu jako prostředku pro provoz podnikatelských aktivit se zvýšená bezpečnost stává nutností, neboť technické know-how související s provozem obchodních aktivit na internetu je z velké části veřejným artiklem a stejně jako ve fyzickém světě existují skupiny jednotlivců, kteří páchají trestnou činnost nebo se snaží vyjádřit své názory a k tomu využívají moderních výrazových prostředků internetu. Ať jsou motivy těchto skupin jakékoliv, v oblasti komerce je potřeba se proti nim aktivně bránit.

3.1 Fikce a skutečná realita

V oblasti bezpečnosti počítačů je zejména z důvodu všeobecného nedostatku porozumění veřejnosti rozšiřováno plno nepravd či polopravd, což vede k tomu, že tato oblast trpí velkým množstvím předsudků. Zejména televizní pořady[1] a také neerudované známé osobnosti značně deformují názor veřejnosti na toto téma a vytváří atmosféru strachu a nepřátelství vůči různým skupinám lidí, kteří se snaží na nízkou bezpečnost sítí a počítačů upozornit z jiného důvodu než k páchání trestné činnosti. Skutečnost je tak obvykle daleko méně fantastická než je uváděno v médiích. Ostatně to ještě stručně zmíním v jedné z dalších částí tohoto textu.

Skutečná realita je značně odlišná, to však nic nemění na tom, že důsledky bezpečnostních slabin v informačních systémech jsou obvykle značné a mohou v mnohých případech i značně ovlivňovat chod podniků, a to zejména v oblasti B2B transakcí.

Ještě předtím než začnu podrobněji popisovat některé otázky bezpečnosti, můžu říci ze svých vlastních zkušeností a postřehů, že je téměř ojedinělým jevem najít takový informační systém[2], který je zabezpečen natolik dobře, aby se nedal úspěšně napadnout bezpečnostním analytikem – auditorem – či zkušeným hackerem z určité pozice. Dá se také říci, že s rostoucím počtem funkčních schopností a s rostoucí sofistikovaností operačních systémů a softwaru se tato bezpečnost relativně snižuje: Naopak však zřejmě i s rostoucím používáním neproprietárního softwaru, častou aktualizací programového vybavení a lepší administrací se velmi výrazně zvyšuje.

Vytvoření systému, který bude odolný proti potenciálním útokům zvenčí i zevnitř je otázkou velmi odborných znalostí a zkušeností, a tak najdou tyto předpoklady uplatnění zejména v armádě, v bankovním sektoru, ve velkých podnicích nebo v podnicích specializovaných na tuto problematiku.

3.2 Mezinárodní normy a standardizace

Stejně jako v průběhu času v každém oboru lidské činnosti, vznikla v posledních letech i v oboru informačních technologií jakási „byrokracie“, jejímž úkolem je definovat modely bezpečného informačního systému. Výsledkem takových snah jsou mezinárodní a národní normy pro informační bezpečnost. My se zde o nich nebudeme podrobněji zmiňovat, jen stručně zmíníme ty, které mají velký význam.

[1] Zejména velká část nekvalitních amerických seriálů

[2] Pod tento termín bych zařadil zejména ERP, groupware a project management systémy

Informační bezpečnost je obecně definována jako *stav, kdy je dosaženo definované úrovně dostupnosti, důvěrnosti a integrity informací v informačním systému, resp. jako proces směřující k tomuto stavu* [34, Sustr03].

Nejdříve si ale musíme uvědomit, že za účelem vytváření informační bezpečnosti již byly podniknuty před několika lety kroky, jejichž výsledkem jsou dnes **(mezi)národní normy a standardy**. Tyto dva termíny jsou nejen v literatuře často zaměňovány, tady si objasníme jejich význam. Asi je nutné podotknout, že pojem „standard“ vychází z anglického jazyka, kdežto pojem „norma“ je spíše termín německého původu [33, Vystavelova02]. Obě slova asi původně byla významově zaměnitelná, dnes se ale hlavně v důsledku doporučení normalizačních organizací v Evropě (i u nás) slova nepovažují za synonymická. Je to tedy částečně také lingvistický problém, který však v USA či Velké Británii asi neexistuje a nevím, jak tyto dvě úrovně standardizace odlišují.

Pod pojmem *standard* se rozumí zejména dokument popisující technické údaje a politiku doporučené implementace a tyto standardy jsou obvykle vytvářeny konsorcii uživatelů a výrobců IT. Tyto dokumenty nejsou závazného charakteru, jsou však obvykle všemi zainteresovanými subjekty dodržovány. Také jsou výrazně starší než mezinárodní normy, které právě z nich často vycházejí.

Pojem *mezinárodní norma* se dá chápat stejně jako jakákoliv jiná norma, např. norma jakosti apod. Normy upravující IT vznikly obvykle začleněním standardizačních opatření, tedy standardů. Jsou však výsledkem o dost většího kompromisu mezi členy těchto organizací. Tyto normy jsou v případě dohody různých stran považovány za závazné, a proto nejsou obvykle tak často implementovány. Většina norem je psána obecněji než standardy, nezabývají se tak mnoho technickými detaily, pokud nejde o telekomunikační technické normy. Např. díky těmto organizacím si teď můžeme na internetu prohlížet video v reálném čase.

Pro rozvoj IT je velmi důležité uplatňování standardů, zatímco normy svou větší rigiditou pokrok spíše trochu zpomalují. Přesto najdou normy uplatnění zejména při implementaci komerčních IT řešení, neboť jsou jasně definovány a obvykle jsou i jednodušší k implementaci, protože je v nich dodržována určitá míra abstrakce. Na základě uplatňování těchto norem normalizační organizace vydávají i vlastní certifikáty.

Teď si vyjmenujeme některé základní organizace, které připravují mezinárodní či národní normy v oblasti informační bezpečnosti. Mezi nejvýznamnější normalizační organizace patří tyto tři:

- ISO - International Organization for Standardization
- IEC - International Electrotechnical Comission

- ITU - International Telecommunications Union

Nejznámější organizací je určitě ISO, jejímiž členy je více jak 140 zemí světa. Její pole působnosti je velmi široké, pouze elektrotechnické a elektronické normy zůstávají v působnosti IEC. Organizace ITU je součástí hierarchie OSN a byla založena už v roce 1865 na principech spolupráce mezi vládami a soukromým sektorem.

Pro certifikaci informační bezpečnosti se dnes nejčastěji používá a uznává nejznámější norma **ISO 17799**, která byla z velké části vytvořena z mezinárodně uznávané britské technické normy BS 7799. Tato norma poskytuje organizacím vodítka a kritéria pro porovnání stavu bezpečnosti informačních systémů. Vedle této normy, která je dnes i součástí českých norem (ČSN ISO/IEC 17999), je známá též obecná norma ISO 9000:2000, která s předešlou velmi souvisí.

Normalizační organizace v Evropě jsou představovány organizacemi CEN (Comité Européen Normalisation), CENELEC (Comité Européen de Normalisation Eléctrotechnique) a ETSI (European Telecommunications Standards Institute).

Mezi další známé organizace patří americké ANSI (American National Standards Institute), IEEE (Institute of Electrical and Electronics Engineers) a mezinárodní IETF (Internet Engineering Task Force), které vydává „internetové standardy“.

Koncepcí informační společnosti se zabývá v Evropě zejména uskupení okolo CEN s názvem CEN/ISSS (Internet Information Society Standardization System), které je známé svou poměrně neformální standardizací a dobrou komunikací s trhem informačních a telekomunikačních služeb. Z hlediska bezpečnosti informačních systémů je dnes nejdůležitější iniciativa EESSI v rámci této organizace.

Výčet všech dalších oficiálních i neoficiálních standardizačních a normalizačních institucí by zahrnul nejméně dalších pár stránek textu, proto zde tímto jejich výčet ukončím a řekneme si něco o internetových standardech.

Internetové standardy jsou v dnešní době reprezentovány hlavně dokumenty, které vydává konsorcium W3C nebo IETF. Zájmem konsorcia W3C jsou hlavně standardizace značkovacích a stylových jazyků pro výměnu dokumentů přes internetové sítě (XML, XHTML, HTML, DSSSL, CSS, XSL, . . .). Tyto standardy jsou všeobecně přijímány a respektovány.

Širší oblast standardizace v oblasti (bezpečnosti) informačních technologií zaujímá IETF, která vydává veřejně dostupné dokumenty RFC (Request for Comment). Protože jsou tyto dokumenty vždy veřejně přístupné a ne nějakým způsobem uzavřené jako u některých jiných normalizačních organizací, jsou středem zájmu všech dotčených subjektů a velmi se na jejich tvorbě i podílí. Celý chod internetu je v dnešní podobě výsledkem uplatňování výsledků této

činnosti. Nejdůležitějšími RFC v této oblasti jsou ty, které popisují jednotlivé internetové protokoly nutné pro běh internetových služeb (HTTP, FTP, SMTP, ...). Tyto dokumenty RFC jsou základem terminologie a nomenklatury dnešních IT specialistů. Časem se většina z nich stává součástí nějaké normy mezinárodní normalizační organizace.

Vedle těchto standardů se do hry dostává obvykle z pozice síly i softwarový gigant Microsoft, který vytváří též své – „pseudo-standardy". Ačkoliv některé z nich jsou buď uzavřené nebo jen omezené uzavřeným světem komerčních microsoftích technologií – jinými slovy tedy těžko použitelné – občas se objeví některý, který internetovou veřejnost inspiruje k běžnému použití i na jiných platformách[3]. V každém případě by však mělo být zvykem, že jakékoliv standardy a normy vydává nezávislá, nevládní a nezisková organizace s mezinárodní působností. Není možné obvykle implementovat soukromé standardy, pokud jsou nízké kvality a v konečném důsledku dokonce úroveň bezpečnosti informačních systémů výrazně snižují.

3.3 Volba operačního systému, síťového řešení a softwaru

Pro bezpečnost informačního systému je volba operačního systému, provozovaného softwaru a síťových prvků a jejich konfigurace přímo strategickou otázkou. Vyřešení této otázky se často neřeší dost důkladně a v konečném důsledku může vyústit i přes velkou snahu administrátorů k tomu, že je konečné řešení informačního systému nakonec přesto nezabezpečené. V tomto oddíle se budu snažit přeformulovat názory odborníků, které jsem postřehl během pár posledních let, a přidám i své názory na problematiku. Berte tyto odstavce jen za jakýsi pokus o trochu subjektivně zabarvený popis dnešní situace, nikoliv jako obecně danou realitu. Na to nejsem zdaleka dost erudován a i mezi odborníky existuje obrovské množství různých názorů.

Budeme se zde zabývat pouze případem, kdy volíme pro provoz svého internetového obchodu vlastní prostředky. Informace však platí i pro provozovatele internetových služeb.

Nejprvnějším úkolem při tvorbě bezpečného systému pro provoz internetového obchodu je návrh počítačové sítě a její konfigurace. K tomu se dnes využívají nejčastěji běžná síťová zařízení (huby, mosty, switche, ...) nebo i postarší počítače s instalovaným operačním systémem, obvykle např. jednodisketovou distribucí Linuxu, které všechny funkce těchto zařízení spojují do jednoho místa. Je také možné na takto slabých počítačích zprovoznit i jednodušší firewall na bázi filtrace či bránu, proxy[4] apod. bez potřeby existence dalších počítačů a operačních systémů v síti. Mělo by být pravidlem při provozu webového serveru s internetovým obchodem

[3] Jedním takovým je např. protokol SMB (Server Message Block) nebo některé autentizační protokoly (např. CHAP)

[4] K těmto účelům už jsou potřeba alespoň běžné počítače a rozsáhlejší linuxové distribuce či jiné operační systémy

jeho oddělení od zbytku vnitřní podnikové sítě, tj. umístit ho na tzv. **demilitarizovanou zónu**. V případě menších podniků k tomu stačí zavést do sítě jeden síťový prvek či počítač, v případě podniků s většími bezpečnostními požadavky lze postavit sofistikovanější firewall nebo doporučit stavbu internetového frontendu. Pokud bude internetový obchod velmi často navštěvovaný, např. bude hrozit přetížení webového serveru, lze postavit i webovou farmu složenou z několika počítačů a implementovat nějaký prostředek vyrovnávání zátěže. Možností, jak postavit funkční a bezpečnou počítačovou síť složenou z několika fragmentů s různými účely, je velmi mnoho a prostředků také. Pro nás tyto informace zde ale nejsou důležité, proto se jimi nebudeme vůbec zabývat.

Na počítačích podnikové sítě, máme-li ji v podniku vytvořenu, je nutné zvolit vhodné operační systémy. Velmi záleží na účelu, který má daný operační systém splňovat. Pro práci na jednoduché uživatelské úrovni u zaměstnanců je nejlepší použít systémy Microsoft Windows pro svou jednoduchost používání a z důvodu velkého množství použitelného aplikačního softwaru. Alternativně lze pro desktopové účely využít i Linux, je-li vyžadována navíc velká stabilita systému a bezpečnost ve vnitřní podnikové síti. To však jen tehdy pokud existují všechny potřebné aplikace nutné pro práci. V jiných případech se na uživatelské úrovni uplatní též systémy Mac OS X, Lindows OS (někde nazývané L—s OS) či další Unix-like či BSD-like systémy, ale obyčejně s určitými omezeními.

Počítače, které mají zabezpečit a poskytovat služby pro klientské počítače zaměstnanců, je nutné vybavit poněkud odborněji. Serverová část sítě by kvůli požadavkům na stabilitu a spolehlivost měla být vybavena vyspělými a kvalitněji nastavenými operačními systémy. V tomto ohledu již použití systémů Microsoft Windows na těchto počítačích z mnoha důvodů obvykle není příliš vhodné (možná dnes s výjimkou Windows 2003 Server), je lépe využít serverově více orientované systémy, mezi které patří hlavně Linux, Free|Open|NetBSD, Solaris, Irix a v případě velkých bezpečnostních požadavků specializované unixové systémy, tj. BSD Unix, HP/UX nebo určité velmi kvalitní linuxové systémy (Corporate Server) apod. Platí, že s rostoucími požadavky velmi výrazně roste cena pořízení OS. Zatímco náklady na pořízení operačních systémů pro klientské aplikace mohou být průměrné (Microsoft Windows) nebo téměř žádné (Linux, FreeBSD), u serverových řešení se pohybují obvykle v desetitisících až statisících korun, přestože je možné vystavět také i vlastními silami bez-nákladová linuxová řešení, která budou také vyhovující a přitom budou stát jen cenu práce za konfiguraci a administraci. Ta však v těchto případech bude také relativně vysoká.

Dále je nutné v případě použití různých platforem v jedné síti řešit i občasné problémy s kompatibilitou, které se snaží některé systémy implementovat (standardy, normy a i některé proprietární technologie) a některé nikoliv. Firma Microsoft dokonce dosažení této kompatibility záměrně brání, zřejmě pouze ze zištných důvodů. Ostatně to je také jeden z důvodů, proč

je soustavně ze strany EU vyvíjen tlak na změnu politiky této firmy [36, Hlavenka04], neboť interoperabilita je důležitým pilířem k vývoji evropské informační společnosti[5].

Otázka volby vhodného softwaru je značně závislá na používaných operačních systémech na klientských počítačích i serverech. Pro provoz internetového obchodu, tedy webového serveru, je nejvhodnějším řešením téměř vždy velmi vyspělý a mnoha lety vyzkoušený server Apache od firmy Apache Software Foundation. Dnes už i implementace pro Microsoft Windows má podobnou stabilitu jako standardní instalace na Unix-like systémech, takže není tolik důležité, jaký operační systém použijeme. Na poli webových serverů je ale plno jiných kvalitních, přestože méně známých webových serverů, které je vhodné použít. S určitými bezpečnostními úpravami, které dnes bohužel spočívají ve vypnutí většiny nabízených funkcí a úpravou operačního systému, pak i Microsoft IIS je možné použít, je-li nutně vyžadováno používání technologie ASP.NET. Existuje zde už i možnost provozu ASP a .NET s určitými omezeními i mimo platformu Windows, pokud je to nutné pro zvýšení bezpečnosti.

Webový server však není jediným softwarem, který se na operačních systémech pro účely provozu internetového obchodu používá. Zejména v případě volby linuxového řešení se tento systém obyčejně v běžných distribucích skládá ze stovek až tisíců téměř nezávislých programů, jejichž bezpečnost může být za určitých podmínek prolomena, což ale jen ojediněle vede k ovládnutí celého systému. V případě systému Microsoft Windows je těchto programů výrazně méně, ale zejména z důvodů výrazně menší bezpečnosti systému jako celku a provázanosti jednotlivých komponent je využití nedostatku v jedné komponentě automaticky možné zneužít pro páchání větších škod v systému. Jelikož však už všechny novější systémy Microsoft Windows (Windows NT, Windows 2000 (Server), Windows XP, Windows 2003 Server) převzaly unixovou politiku přístupových práv k souborovému systému, už i dnes jsou méně zranitelné než před pár lety.

Pro systémový i aplikační software počítačů by se měly dodržovat některá základní bezpečnostní pravidla. Hlavním pravidlem je **častá aktualizace**, i kdyby to u některých systémů mělo znamenat neustálé stahování oprav z internetu. Jen tak je možné obvykle zajistit jeho bezpečnost. Dalším pravidlem je **instalace jen nutného softwaru**, což snižuje úspěšnost průniků do systému. Není např. nutné mít na počítači, který má pouze poskytovat služby poštovního serveru, instalovány jiné serverové aplikace či dokonce klientský aplikační software. Třetím důležitým pravidlem je **odborná administrace**. Je totiž úplně zbytečné mít nainstalován ten nejlepší právě dostupný operační systém se všemi updaty, pokud mezi počítačem a židlí sedí BFU[6].

[5] V této problematice se angažuje evropský komisař Mario Monti

[6] Česky slušně přeloženo jako „Běžný Franta Uživatel“

3.4 Úrovně zabezpečení

Pokud se zmiňujeme v této kapitole o zabezpečení informačního systému, měli bychom se také zmínit o způsobech narušení bezpečnosti. Protože však cílem této práce není bližší náhled do problematiky, tak si jen uvedeme základní informace o způsobech napadání částí informačního systému, zejména pak pro nás důležitého webového serveru a samotné webové aplikace, která tvoří náš internetový obchod.

Mělo by být pravidlem pro každou velkou firmu provozující vlastní internetový obchod či serverové služby vytvoření komplexní bezpečnostní politiky a tu pak také bezpodmínečně dodržovat. V případě malých firem, kdy obvykle nehrozí v případě narušení bezpečnosti velká ztráta důležitých a zneužitelných dat, není tato politika příliš nutná.

Fyzická bezpečnost

Ať se to zdá možná dost nepochopitelné, největšího narušování bezpečnosti je dosaženo zejména povolením fyzického přístupu k nezabezpečeným počítačům vůči přístupu přes terminál. To platí dnes dvojnásob, neboť **naprostá většina úspěšných útoků** na informační systémy **je prováděna vlastními zaměstnanci**, tj. z vnitřního prostředí. I v případě výborně vůči vnějším útokům zabezpečeného IS je stále lidský faktor tím nejslabším místem bezpečnosti. To si dnes uvědomují zejména bankovní ústavy, které proto implementují sofistikované metody, jak se těmto útokům bránit.

Přestože existují dnes již velmi vyspělé operační systémy, stále je možné nějakým způsobem restartovat počítač a vnutit mu spuštění speciálně upraveného softwaru z média, který umožní často přístup ke všem součástím počítače. K těmto účelům lze využít zejména různé záchranné diskety, CD, nebo specializovanou linuxovou distribuci, která je pro tyto účely vytvářena.

Jak zvýšit fyzickou bezpečnost? To už je dost těžký úkol, který obyčejně není možné dokonale vyřešit. Proto se častěji počítače zabezpečují tak, aby případný fyzický útok nebyl úspěšný. Lze na citlivých místech využít šifrované souborové systémy s proměnnými klíči, znemožnit nabootování počítače kýmkoliv[7], používat na většině důležitých míst bezdiskové stanice, používat počítače bez možnosti použití výměnných médií, znemožnit krádež přenosných médií, disků, notebooků apod. Lze taktéž vymezit vlastní místnost, do které je umožněn přístup jen v ojedinělých případech (poruchy, administrace, ...), popř. také s dozorem, nebo použít jiný přímější způsob.

[7] Např. lze vyžadovat zaheslovaný přístup do BIOSu

Nelze také opominout nebezpečí použití **sociálního inženýrství**[8] některým externím zaměstnancem nebo úplně neznámou osobou, která se bude kupříkladu představovat jako „administrátor“ nebo „technik“, vynutí si spolupráci člověka, od kterého „potřebuje pomoci“, popř. jinou manipulací donutí zaměstnance k umožnění útoku.

Síťové zabezpečení

Zabezpečení sítě bylo popsáno již výše při popisu možných síťových řešení.

Opět bych zde ale poznamenal, že i síťové útoky bývají obvykle směřovány z vnitřních sítí a často jsou tedy výsledkem činnosti firemních zaměstnanců.

U menších podniků a organizací lze využít stavbu klasické sítě LAN[9] s malým zabezpečením klientských stanic[10], u velkých podniků je nutné mít nastaven alespoň jeden počítač s firewallem, proxy nebo sofistikovanějším softwarem pro detekci a obranu před útoky a klientské stanice by měly být také více zabezpečeny.

Systémy zajišťující provoz na síti je vhodné často aktualizovat, a to se týká jak operačních systémů tak firmwaru jednotlivých síťových prvků, jsou-li používány.

Zabezpečení operačního systému

Administrace operačních systémů je vedle volby jeho typu dalším prvkem, který má podstatný vliv na bezpečnost. V případě většiny podniků není nutné mít zaměstnaného vlastního zaměstnance, který má na starosti administrační práce[11]. S rostoucí velikostí podniku se stává potřeba takové administrace velmi důležitá, neboť je obvykle vyžadována větší bezpečnostní úroveň informačních systémů.

Prací administrátora se zejména rozumí udržování operačních systémů v provozuschopném stavu, aplikace bezpečnostních záplat, sledování aktuálního vývoje v oblasti bezpečnosti a také občasné technické práce související s provozem sítě (síťový administrátor).

[8] Jde o snahu útočníka získat pomoc při útoku od další osoby tím, že ji obelstí či uvede v omyl

[9] Local Area Network – místní počítačová síť

[10] Klasické řešení pro většinu školských zařízení

[11] Snad jen v případě systémů Microsoft Windows je to vhodné i pro menší firmy, přestože je administrace těchto systémů většinou velmi jednoduchá

Softwarová bezpečnost a kritický význam bezpečnosti na úrovni webové aplikace

O softwarové bezpečnosti jsme si již něco řekli, z hlediska bezpečnosti webové aplikace (našeho internetového obchodu) je však velmi důležitá **bezpečnost skriptového kódu**. Vesměs jsou to chyby programátora, které mohou z webové aplikace vytvořit vděčné místo pro pokusy zkušeného crackera. Je to taktéž nejčastější postup, kterým se dá zkompromitovat určitá webová stránka.

Jak si názorně uvedeme později a na jednom více ilustrativním příkladu, může i velmi malá chybička, překlep či opomenutí při vytváření kódu aplikace vést k velmi důležitým bezpečnostním nedostatkům. Je samozřejmé, že není dnes možné i přes velkou snahu vytvořit programový či skriptový kód tak, aby byl naprosto dokonalý jak z hlediska funkčnosti, tak bezpečnosti. Občas se také stává, že aplikace, která je bezpečná dnes, nemusí být bezpečná v budoucnosti v důsledku rozsáhlých změn v softwaru, který spouští skripty, nebo ve změnách softwaru webového serveru či operačního systému. Ne vždy je aktualizace žádoucí, i když to platí jen v ojedinělých případech.

Protože je však bezpečnostní problematika velmi složitá a v komplexním pohledu není obvykle možné vyznat se ve všech bezpečnostních aspektech skriptů, instalovaného softwaru (i hardwaru), musíme se smířit s tím, že nikdy nebude dosaženo dokonalého stavu. O tom však bezpečnost IS tak úplně není; můžeme opět připomenout již zmíněnou definici informační bezpečnosti, která praví, že tato bezpečnost není pouze stav v daném okamžiku, ale zejména proces směřující k dosažení ideálnímu stavu.

3.5 Vybrané metody infiltrace

Stejně tak jako je nedokonalý jakýkoliv software, platí to samé i pro webové aplikace. V minulém textu jsme si obecně popsali situaci se zabezpečením operačních systémů, softwaru a pro nás nejdůležitějších programů, webových aplikací, pomocí kterých se tvoří vlastní internetový obchod.

V následujícím textu zmíním pár postupů, které se používají pro dosažení kompromitace webové aplikace internetového obchodu. Kvůli omezeným možnostem této práce nebude následující text ani úvodem do téměř nekonečného „moře“ bezpečnostních slabin a informací o počítačových systémech. Věřte, že jen povrchní pohled na tuto problematiku by obsáhl rozsah několika knih.

Nastíním jen základní postupy, kterými útočník obvykle prochází při plánování útoku. Někdy však některé metody nejsou důležité a často bývají i zbytečné, takže neexistuje obecně

platný postup. Často totiž nebývá cílem kompromitace internetového obchodu, ale například získání citlivých informací z databázových systémů, souborového systému, sledování přenášených dat, ovládnutí celého systému za účelem odstartování útoků na jiné systémy atd.

3.5.1 Zjišťování informací, skenování, inventarizace

Předtím, než se začne potenciální útočník zajímat o způsob napadení vzdáleného systému, na kterém je provozována zajímavá webová aplikace, je pro něj občas důležité **získání** všech dostupných technických **informací**, které mu mohou pomoci při volbě konkrétního postupu.

Útočník má v tomto ohledu velmi mnoho informačních zdrojů. Některé z nich jsou veřejně dostupné a považovány za „bezpečné“, k jiným se musí dopracovat složitěji. Nejlépe dostupnými informacemi jsou data zveřejňovaná na informačních serverech pro účely administrátorů. Z těchto informací lze zjistit např. konkrétní rozsahy IP adres[12], kterými firma provozující internetový obchod disponuje, informace o jednotlivých počítačích v podnikových sítích, jména správců, administrátorů, emailové kontakty, instalované operační systémy a hardwarovou vybavenost. Z těchto údajů se dají někdy odvodit dedukcí i další zajímavé údaje. Další údaje, které jsou také veřejné, lze vyzískat prohledáváním obsahu Internetu.

Po zjištění některých základních informací útočník provede jakousi „prohlídku“ počítačové sítě nebo vzdáleného systému, kterému se říká **skenování**. Je-li útočník alespoň trochu znalý problematiky, obvykle touto činností ještě nevzbudí pozornost administrátora. I kdyby se tak stalo, samotné skenování není „trestná činnost“ a není ničím zakázáno. Pouze může vzbudit pozornost, což každý útočník určitě neuvítá. Má-li útočník velmi kvalitně nastavený počítač a vzdálený systém se už při skenování začne o potenciálního útočníka zajímat, může získat i další informace o použité ochraně vzdáleného systému. Skenováním útočník může ale hlavně získat bližší údaje o systémech, zejména o běhu různých služeb a aplikací na systému, verzi operačního systému, informace o poslední aktualizaci systému apod. Při hlubší „prohlídce“ jednotlivých služeb může získat i údaje o nainstalovaném softwaru a jeho konkrétní vývojové verzi. Tyto informace jsou výsledkem procesu inventarizace a bývají již velmi cenné a dají se využít k volbě strategie útoku. Proti těmto útokům se lze bránit z pohledu podniku aplikací vhodného síťového zařízení, filtru či firewallu[13]. Avšak i firewall není někdy neproniknutelný a také útočníkovi obvykle prozradí svou existenci, popř. typ a vzácně i část nastavení.

Pokud je vzdáleným systémem některý ne-unixový systém nebo je vzdálenou sítí síť Novell Netware nebo Microsoft Windows, je navíc obyčejně možné vyzískat i další zajímavé údaje o provozu na síti, o jednotlivých uživatelích v síti, o jednotlivých počítačích, administrátorech

[12] IP adresa je jedinečná síťová adresa v Internetu

[13] Firewall je specializovaný software, který chrání síť před vnějším prostředím

apod. Tyto sítě jsou totiž velmi často nezvykle „upovídané“, což je pro útočníka jedině dobře. Pro nás jako provozovatele webové aplikace je to však hotová pohroma. Dá se to srovnat s únikem osobních údajů. Je-li cílem napadnutí webové aplikace, nejsou podobné informace moc zajímavé.

3.5.2 Profilování a útok na webovou aplikaci

Existuje veliká skupina těch, kteří touží z různých důvodů po kompromitaci webové aplikace. Zejména se útočníci snaží poškodit jméno a image firmy, způsobit hmotnou škodu a poškozovat zákazníky, nebo kupř. zajistit delší nefunkčnost internetového obchodu. I když tento cíl téměř nikdy nemá zkušený hacker, který navíc nepotřebuje získat „popularitu“ a bezúčelně na sebe upozornit, jsou tyto útoky nejčastějšími, téměř výhradně spojené s méně schopnými útočníky vybavenými často jen znalostmi skriptovacích jazyků a hackingu webových aplikací.

Je-li cílem crackera kompromitace webové aplikace, je především nutné získat přehled o její funkčnosti a struktuře. Tomuto procesu se říká **profilování**. Útočník se snaží získat povědomí o tom, jak daná aplikace funguje a najít v ní popř. skrytá místa a programátorovy chyby.

Pro účely profilování aplikace se útočník snaží podsunovat údaje do jednotlivých URL a sledovat reakce a případná chybová hlášení webové aplikace. Vhodnými místy pro testování jsou i HTML formuláře. Podsunuté údaje pak mohou odstartovat typ útoku založeného na nedostatečné kontrole uživatelského vstupu.

Útočník také může propátrávat před ním neskrytý kód webových stránek skriptů, které běží na klientské straně[14] a ze kterých lze získat informace o „stylu“ psaní kódu programátorem.

Uvedeme si dva příklady, které jasně ukáží, co se tímto vším rozumí. Jeden příklad bude demonstrací, jak může vést nedostatečná kontrola uživatelského vstupu k neoprávněnému přihlášení pod cizím uživatelským jménem v internetovém obchodu. Bude použita často používaná a známá metoda nazývaná „SQL injection“. Druhý příklad bude podobný a využijeme webového formuláře. Ten bude výrazně jednodušší.

Následující příklad byl zveřejněn nedávno na serveru www.root.cz, na kterém se soustředí názory a články elity české „IT inteligence“. Příklad vychází z implementace vícejazyčného webu, která byla publikována na internetu. Svým charakterem se tento typ útoku zařazuje k těm, které již vyžadují určité odbornější znalosti.

Skript vícejazyčné webové aplikace řešil vše přes využití databázové tabulky, která v sobě obsahovala řetězce v různých jazycích a měla tuto strukturu (zjednodušeno pro přehlednost):

[14]Tyto skripty jsou prováděny na uživatelově počítači a mají jiné účely než skripty „na straně serveru“, který řídí webovou aplikaci

```
TABULKA msg (
   id INTEGER,          % číselný identifikátor řetězce
   langcz TEXT,         % česká verze řetězce
   langen TEXT,         % anglická verze
   langde TEXT,         % německá verze
);
```

Tabulka tedy obsahuje 4 sloupce, z nichž prvním je číselný identifikátor a další sloupce jsou už řetězce v různých jazykových verzích. Příkladem jednoho řádku tabulky mohou být např. hodnoty – "1", "budova", "building", "Gebäude".

Níže je přibližný kód napadnutelné webové aplikace. Pro nás je zajímavá část věnovaná definici funkce na řádcích 2-9, která způsobuje zobrazení požadovaného řetězce ve zvoleném jazyce. Volba jazyka se provádí v proměnné `lang`, která se přenáší v URL webové stránky. Např. URL „http://www.mujobchod.com/obchod.php?id=1&lang=cz“ by měla na stránce zobrazit nápis `ahoj`, kdežto odkaz „http://www.mujobchod.com/obchod.php?id=1&lang=de“ nápis `Gebäude`. Myslím, že je to jasné.

```
 1:<?
 2: // funkce pro výpis vícejazyčných hlášení
 3: function msg($id,$lang) {
 4:    $result = mysql_query("SELECT lang$lang FROM msg WHERE id=$id");
 5:    if ($result) {
 6:      $row=mysql_fetch_array($result);
 7:      mysql_free_result($result);
 8:      echo $row[0];
 9:    }
10: }
11:
12: // zjištění request proměnné "lang"
13: $lang=$_REQUEST['lang'];
14: if (!$lang)        // pokud proměnná neexistuje, volíme češtinu
15:    $lang='cz';
16:
17: // použití vícejazyčné hlášky
18: msg(1,$lang);
19:
20: // atd...
21:?>
```

Problém však způsobuje nedostatečná kontrola vstupních údajů. Skript se chová tak, že v případě, že je do proměnné `lang` vložena útočníkem jiná hodnota než `cz`, `de` či `en`, stejně se

tato hodnota dostane do výsledného dotazu na obsah naší tabulky se seznamem řetězců. Tento dotaz by v případě prvně zmíněného URL měl mít podobu[15]:

```
SELECT langcz FROM msg WHERE id=1
```

Jednoduše tedy vybere českou verzi řetězce a zobrazí ho na stránce. Útočník si však „zkusí“ vložit do URL nějaký náhodný řetězec a zkoumá reakci aplikace. Pokud například vytvoří zdánlivě nesmyslný odkaz, např.:

„http://www.mujobchod.com/obchod.php?id=1&lang=tojsemja“,

pak mu aplikace ochotně oznámí, že při výběru dat z tabulky msg došlo k chybě, protože neexistuje sloupec `langtojsemja`. Pokud útočník najde takovou slabinu, je „šťastný jako blecha“, protože objevil nedostatek, kterého může využít pro pokusy.

Po objevení možnosti pozměňovat databázové dotazy v tabulce si vytvoří svůj vlastní odkaz, kterým se bude snažit uhádnout název tabulky a sloupce, ve které se kupříkladu ukládají hesla. Nejčastějšími volbami jsou zejména `user`, `users`, `uzivatel`, `uzivatele`, `hoste` apod. V případě sloupců to pak mohou být `heslo`, `pass`, `password` atd. Po zvolení níže uvedeného odkazu může dostat očekávanou odpověď:

```
http://www.mujobchod.com/obchod.php?id=1&lang=.password%20FROM%20user \\
%20lang%20WHERE%20id=1%20/*
```

Po zvolení načtení tohoto odkazu dostane kupříkladu tuto odpověď:

```
skakalpespresoves
```

To už je heslo. Vysvětlení, proč se tak stalo, není tak úplně na první pohled zřejmé. Lepší to bude, když si vysvětlíme, jakým způsobem se dotaz předaný do skriptu přeměnil v dotaz do databáze.

V URL jsou použity znaky `%20`, kterými se vkládají mezery ve formě Unicode[16]. Výsledný databázový dotaz bude vypadat takto:

```
SELECT lang.password FROM user lang WHERE id=1 /*FROM msg WHERE id=1
```

[15] Dotaz vychází z řádku č. 4 kódu skriptu

[16] 16ti či 8bitové kódování, které se užívá pro použití všech dostupných znaků různých světových jazyků; jejím prostřednictvím je možné na internetových stránkách zobrazovat desetitisíce různých znaků

Ani teď nemusí být pro laika smysl patrný. Pokusím se vysvětlit, co se díky tomuto dotazu v databázi stane. Dvěma dalšími slovy za řetězcem `FROM` v dotazu se vytvoří synonymum (tzv. alias) pro tabulku `user` (jejíž název je předpověditelný) a toto synonymum (`lang`) se zneužije pro vstup do tabulky s uživatelskými daty, kde se získá údaj o heslu (`lang.password`) uživatele s identifikátorem `1`. Vše v dotazu, co je uvedeno za znakem `/*` je poté ignorováno.

Další práce crackera je již lahůdkou. Vytvoří si nějaký automatizovaný skript (obyčejně v Perlu[17]), kterým celou akci zrychlí pro výběr „všech“ uživatelských hesel v databázi. Pro tento případ jsem si vytvořil tento jednoduchý jednořádkový skript (v jazyce Bash) pro ilustraci. Ten stačí spustit na linuxové konzoli:

```
i=1;while();do echo -ne "GET obchod.php?id=$i&lang=.user%20FROM%20lang \\
%20WHERE%20id=$i%20/*"|nc www.mujobchod.com 80 >> hesla.txt; echo -ne ":"; \\
echo -ne "GET obchod.php?id=$i&lang=.password%20FROM%20lang%20WHERE \\
%20id=$i%20/*"|nc www.mujobchod.com 80 >> hesla.txt;echo -ne "\n";$i++;done
```

Skript jsem osobně nezkoušel, ale obyčejně je to pro zkušeného crackera hračka. Po předpokládaném výběru dostatku hesel skript útočník jednoduše ukončí a v souboru `hesla.txt` mu zůstanou pouze uživatelská jména a hesla v této podobě:

```
novak:jajsemtrouba
novotny:tohlenikdoneuhadne
prochazka:dkfs8df8
franta:atnarf
zikmund:hanzelka
...
```

Hezké. A teď má útočník vše jako na dlani. Buď se rozhodne hesla použít k plánovanému útoku, kdy může prostřednictvím automatizovaných skriptů v určitých časových periodách objednávat na všechna uživatelská jména výrobky a zahltit tak administraci a poškozovat obchod i jednotlivé uživatele, nebo může provést útok zahlcením, čímž může znemožnit práci internetového obchodu na nejméně pár hodin. Možností je neomezené množství.

V žádném případě takovéto útoky nemusí být „tak složité“. Někdy stačí i prosté vyplnění do políček formuláře, do kterých se uvádí uživatelské jméno a heslo při přihlašování zákazníka k obchodu. Do políčka uživatelského jména zadá jakékoliv předpokladatelné jméno (např „novak“) a do políčka s heslem připravený dvoulomítkový řetězec, např. typu „`'-"`. Je-li webová aplikace psána programátorem – laikem a kontrolu přihlášení provádí dotazem „SELECT * FROM uzivatele WHERE jmeno='$jmeno' AND prijmeni='$prijmeni'“[18] bez hlubší kontroly údajů zadávaných uživatelem, konečný dotaz může mít podobu:

[17] Skriptovací (interpretovaný) jazyk s neobyčejně velkými schopnostmi

[18] Tento dotaz byl záměrně zjednodušen pro přehlednost, není přesný. Dolary jsou označené proměnné.

```
SELECT * FROM uzivatele WHERE jmeno='novak'--' AND heslo=''
```

a za určitých podmínek také může vést ke kompromitaci webové aplikace a útočník si dosažením falešné autentizace může objednávat zboží přes cizího uživatele, změnit u něj osobní údaje, adresu apod. Důvodem je totiž skutečnost, že v daném dotazu je vše za znaky dvou pomlček ignorováno.

Naše webová implementace by měla být vůči těmto útokům víceméně odolávat, i když to nemůžu zcela zajistit. Na místech zdrojového kódu, kde je v komentářích uvedeno slovo „SFBUG“ je zřejmě možné nějakým způsobem prolomit bezpečnost internetového obchodu. Hlavní obranou obchodu je taková práce programátora, která spočívá v dokonalé kontrole vstupů do aplikace, které mohou být „falšovány“ útočníkem. Těchto vstupů může být veliké množství, a proto je psaní bezpečného kódu obvykle několikrát pomalejší než obyčejné psaní kódu.

Důležitým bezpečnostním prvkem pro obranu uživatelů internetového obchodu je také využívání šifrování hesel, které může zamezit masovému zneužití. Pokud hesla uložená v databázi zašifrujeme např. hashovací funkcí MD5, má útočník místo dat ve formě „novak:mojeheslo“ v podobě „novak:b26e58c375375aa974938a801c581f40“. To už klade útočníkovi do cesty velikou překážku, přestože se mu podaří kompromitovat aplikaci. Díky nesvědomitosti většiny uživatelů a volbě slabých hesel však je možné i tyto nepřehledné řetězce rozšifrovat alespoň pro část uživatelů obchodu.

O možnostech webového hackingu by se dalo napsat daleko více, myslím ale, že předcházející text alespoň trochu uvedl do problematiky i laiky, kteří o takových věcech ani neslyšeli a myslí si, že se problémy z bezpečností týkají pouze operačních systémů.

3.5.3 Síťové útoky

Napadání počítačových sítí útočníky je poněkud odbornější záležitost. Tyto útoky vedou k takovým typům narušování bezpečnosti, kterých si nemusí administrátoři u počítačů v síti všimnout. Výsledkem může být situace, kdy jsou počítače napadány např. za účelem využití počítačů v síti pro útoky na jiné vzdálené systémy.

Mezi tyto typy útoků patří pokusy o kompromitaci sítí VPN[19], hlasové pošty, síťových zařízení[20], firewallů a k provádění útoků typu DoS a DDoS[21].

[19] Virtual Private Network – typ zabezpečení počítačové sítě

[20] Těmi zde rozumím zejména různé přepínače, huby, směrovače, opakovače, mosty apod.

[21] DOS = Denial of Service, DDoS = Distributed DoS - metody útoků sloužící k zahlcení sítě

Protože tyto útoky vyžadují poměrně značné know-how, je těchto útoků spíše menší množství. Nejčastějšími v této oblasti jsou útoky typu DoS a DDoS, které mají za účel zahltit nepřátelskou síť takovým způsobem, aby nemohla vyřizovat požadavky klientů. DDoS je typ útoku, kdy se zahlcení cizí sítě využívá skrze napadení stovek, tisíců až desetitisíců cizích napadených počítačů. K těmto útokům jsou zejména náchylné všechny verze operačních systémů Windows a k napadání jsou konstruovány internetové červi a viry. Dnes je možné za využití těchto „přátelských“ operačních systémů napadnout jakýkoliv webový či jiný server. A to dokonce i v případech, kdy jsou na straně provozovatele webových služeb aktivní i stovky počítačů spojené do webové farmy za tímto účelem.

3.5.4 Útok na operační systém a softwarové komponenty

Kromě výše zmíněných útoků je bezpečnost operačního systému a na něm běžícího softwaru dalším rizikem pro provoz internetové aplikace. Zjištění bezpečnostní chyby v softwaru může vést ke kompromitaci samotné webové aplikace, přestože ta může být na své úrovni zabezpečena velmi dobře.

Útoky na operační systém lze zařadit mezi méně zdařilé, přesto je neustále nutné pro jeho bezpečnost aplikovat průběžně všechny nutné bezpečnostní opravy. Pokud však ani po aplikaci oprav není zabezpečen operační systém, měl by se přestat používat a nahradit vyspělejším. Na poli úrovní bezpečnosti operačních systémů dnes bojuje několik operačních systémů, mezi nimi hlavně můžeme jmenovat systémy BSD Unix a jejich klony (FreeBSD, NetBSD, OpenBSD), HP/UX, Solaris, Linux, ... Možná lze do těchto systémů zařadit i poslední verzi systému firmy Microsoft (Windows Server 2003), u kterého též nebylo v poslední době nalezeno tak výrazné množství chyb jako v minulých verzích. Je však pravidlem, že s větší úrovní integrace operačního systému se tento systém stává méně bezpečným, proto mají modulárně řešené systémy dodnes výrazně větší úroveň zabezpečení a stability.

Příkladů narušení bezpečnosti samotného operačního systému a softwarových komponent je bezpočet, např. na úrovni produktu Internet Explorer lze najít dnes mnoho desítek chyb či „vlastností“, které mohou vést i k pádu operačního systému. Jedním takovým příkladem je např. začlenění níže uvedeného textu do kódu webové stránky [39, SecNet].

```
{cssText: font-weight: bold;}
```

Tento primitivní text způsobí pád IE a na mnoha systémech i pád celého systému Windows (týká se především Windows 98, méně pak pro Windows 2000). Toto je jen kratičký příklad toho, jak lze úspěšně argumentovat tím, že integrace celého operačního systému může být více

riziková. Toto je jen velmi primitivní chyba a navíc nemá žádné výrazné důsledky, její použití zvládne i běžný uživatel. Velká část chyb však bývá daleko závažnější[22].

Z hlediska bezpečnosti webové aplikace je nejvíce zranitelným místem **webový server**, který jeho funkčnost zajišťuje. Zde jsou nejnebezpečnějšími servery téměř všechny verze serveru IIS. Jeho většina verzí je zranitelná takovými způsoby, které vedou buď k prozrazení zdrojového kódu webové aplikace, ke způsobení restartu celého systému či k ovládnutí celého systému [37, HBTwebaplikace03]. Všechny tyto možnosti vedou k tomu, že je webová aplikace ve velikém ohrožení. Poslední verze IIS 6.0 je již proti některým způsobům napadení imunní, obvykle však za cenu nefunkčnosti většiny jeho funkcí. Přestože systémy Windows už před několika lety implementovaly unixový způsob práv do souborového systému NTFS, stále je eskalace práv[23] na těchto systémech velmi dobře možná.

Co se týče webových serverů, i dnes nejlepší webserver Apache není úplně bez chyb. Přestože je samotné jádro serveru téměř dokonale bezpečné, různé rozšiřující moduly běžící s právy, jaké má webserver[24], mohou být zdrojem bezpečnostních nedostatků. Takže ani „modularizace“ nemusí být vždy výrazně bezpečnější než „integrace“ na úrovni jednotlivých softwarových komponent. I přes všechny tyto skutečnosti je použití serverů Apache a IIS pro provoz webu stejně často používané. Ostatní webservery se dělí o zbylých pár procent na trhu.

Podle mého názoru jsou nejdůležitější součásti jádra Internet Exploreru zrcadlícího se v mnoha dalších integrovaných součástech operačního systému Windows a webserver IIS největším zdrojem bezpečnostních hrozeb pro moderní webové aplikace a celý Internet. Jejich nepoužíváním by se značně eliminovaly dnešní velké bezpečnostní problémy s činností Internetu jako celku. Zatímco se téměř většina dalšího software na různých operačních systémech průběžně inovuje téměř každý týden, jádro Internet Exploreru je v téměř nezměněné podobě už téměř 5 let a aplikují se u něho pouze bezpečnostní opravy a jen malé množství nových funkcí. Zřejmě tato práce zcela vyplní čas stovek programátorů, jinak si to neumím vysvětlit[25].

3.5.5 Útoky na klientské aplikace

Pokud je pro provoz webové aplikace nutná bezpečnost serveru, pak pro útoky na klientské aplikace je důležitá bezpečnost našich zákazníků. Je totiž stejně tak důletité neohrožovat

[22] Např. vyzrazení obsahu paměti na systémech Windows XP při síťovém útoku [40, SecFocus], přetečení bufferu na systému Linux vedoucí k získání práv uživatele „root“, mazání celých adresářů na systému Windows XP [41, Nexx02], ...

[23] Získání silnějších práv v systému

[24] Tedy pokud neběží server na jednouživatelských Windows

[25] Je však ale nutné říci, že zobrazovací schopnosti IE byly v mnoha předešlých letech téměř vždy na vyšší úrovni než u konkurence; dnes tomu už tak není a neustále nové bezpečnostní chyby a zastarávání uživatelského rozhraní teď vyúsťují v odklonu i neinformovaných uživatelů od používání IE

prostřednictvím vlastních chyb bezpečnost zákazníků u počítače.

Při špatné implementaci webové aplikace je totiž dost pravděpodobné, že umožníme útočníkům napadat vlastní zákazníky. Proč? Je to možné skrze vkládání kódu přímo do webových stránek zobrazených všem klientům[26]. Tento kód má obvykle podobu nepřátelského Javascriptu, JScriptu, VBScriptu či odkazu na javovský applet. Také je možné manipulovat s ActiveX komponenty, ukrást uživatelská „session“, cookie nebo zneužít počítač pro útok na další systémy na internetu.

Možností je v tomto ohledu mnoho, nejvíce zneužitelným softwarem pro tyto útoky je opět s neuvěřitelně bezkonkurenčním náskokem produkt Internet Explorer firmy Microsoft. Tyto útoky mohou být směrovány i na jiné webové prohlížeče či jiný software, především však díky malé úspěšnosti takových útoků a menšímu využívání jiného softwaru je to víceméně rarita.

Důsledky takových útoků jsou zejména ztráta anonymity na internetu, smazání jakýkoliv dat na disku, ukradení uživatelských dat, náhlé pády softwaru i operačního systému Windows[27], virová nákaza s různými důsledky, instalace trojských koňů a zadních vrátek do systému a také často nenávratná ztráta dat na disku vedoucí i k narušení instalace systému.

Způsoby, jak se proti těmto útokům bránit je dost, jsou však málo využívány. Obvykle to vyžaduje na straně uživatele počítače určitou činnost, o jejíž nutnosti se však někdy ani nedozví a navíc ho to obvykle ani nezajímá. Tyto útoky patří mezi nejčastěji používané, protože si jich uživatel u počítače často ani nevšimne. Často vedou k nejzávažnějším důsledkům. Většinu takových útoků mohou provádět i uživatelé bez větších znalostí. Důsledky těchto útoků jsou navíc tím úspěšnější, čím je více využíváno nelegální kopií operačních systémů (zejména Windows), tj. když nemohou být dobře využívány poslední aktualizace softwarového vybavení.

Na závěr uvedu skromný příklad ze světa Internet Exploreru, ale i Mozilly. Oba prohlížeče byly postiženy chybou, která umožňuje klamání uživatele prohlížejícího si internetové stránky skrze vytvoření speciálně formulovaného URL odkazu [41, Nexx02], který uživatele sice seznámí s obsahem požadované stránky, zároveň je však připojen k cizí stránce, která může být upravena tak, že bude sledovat činnost uživatele. Tohoto nedostatku dnes využívají některé internetové červi. Uživatel si této činnosti obvykle nevšimne. Řešení aplikací opravy bylo otázkou pár hodin u prohlížeče Mozilla, společnost Microsoft se však rozhodla používání daného formátu URL odkazů rovnou „zakázat“, aniž by se nějak snažila problém v softwarovém kódu lokalizovat a stejně tak jako v případě dalších předešlých stovek problémů chybu úspěšně opravit. Opět další krok zpět k neuplatňování mezinárodních internetových standardů u nejčastěji využívaného webového prohlížeče.

[26] Lze pro tento účel použít zejména metodu „cross-site scripting“

[27] Na jiných operačních systémech tyto útoky nemají takové důsledky

3.5.6 Viry, červi a jiná "havěť"

Téměř každý člověk trávící u počítače alespoň pár dnů v roce byl vědomě i nevědomě konfrontován s počítačovými viry či jejich modifikacemi v podobě trojských koňů, backdoor aplikací, internetových červů apod. I když se tyto nepřátelské programy týkají z obrovské části pouze uživatelů systémů Microsoft Windows, svou aktivitou znepříjemňují život také uživatelům používajících jiné operační systémy. Hlavně však ohrožují a zpomalují běh Internetu jako celku.

Obrana proti obrovskému množství virů, jejich mutací a modifikací a jiných programů je velmi omezená. Viry jsou důsledkem existence obrovského množství chyb v proprietárních uzavřených systémech a nedostatečného dodržování či implementace mezinárodních standardů. Je možné se bránit prostřednictvím počítačů filtrujících a odstraňujících viry na cestě od útočících systémů k uživatelům. Tento způsob však dnes ještě není na dobré úrovni a navíc není ještě uzákoněna odpovědnost poskytovatelů internetových služeb za jejich nepoužívání[28]. Situace se ale časem zlepšuje, zřejmě v důsledku zvětšujícího se tlaku veřejnosti na poskytovatele internetových služeb. Dalším řešením je instalace antivirového softwaru na uživatelově počítači a jeho neustálá aktualizace. Žádné řešení však není dokonalé.

Viry jsou dnešním internetovým fenoménem. Jejich schopnosti jsou stále větší a způsoby jejich eliminace vyžadují sofistikovaná řešení či nějaké radikální prosazení nové koncepce[29].

3.6 Narušování informační bezpečnosti jako světový fenomén

V této podkapitole si shrneme některé věci, které jsme krátce zmínili v předešlém textu a vysvětlíme si, kdo nejčastěji útoky snižující informační bezpečnost provádí, za jakým účelem a jaké to může mít důsledky.

Jak bylo již zmíněno, převážná většina úspěšných a závažných útoků na informační systémy je prováděna **zaměstnanci** společností. Takže na tomto stupni je také nutné přijmout určitá bezpečnostní opatření, která byla zmíněna. Největší množství útoků je dnes zautomatizována prostřednictvím zákeřných programů různých typů (viry, červi, backdoor software,

[28] To už v Evropě přestává platit, neboť byla v měsíci březnu 2004 vytvořena direktiva, která odpovědnost poskytovatelů vyžaduje

[29] S takovou koncepcí v poslední době přišel známý Bill Gates. Spočívá ve zpoplatnění emailových služeb. Přestože se může toto řešení ze začátku zdát být klasickým americkým marketingovým blábolem, jádro myšlenky při podrobnějším náhledu na věc není až tak úplně odtržené od reality. Tento nástroj by měl zamezit šíření virů a spamu na internetu. Realizace jakéhokoliv řešení je přesto otázkou několika dalších let. V Evropské Unii se zatím více uplatňuje realističtější myšlenka spočívající ve stanovení zodpovědnosti za filtrování emailových zpráv poskytovatelů emailových služeb. „Nakažené“ emailové zprávy by se neměly k uživateli vůbec dostat. To je obsahem nejnovější pracovní verze direktivy EU, věnované duševním právům a bezpečnosti v oblasti IT z března 2004.

root-kity, exploity, trojan horses, spyware, ad-ware, ...). Tyto programy vytváří nejčastěji buď **hackeři nebo hackerské skupiny**, které se snaží upozornit na bezpečnostní nedostatky dnešních systémů, nebo **crackeři**, kteří chtějí páchat trestnou činnost a poškozovat jiné skupiny lidí a obchodní společnosti. Další skupinou jsou **IT profesionálové**, kteří se obvykle také snaží upozornit na chyby a umožnit prostřednictvím softwaru detekujícím slabiny lepší administraci sítí a systémů pro zvýšení bezpečnosti. Problém s většinou softwaru sloužícího k detekci bezpečnostních slabin však je, že je časté jeho používání nejen administrátory, ale také crackery a hackerskými skupinami. Existuje zřejmě i obrovská skupina lidí, kteří provádějí útoky prostřednictvím těchto programů buď „jen tak z dlouhé chvíle" nebo si ani dost neuvědomují, co vlastně dělají.

Skupiny potenciálních útočníků se také dají neurčitě rozdělit podle odbornosti. Skupiny či jednotlivci, kteří často patří do poslední výše jmenované skupiny a kterým se často v terminologii odborníků přezdívá **„script-kiddies"**, jsou speciální typy osobností (nebo dětí), kteří často využívají administrační software, software hackerů a další specializovaný software za účelem testování bezpečnosti IS za různými účely. Do podobné skupiny patří i část crackerů. „Script-kiddies" jsou jednotlivci či skupiny, které obvykle neznají technické podrobnosti prováděných útoků, dokonce ani někdy neví, co vlastně dělají; jen využívají programů odborníků a ve výsledku tak mohou napáchat stejné škody jako pokročilý cracker.

Není vůbec výjimkou, když se mezi těmito skupinami nalézají velmi mladí lidé a děti, v ojedinělých případech je možné mezi nimi najít i 10ti-leté děti. Nejčastěji jsou skupiny „script-kiddies" tvořeny jednotlivci, v některých dalších případech je tvoří menší skupinky domlouvajíc se přes ICQ, IRC a jiné komunikační systémy. Ani si často neuvědomují, že tyto komunikační kanály jsou často monitorovány a data v nich zálohovány a mohou je tak usvědčit z páchání trestné činnosti. Fenomén dětí typu „script-kiddies" souvisí s vývojem dnešní moderní společnosti, zejména jsou tvořeny sociálně nepřizpůsobivými nebo znuděnými dětmi, nebo také rodiči zanedbávanými dětmi. Z podobných dětí se časem mohou vytvořit i pokročilí hackeři už ve velmi mladém věku. Musím zde ale uvést, že tento fenomén je globálního rozsahu ve všech vyspělých státech světa.

Zdrojem znalostí o útocích na IS jsou téměř vždy čerpány z internetu. Jen menší skupiny obvykle pokročilých hackerů si předávají informace ústně nebo jiným způsobem. Hackerem se člověk stává zřejmě tehdy, pokud téměř nikdo o jeho činnosti neví a míra jeho znalostí obvykle překračuje velmi výrazně i znalosti odborníků v oboru IT.

Důsledky útoků prováděných různými typy lidí jsou velmi odlišné. Někteří narušitelé bezpečnosti chtějí jen vyzkoušet své znalosti a nepáchat žádnou nekalou činnost, jiní mohou ničit vědomě i nevědomě a způsobovat škody různého rozsahu. V případě webových aplikací typu internetový obchod se snaží např. poškodit renomé podniku, poškozovat zákazníky, způsobo-

vat chaos v dodávkách zboží zákazníkům, paralyzovat celý systém obchodu, odhalit a zneužít osobní informace o zákaznících ke svému prospěchu nebo dokonce totálně ovládnout obchod a dělat si s ním, co chtějí. Pokročilí útočníci se snaží za sebou maskovat všechny stopy a využívat i více počítačů k útokům na cizí systémy. Škody vznikající jejich činností mohou být obrovské, je-li vzdálený systém zcela závislý na počítačové síti.

3.7 (Secure) eFuture?

Důležité pro provoz informačních systémů na internetu je pochopení toho, proč vlastně je internet dnes takovým fenoménem a proč se jím tolik zabýváme? V posledních letech dokonce využíváme internet i pro rozšíření pole komerčních aktivit v podnikové sféře, což je tématem této práce. Proč však v posledních letech „vznikl“ pojem informační bezpečnost? Proč se tolik zabýváme informačními technologiemi? Kdo řídí Internet?

Najít odpovědi na takové otázky je velmi těžké a asi těžko můžeme odpovědět několika větami. Internet se ze svého počátečního stadia vyvinul do podoby, které reprezentuje jakési rozšíření fyzického světa, tvoří novou oblast, kde se střetává obrovské množství informací, které se do „fyzického světa nevejdou“. Usnadňuje práci, také ji jiným bere, zefektivňuje mezinárodní obchod, rozšiřuje možnosti výměny informací, ... Nikdo ho neřídí ... prostě jen tak existuje.

Internet v dnešních časech je místem, kde si každý může najít svůj „virtuální svět“ a podílet se na jeho případném vývoji. Internet se může stát nástrojem pro vyjadřování svých názorů. Může ale také být zdrojem pro nekalou „informační válku“ jednotlivých subjektů, neboť informace mají dnes stále větší a větší důležitost a jejich distribuce ke stále větší části obyvatelstva získávající informace na internetu dokáže touto masou snáze manipulovat a dosáhnout i efektu „vymývání mozků“ za určitým účelem (moc, peníze). Tato válka se neomezuje pouze na virtuální svět internetu, je stále ještě více přítomná v běžném životě (masmédia, marketing, reklama), ale je trochu méně viditelná, popř. více tolerovaná nebo si jí „ovlivňovaní“ ani neuvědomují. Na internetu je plno skupin lidí, kteří se snaží upozornit na důsledky této „války“ v reálném světě i na internetu a dokonce propagují své myšlenky způsoby, které mají až „anarchistický“ charakter (hactivism[30]). Tyto zájmové skupiny jsou pak také zařazovány do skupin vedoucích informační válku. I když se to zdá být pro někoho trochu „sci-fi“, dnes již skutečná kybernetická válka existuje a odehrává se především na politickém poli. Je jen otázkou času, kdy se projeví i více extrémními způsoby.

[30] Novodobé hnutí aktivistů využívajících k propagaci a vyjadřování svých názorů na svět komunikační a hackerské dovednosti

Internet v dnešním stádiu vývoje je pouze rozšířením informačního pole celosvětové společnosti a jakýmsi zvýšením informační entropie ve světě. Tak jak se bude internet stále demokratizovat nebo naopak regulovat mocenskými skupinami a vládami, bude docházet buď k většímu přibližování se ideálu světové demokracie nebo naopak bude rychle splývat s dnešní realitou omezeného fyzického světa.

Osobně si myslím, že nikdy nevyhraje ani jedna strana. A pokud bych měl zde vyjádřit svůj názor na vývoj Internetu v příštích desítkách let, tak si myslím, že za 30-50 let si už těžko bude někdo pamatovat, že existoval nějaký „svět před Internetem“ a velká část průměrným člověkem vnímané reality se bude odehrávat mimo fyzický svět. Internet však bude mít jinou podobu, zřejmě ještě méně „fyzickou“ než dnes.

Kapitola 4

Obecná doporučení

V této poslední a velmi krátké kapitole se pokusím taxativně vyjmenovat všechna nejdůležitější a obecná doporučení pro provoz aplikace internetového obchodu. Vzhledem k rozsahu celé této práce není vhodné vyjmenovávat všechny aspekty, neboť by to bylo téměř určitě na úkor přehlednosti.

1. **Stanovení cílů podniku v souvislosti s provozem internetového obchodu**

   Není vhodné provozovat internetový obchod za každou cenu, pokud podniku nepřinese žádné výrazné výhody oproti stávajícímu stavu. Zejména v případě malých podniků je provoz internetového obchodu méně významnou investicí a malým zdrojem zisků.

2. **Zvolení metody implementace obchodu**

   Stejně jako předchozí bod je toto rozhodování úkolem manažera a do značné míry může znamenat strategické rozhodnutí. Finanční náročnost a konečný výsledek zvolené metody jsou hlavní faktory předurčující úspěšnost internetového obchodu.

   V případě malých podniků je lepší volit finančně nenáročná a méně kvalitní řešení. Podniky s většími ambicemi by měly vždy spoléhat na profesionální práci zvoleného implementátora.

3. **Zajištění funkce nevirtuální části obchodu**

   Je nutné zajistit takovou organizaci práce a vyřizování obchodních záležitostí, aby plnila předpokládané požadavky a splňovala ty, které jsou uváděny na webových stránkách obchodu.

4. **Respektování platných zákonů a jiných předpisů při provozu obchodu**

I přes poněkud jinou formu obchodování se musí dodržovat zákonem stanovené podmínky pro provoz běžného obchodu s určitými specifiky vyplývajícími z povahy uzavírání smluv na dálku.

Zejména se to týká formálních náležitostí a povinností souvisejících s ochranou spotřebitele, ochranou před nekalou soutěží, narušováním hospodářské soutěže, ... Základními právními předpisy stále zůstávají obchodní, občanský zákoník a „autorský zákon“.

5. **Přehlednost informační architektury a vhodný design**

   Internetový obchod by měl být zejména přehledný pro návštěvníky webové prezentace obchodu. Měl by umožňovat zákazníkům snadnou orientaci, zejména v katalogu výrobků a zjednodušovat proces objednávání. Také by měl umožnit účinné vyhledávání jednotlivých informací.

   Grafické provedení obchodu by mělo být střízlivé a příjemné, co nejvíce uzpůsobené primární funkci obchodu, tedy nákupu. Také by měl být upraven tak, aby umožňoval prohlížení co největší skupině uživatelů. Nemělo by docházet k diskriminaci na základě schopností softwaru a hardwaru na straně klienta.

6. **Dodržování mezinárodních standardů či norem**

   Webová prezentace obchodu by měla být zpracována tak, aby nebyla v rozporu s ustanoveními přijímaných mezinárodních (internetových) standardů nebo dokonce norem, je-li vyžadována jejich aplikace pro splnění certifikačních nároků.

   Případná nestandardní rozšíření funkčnosti by měla být pouze volitelnou součástí aplikace.

7. **Respektování bezpečnosti klientů**

   Aplikace internetového obchodu by měla být vždy konstruována tak, aby nebylo možné ji někým zneužít k útokům na zákazníky či třetí osoby nebo systémy.

8. **Dosažení co nejvhodnější úrovně informační bezpečnosti**

   Internetový obchod a veškeré funkční prvky nutné pro jeho provoz je nutné udržovat na takové úrovni bezpečnosti, aby nezakládaly pochybnosti o jeho kvalitě jak ze stran zákazníků, tak ze stran třetích osob.

Při dodržování a respektování v této práci zmíněných aspektů a pravidel internetového obchodování v podnikové sféře by měl být používaný internetový obchod vhodným rozšířením či hlavní náplní činnosti podniku.

Závěr

Před začátkem psaní této práce jsem si nebyl chvíli jist, zda není zvolené téma příliš specializované a zda je možné vše potřebné dostatečně dobře popsat a vysvětlit, a to hlavně z důvodu, že k dané problematice neexistuje do dnešní doby žádný kvalitní zdroj české literatury a nebylo tedy možné z něčeho vycházet. Poté, co jsem se přesvědčil, že vhodná literatura skutečně na tomto poli chybí, popř. je redukována pouze na technicky náročnější literaturu, jsem došel k závěru, že je to unikátní příležitost se o její sepsání pokusit a přitom využít části svých dosavadních znalostí a dovedností a také popřemýšlet, zda by se z jejího obsahu později nedalo vycházet při sepsání odborné knihy na dané téma. Tato práce, přestože jsem se snažil, může být sice dobrým zdrojem pro pochopení základní problematiky, pro hlubší pochopení a lepší popis všech aspektů internetového obchodování je však nutné se zabývat daleko širším spektrem znalostí a informací odborného charakteru, které by tuto práci mohly případně doplnit.

Není zřejmě možné problematiku internetového obchodování v podnicích popsat nějakým vyčerpávajícím způsobem v tak malém formátu, který představuje diplomová práce, a o to méně je to pravděpodobné, jestliže zatím nemám v této oblasti dlouhodobé praktické zkušenosti, o které bych se mohl případně opřít. Tedy pokud lze vůbec o dlouhodobé praxi mluvit i u profesionálních tvůrců dnešních virtuálních obchodů. Má nedostatečná zkušenost je asi také i důvodem, proč pro člověka zabývajícího se profesionálně tvorbou internetových obchodů a jiných webových aplikací v obchodě může být v této práci přínosem spíše jen teoretická část věnovaná víceméně legislativním a ostatním podmínkám pro provoz internetového obchodu a v některých případech i oddíl věnovaný designu jakožto strategického prvku každé jednotlivé prezentace na internetu.

Kapitola věnovaná bezpečnosti – která obsahuje z dost podstatné části mé názory – může být velmi inspirativní i pro tyto tvůrce, a především pak jistě překvapí každého běžného čtenáře, ačkoliv nebylo možné zahrnout do práce více příkladů kompromitace internetových obchodů a nastínit tak podrobnosti nutné pro pochopení dnešního stavu informační bezpečnosti z nejen globálního pohledu.

Zvláště je v případě zájmu vhodné pečlivě prostudovat i přiložený zdrojový kód mé implementace internetového obchodu, která si neklade být univerzálním ani dokončeným řeše-

ním, může však poskytnout prostor pro inspiraci. Tento kód je použitelný v rámci licence GNU/GPL 2 a je možné ho po drobných korekturách ihned aplikovat.

Účelem této diplomové práce je pro nezasvěceného člověka poskytnout téměř komplexní pohled na aktuální a především praktickou část komercionalizace té části internetu, která se zabývá rozšířením podnikatelských aktivit směrem k internetovým uživatelům. Lze totiž v budoucnosti jistě čekat daleko větší odklon od využívání služeb dnešních „kamenných“ obchodů a daná problematika se stane ještě více diskutovanou než dnes, zvláště pak v souvislosti s hledáním nových marketingových odbytišť výrobků i služeb a se stále více viditelnými problémy s bezpečností informačních systémů.

Hlavním motivem k sepsání práce věnované právě tématu internetového obchodování byl můj již téměř čtyřletý zájem o nejnovější informační technologie doprovázený zájmem o jejich možnou aplikaci v ekonomickém prostředí běžného obchodu. V neposlední řadě jsem si také vyzkoušel, jak náročná je technická implementace virtuálního obchodu a uvědomil si, že profesionální návrh internetových řešení vyžaduje skutečně nadmíru velké znalosti internetových technologií a zejména komplexní přístup, který je dnes tak vyžadován.

Po přečtení práce a zejména jejích některých částí si podle mého názoru obecný čtenář uvědomí, co internetové obchodování v moderní společnosti znamená a jistě dojde k závěru, že nejde o jakýsi módní výstřelek posledních pár let, ale o skutečnou metodu rozvíjení komerčních aktivit.

Seznam použité literatury

[1] [Ekomerce] *E-komerce.cz – internetový server věnující se elektronickému obchodu nejen v ČR*
`http://www.e-komerce.cz`

[2] [Skochova01] *Škochová, E.:* **Návrh legislativního postupu pro podporu elektronického obchodu v ČR v návaznosti na Směrnici 2000/31/EC Evropského parlamentu a Rady z 8.6.2000 o elektronickém obchodu**
2001

[3] [Mindzak02] *Mindžák, R.:* **Dokonalý web design**
Computer Press, 2002

[4] [Peterka03] *Peterka, J.:* **Státní informační a (tele)komunikační politika I. až III.**
Internetový server Lupa nebo e-archiv Jiřího Peterky, 13.10.2003 – 16.10.2003
`http://www.lupa.cz` nebo `http://www.earchiv.cz`

[5] [Europa] *Portál Evropské unie*
`http://europa.eu.int`

[6] [Bilakniha03] **Bílá kniha o elektronickém obchodu**
Ministerstvo informatiky ČR, 19. 5. 2003
`http://www.micr.cz`

[7] [SIP02] **Státní informační politika**
Ministerstvo informatiky ČR, 18. 12. 2002
`http://www.micr.cz`

[8] [AkplanSIP02] **Akční plán realizace státní informační politiky**
Ministerstvo informatiky ČR, 18. 12. 2002
`http://www.micr.cz/dokumenty/strategicke.htm`

[9] [Zhang02] *Zhang, Y.:***Building an E-Commerce Site**
Developer Shed, Inc., 2002
`http://www.devshed.com/Server_Side/PHP/Commerce/Commerce1/`

[10] [Vrabec02] *Vrabec, V.:* ***e*Europe 2005 – Informační společnost pro všechny**
Tiscali.cz, 27. 6. 2002
`http://www.tiscali.cz`

[11] [Root] *Root.cz – internetový portál o počítačích a Linuxu*
`http://www.root.cz`

[12] [Zaksluzbyinfspol03] **Návrh zákona o službách informační společnosti a o změně zákona č.40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů (zákon o službách informační společnosti)**
Ministerstvo informatiky ČR, 10. 9. 2003
`http://www.micr.cz`

[13] [Zakelektrpodpis03] **Zákon, kterým se mění zákona č.227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů (zákon o službách informační společnosti)**
Ministerstvo informatiky ČR, 19. 8. 2003
`http://www.micr.cz`

[14] [Celustka99] *Čelustka, E.:* **Pravidla pro budování internetových obchodů**
E-komerce.cz, 21. 7. 1999
`http://www.e-komerce.cz`

[15] [eEurope2005] ***e*Europe 2005: An information society for all**
Commission of the European Communities, 29. 5. 2002
`http://europa.eu.int`

[16] [Petr96] *Petr J. a kolektiv:* **Elektronický obchod a EDI**
Unis publishing, 1996

[17] [Psika02] *Psika, T.:* **Elektronické obchodování a predikce jeho rozvoje v integrované Evropě**
Bakalářská práce 2001/2002 FSE Univerzity J. E. Purkyně v Ústí n. Labem, 2002

[18] [Hradek01] *Hrádek, J.:* **Směrnice ES o elektronickém obchodu**
Itpravo.cz, 21. 11. 2001
`http://www.itpravo.cz`

[19] [Vrabec01] *Vrabec, V.:* ***e*Europe+ 2003**
Tiscali.cz, 29. 6. 2001
`http://www.tiscali.cz`

[20] [Prodi99] *Prodi, R.:* **eEurope? Information Society for All**
Commission of the European Communities, 1999
`http://www.europa.eu.int`

[21] [Vrabec01/2] *Vrabec, V.:* **My a eEurope 2005**
Tiscali.cz, 23. 2. 2003
`http://www.tiscali.cz`

[22] [APEK] *Asociace pro elektronickou komerci*
`http://www.apek.cz`

[23] [Hrazdila03] *Hrazdila, Z.:* **Deset osvědčených rad, jak přijít o e-zákazníka**
Interval.cz, 14. 10. 2003
`http://www.interval.cz`

[24] [Prusvic99] *Prušvic, L.:* **Internetové obchody, certifikace, APEK**
E-komerce.cz, 15. 12. 1999
`http://www.e-komerce.cz`

[25] [Froulik00] *Froulík, R.:* **Elektronický obchod**
Jihočeská Univerzita, 2000
`http://home.zf.jcu.cz`

[26] [Sarmanova02] *Šarmanová, J.:* **Metody dolování znalostí z dat**
Katedra informatiky FEI VŠB-TU Ostrava,2002
`http://www.vsb.cz`

[27] [AFOI] *Asociace firem pro ochranu informací*
`http://www.afoi.cz`

[28] [Pulpan02] *Půlpán, J.:* **Dolování dat aneb hledání skrytých souvislostí**
SAS Institute, 2002

[29] [CIS03] **Certifikace informačních systémů**
srpen 2003

[30] [Root00] *Root.cz:* **Groupwarové systémy**
Root.cz, 2000
`http://www.root.cz`

[31] [Kralova03] *Králová:* **Informační bezpečnost v integrované Evropě**
2003

[32] [RAC] *Risk Analysis Consultants:* **ISO 17799: Information Security Management**
RAC, 2003

[33] [Vystavelova02] *Vystavělová, H.:* **Standardizace bezpečnosti IT**
Fakulta informatiky MU Brno, prosinec 2002
`http://www.fi.muni.cz`

[34] [Sustr03] *Šustr, J.:* **Informační bezpečnost jako součást systému řízení jakosti podle normy ISO 9000:2000**

[35] [HBTlinux03] *Hatch, B., Lee, J., Kurtz, G.:* **Hacking bez tajemství: Linux**
Computer Press, 2003

[36] [Hlavenka04] *Hlavenka, J.:* **Microsoft bude zřejmě muset vyrobit „evropská“ Windows**
Zive.cz, 9. 3. 2004
`http://www.zive.cz`

[37] [HBTwebaplikace03] *Scambray, J., Schema, J.:* **Hacking bez tajemství: Webové aplikace**
Computer Press, 2003

[38] [HBTwin_net_unix03] *Scambray, J., McClure, S., Kurtz, G.:* **Hacking bez tajemství: Windows, NetWare, UNIX/Linux**
Computer Press, 2003

[39] [SecNet] *SecurityNet.cz – server věnovaný bezpečnostní problematice počítačů*
Securitynet.cz `http://www.securitynet.cz`

[40] [SecFocus] *Securityfocus.com – server o bezpečnosti počítačů*
`http://www.securityfocus.com`

[41] [Nexx02] *Nexx:* **Windows XP dovolují na dálku smazat obsah adresáře!**
15. 9. 2002
`http://www.securitynet.cz`

[42] [Holcik04]*Holčík, T.:* **Microsoft zakáže používání jména a hesla v adrese webových stránek**
Živě.cz, 29. 1. 2004
`http://www.zive.cz`

Seznam příloh

1. Funkční implementace internetového obchodu ve skriptovacím jazyce PHP
2. Struktura databázové části implementace obchodu
3. Ostatní soubory nutné pro funkčnost implementace obchodu

Příloha č. 1

Funkční implementace internetového obchodu ve skriptovacím jazyce PHP

```php
<?
/* >>> index.php <<< */

//*****************

// Tento projekt byl vytvořen pro mou diplomovou práci na FSE UJEP v roce 2003/2004
// Jednotlivé části projektu mohou být šířeny a upravovány pod licencí GNU/GPL
// Není zaručeno komerční využití projektu a nejsou poskytovány žádné záruky.

// Až do verze 0.8 se stav implementace považuje za "unstable" a není doporučeno jeho
// reálné a dlouhodobé nasazení, pouze doporučeno pro testovací účely a popřípadě
// pro odstartování vývoje složitější implementace či jako inspirace pro tvorbu jiné
// práce na dané téma

// Funkční prezentace obchodu, zdrojové kódy a grafické soubory jsou umístněny
// na webu, na adrese http://www.tstobchod_xin.wz.cz

// - prezentace:
//      http://www.tstobchod_xin.wz.cz/prezentace/index.php
// - zdrojové kódy ve formě textových souborů:
//      http://www.tstobchod_xin.wz.cz/zdrojove_kody/seznam.php
// - grafické soubory:
//      http://www.tstobchod_xin.wz.cz/grafika/grafika.php

// !!!! Pokud není stránka v provozu, tak byla stránka zřejmě provozovatelem
// !!!! webserveru Webzdarma z důvodu malé návštěvnosti smazána

// Popis: Odlehčená verze plně funkčního internetového obchodu

// Copyright: Tomáš Psika,2003-2004

// Email:tomas_psika@cbox.cz

//*****************

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//***************************************
//    Hlavní startovací skript
//***************************************

$verze="0.6 alpha";     // aktuální verze implementace

header("Location: obchod.php");

?>
```



```php
<?
/* >>> obchod.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//************************************************
//   Hlavní startovací skript internetového obchodu
//************************************************

// benchmarking
$_start=getmicrotime();

// safe mode
define("USF","UNSAFE_MODE");        // konstanta pro účely bezpečnostního profilování aplikace
                    //(u release verze nedefinovat)

// globální proměnné
$debug=TRUE;                    // pro ladění, jinak nastavit na FALSE
$firma="Xinerama, s.r.o";           // název firmy
$domenova_adresa="http://localhost";        // základ URL
$uz_online=FALSE;               // informace o tom, zda je uživatel znám
$uz_jmeno=NULL;                 // jméno aktuálního uživatele
$uz_pole=array();               // pole dat o uživateli (pro účely serializace dat)
$time=time();                   // aktuální čas
$zobrazit_stav=TRUE;                // ukázat stav přihlášení v pravé části okna
                        // (někdy se vypíná, pokud se člověk aktuálně přihlašuje
                        // či odhlašuje)

session_start();

ignore_user_abort(TRUE);
error_reporting(E_ALL);

// některé základní součásti
require("lib.php");         // knihovna funkcí
require("db.php");          // nastavení databáze
require("podnikove_udaje.php");     // podnikové údaje
require("pausaly.php");         // údaje o poštovném, manipulačním poplatku apod.
require("uzivatel.php");        // třída obsluhující jednotlivé uživatele
require("stranka.php");         // základní třída pro generování stránek
require("vyrobek.php");         // třída pro obsluhu zobrazování jednotlivých výrobků
require("chyba.php");           // handler chyb
require("dph.php");         // definuje jednotlivé sazby DPH

pripoj_se_k_databazi();

$dnes=posledni_pristup();       // proměnná inicializovaná na FALSE pouze při změně data
                    // (pro účely statistik)
zvys_pocitadla();           // počítadla přístupů
if (!je_server_ok()) {
    exit;
}

$stranka=new stranka(empty($_GET['m'])?NULL:$_GET['m']);
$uzivatel=new uzivatel();
if ($uzivatel) {
    $GLOBALS['uz_jmeno']=$uzivatel->uzivatel;
    $GLOBALS['uz_pole']=$uzivatel->g_jpamt_email();
} else {
    unset($uzivatel);
}

if (!$stranka->stranka_neexistuje) {
    $stranka->vystup();
} else {
    echo "Tato stránka neexistuje.<br>";
```

```
72      return;
73  }
74
75  odpoj_se_od_databaze();
76
77  $_end=getmicrotime();
78
79  function getmicrotime()    {
80      list($usec, $sec) = explode(" ",microtime());
81      return ((float)$usec + (float)$sec);
82  }
83
84  if ($debug) {
85  ?>
86  <p align="center">Skript běžel <? echo $_end-$_start; ?> sec.</p>
87  <?
88  }
89  ?>
90
91
```



```
1  <?
2  /* >>> lib.php <<< */
3  //************************************************************
4  //*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
5  //***********  implementace internetového obchodu  ************
6  //**************** @ Tomáš Psika, 2003-2004 *******************
7  //*******************  (licence GNU/GPL) **********************
8  //************************************************************
9
10 //*************************************
11 //   Některé doplňkové funkce
12 //*************************************
13
14
15 function posledni_pristup() {
16     $res=mysql_query("SELECT kolik FROM data WHERE data='posledni_pristup'");
17     if (!$res) { mysql_chyba(NULL,"Došlo k chybě při zjišťování posledního přístupu na stránky.
18         Zřejmě je problém s tabulkou 'data' nebo došlo k blíže nespecifikované chybě."); }
19     $res2=mysql_query("UPDATE data SET kolik=".$GLOBALS['time']." WHERE data='posledni_pristup'");
20     if (!$res2) { mysql_chyba(NULL,"Neaktualizoval se čas posledního přístupu na web."); }
21     if (!mysql_affected_rows()) { mysql_chyba(NULL,"Zřejmě chybí řádek 'posledni_pristup' v tabulce
22         'data'"); return FALSE;}
23     if (mysql_num_rows($res)) {
24         list($posledni_pristup)=mysql_fetch_row($res);
25         return (date("dmY",$GLOBALS['time'])!=date("dmY",$posledni_pristup))?0:1;
26     }
27     return 0;   // implicitní odezva
28 }
29
30 function zvys_pocitadla() {
31     $res=mysql_query("UPDATE pocitadla SET kolik=kolik+1 WHERE co='pristupy'");
32     if (!$res | !mysql_affected_rows()) { mysql_chyba(NULL,"Nezvýšilo se počítadlo všech
33         přístupů"); }
34     if (!$GLOBALS['dnes']) {
35         $res2=mysql_query("UPDATE pocitadla SET kolik=0 WHERE co='pristupy_dnes'");
36         if (!$res2) { mysql_chyba(NULL,"Nevynulovalo se počítadlo dnešních přístupů"); }
37     } else {
38         $res2=mysql_query("UPDATE pocitadla SET kolik=kolik+1 WHERE co='pristupy_dnes'");
39         if (!$res2 | !mysql_affected_rows()) { mysql_chyba(NULL,"Nezvýšilo se počítadlo
40             dnešních přístupů"); }
41     }
42 }
43
44 function je_server_ok() {
45     $res=mysql_query("SELECT kolik FROM data WHERE data='server_on'");
46     if (!$res) { mysql_query(NULL,"Nepodařilo se zjistit, zda není server pozastaven."); }
47     list($res_)=mysql_fetch_row($res);
48     if (!$res_) {
49         echo "<html><head><title>Server pozastaven.</title></head><body bgcolor=\"white\"
50             text=\"black\" style=\"margin-top:50px\"><p align=\"center\"><b>Obchod
51             je přechodně uzavřen. Omlouváme se a doufáme, že nás v nejbližší době znovu
52             navštívíte.</b></p></body></html>";
53         return FALSE;
54     }
55     return TRUE;   // OK!
56 }
57
58 ?>
59
```

```php
<?
/* >>> chyba.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//************************************
//      Řízení chybového výstupu
//************************************

#error_reporting(E_ALL);
set_error_handler('chyba');

function chyba($cislo_chyby,$hlaska_chyby,$errfile,$errline) {
    #if ($cislo_chyby==E_WARNING) {
    #   return;                 // ignorujeme pouhá upozornění
    #} else {
        // standardní hláška uživateli
        echo "Došlo k chybě, stránka nemůže být zobrazena.<br><br>\n";
        if ($GLOBALS['debug']) {
            // nadstandardní hláška
            echo "<b>V souboru '".$errfile."' na řádku číslo ".$errline." došlo k chybě, která
            vyprodukovala tuto hlášku:<br>".$hlaska_chyby.".<br><br>";
        }
        exit;   // ukončíme skript
    #}
}

function mysql_chyba($text=NULL,$text_debug=NULL) {
    // chyba v MySQL databázi, taky vypíšeme menší hlášku a ukončíme skript
    if ($GLOBALS['debug']) {
        echo "Chyba v databázi. Ukončujeme běh skriptu.<br>Poslední hláška chyby:'".
            mysql_error()."'.<br><br>".$text_debug."<br><br>\n";
    }
    echo "Došlo k chybě.<br><br>\n";    // standardní hláška (minimalistická)
    echo $text;
    exit;
}

?>
```



```php
<?
/* >>> stranka.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//************************************
//Definice třídy reprezentující stránku
//************************************

class stranka {
    var $id;
    var $parametr;
    var $titulek;
    var $skript;
    var $pocitadlo;
    var $stranka_neexistuje;   // pomocná vlastnost

    //function stranka($parametr=NULL); // defaultní konstruktor
    //function vystup();            // vlastní výstup do HTML
    //function vloz_odkaz($text=NULL);  // vloží odkaz na vlastní stránku
    //function napis_titulek();     // vloží tag <TITLE>..</TITLE> do stránky
    //function zvys_pocitadlo();        // přičtení primitivního počítadla návštěv stránek
    //function zahlavi();           // tisk záhlaví
    //function zapati();            // tisk zápatí
    //function posli_no_cache_HTTP_hlavicku();  // HTTP hlavičky typické pro dynamické weby
    //function nadpis();            // hlavní nadpis stránky (stejné uvození jako
                        // v titulku stránky)

    function stranka($parametr=NULL) {

        $this->stranka_neexistuje=FALSE;

        if (empty($parametr))
            $parametr="uvodni_str"; // defaultní stránka, když není zadán parametr

        $res=mysql_query("SELECT id,titulek,skript,pocitadlo FROM stranky WHERE param='".
            $parametr."'");
        if (!$res) { mysql_chyba(NULL,"Stránka zřejmě neexistuje nebo došlo k jiné chybě."); }
        if (!mysql_num_rows($res)) {
            $this->stranka_neexistuje=TRUE;
            return FALSE;  // stránka neexistuje
        }
        list($this->id,$this->titulek,$this->skript,$this->pocitadlo)=mysql_fetch_row($res);
        $this->zvys_pocitadlo();

        // zamezení zobrazování stavu přihlášení pro určité stránky (kvůli struktuře aplikace)
        $dalsi_parametr=(empty($_GET['sub']))?NULL:$_GET['sub'];
        if ($parametr=="prihlaseni" || $parametr=="odhlaseni" || (($parametr=="registrace") &&
            $dalsi_parametr=="potvrzeni_upravy_registrace") || (($parametr=="registrace") &&
            $dalsi_parametr=="obnova"))
                $GLOBALS['zobrazit_stav']=FALSE;
    }

    function vystup() {
        $this->posli_no_cache_HTTP_hlavicku();
        if (strpos($this->skript,"_self")===false) {
            $this->zahlavi();
            include("_in_".$this->skript);      // odkaz na hlavní skript dané stránky
            $this->zapati();
        } else {
            include("_self_".$this->skript);        // stránka má svůj vlastní výstup
        }
    }

    function vloz_odkaz($text=NULL) {
        echo "<A HREF=\"".$GLOBALS['PHP_SELF']."m=".$this->parametr."\"></A>";
```

```
    }

    function napis_titulek() {
        echo "<title>",$this->titulek,"</title>\n";
    }

    function zvys_pocitadlo() {
        $res=mysql_query("UPDATE stranky SET pocitadlo=pocitadlo+1 WHERE id=".$this->id);
        if (!$res) { mysql_chyba(NULL,"Nezvýšilo se počítadlo přístupu na stránku."); }
    }

    function zahlavi() {
        include("_in_standardni_zahlavi.php");
    }

    function zapati() {
        include("_in_standardni_zapati.php");
    }

    function posli_no_cache_HTTP_hlavicku() {
        // nedůležité, při chybě v běhu skriptu by PHP hlásilo chybu 'headers already sent'
        if (headers_sent()) return;
        header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
        header("Pragma: no-cache");      // pro HTTP/1.0 (staré proxyny a prohlížeče)
    // HTTP/1.1
    header("Cache-Control: max-age=0, s-maxage=0, no-cache, must-revalidate, no-store, no-transform");
        header("Cache-Control: post-check=0, pre-check=0", false);
    }

    function nadpis() {
        echo "<h3>".$this->titulek."</h3>\n";
    }
}

?>
```



```
<?

/* >>> vyrobek.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//***********  implementace internetového obchodu  ************
//**************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ***********************
//************************************************************

//************************************
//Definice třídy reprezentující výrobek
//************************************

class vyrobek {
    var $id;        // identifikátor v databázi (v tabulce primární klíč)
    var $nazev;
    var $gid;       // identifikátor skupiny výrobků (tabulka skupina)
    var $gid_nazev;     // název skupiny výrobků
    var $cena;
    var $dph;       // dph (0..osvobozeno,1..nižší sazba,2..základní sazba)
    var $popis;
    var $obrazek;       // popisný obrázek
    var $sklad;     // je výrobek na skladě (možná se nebude používat)
    var $rel;       // je možné výrobek zajistit

    //function vyrobek($id);        // jednoduchý konstruktor provádějící inicializaci
    //function cena_bez_dph();      // vrátí cenu bez DPH
    //function dph();           // vrátí daň z přidané hodnoty
    //function celkova_cena();      // vrátí cenu i s DPH
    //function vypis_polozku_tabulky(); // HTML výstup

    function vyrobek($id)
    {
        $_id_=-1;

        $res=mysql_query("SELECT * FROM vyrobky WHERE id=".$id);
        if (!$res) { mysql_chyba(NULL,"Výrobek zřejmě neexistuje. Špatný identifikátor nebo
            jiná nespecifikovaná chyba."); }
        if (!mysql_num_rows($res)) {
            // výrobek v databázi není, modifikujeme id (můžeme testovat při volání)
            $this->id=$_id_;
            return;
        }
        list($this->id,$this->nazev,$this->gid,$this->cena,$this->dph,$this->popis,$this->obrazek,
            $this->sklad,$this->rel)=mysql_fetch_row($res);

        $this->popis=nl2br($this->popis);

        $res=mysql_query("SELECT * FROM skupiny WHERE gid=".$this->gid);
        if (!$res) { mysql_chyba(NULL,"Skupina výrobků neexistuje. Špatný identifikátor."); exit; }
        list($tmgid,$this->gid_nazev,$tmngig)=mysql_fetch_row($res);

        // zjistíme, zda existuje obrázek, pokud ne, nahradíme ho obrázkem skupiny
        if (file_exists("grafika/".$this->obrazek))
            $this->obrazek="grafika/".$this->obrazek;
        else
            $this->obrazek="grafika/".strtolower($this->gid_nazev)."_obrazek_skupiny.jpg";
    }

    function cena_bez_dph() {
            return $this->cena;
    }

    function dph() {
        if (!$this->dph) {
            return $this->cena;
        } elseif ($this->dph==1) {
            return round($this->cena*$GLOBALS['snizena_sazba_dph'],2);
        } elseif ($this->dph==2) {
```

```
72              return round($this->cena*$GLOBALS['zakladni_sazba_dph'],2);
73          } else {
74              chyba();
75          }
76      }
77
78      function celkova_cena() {
79          return ($this->cena+$this->dph());
80      }
81
82      function vypis_polozku_tabulky() { // layout do tabulky katalogu (jeden řádek tabulky)
83  ?>
84      <tr>
85          <td width="50" height="50" align="center" valign="center"><?
86              // obrázek výrobku (pokud není, pak standardní obrázek skupiny) ?>
87              <a href="<? echo $_SERVER['PHP_SELF']; ?>?m=katalog&sub=obrazek&u=<?
88                  echo $this->id; ?>" target="_blank"><img src="<?
89                  echo $this->obrazek; ?>" width="50" height="50" alt="Obrázek výrobku"></a>
90          </td>
91          <td align="center">
92              <? echo $this->nazev,"\n"; ?>
93          </td>
94          <td align="center">
95              <? echo $this->popis,"\n"; ?>
96          </td>
97          <td align="center">
98              <? echo number_format($this->cena,2)," Kč\n"; ?>
99          </td>
100         <td align="center">
101             <? echo number_format($this->celkova_cena(),2)," Kč\n"; ?>
102         </td>
103         <td align="center">
104             <a href="<? echo $_SERVER['PHP_SELF']; ?>?m=nak_kosik&sub=pridat&v=<?
105                 echo $this->id; ?>&p=1"><img src="grafika/pridat.png" alt="Do košíku" width="25"
    height="25" border="0"></a>
106         </td>
107     </tr>
108 <?
109     }
110
111 }
112
113 ?>
114
```



```
1  <?
2
3  /* >>> uzivatel.php <<< */
4
5  //************************************************************
6  //*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
7  //***********  implementace internetového obchodu  ************
8  //**************** @ Tomáš Psika, 2003-2004 ******************
9  //*****************  (licence GNU/GPL) ***********************
10 //************************************************************
11
12 //************************************
13 //      Třída obsluhující uživatele
14 //************************************
15
16 class uzivatel {
17
18     var $sid;           // název dynamické session
19     var $uzivatel;          // přihlašovací jméno
20     var $heslo;         // heslo (implicitně se neinicializuje v konstruktoru (NIvK)
21     var $posledni_pristup;      // poslední kliknutí přihlášeného uživatele
22     var $predesly_pristup;
23     var $pocitadlo;         // NIvK, počítadlo přihlášení
24     var $email;
25     var $adresa;            // NIvK
26     var $telefon;           // NIvK
27     var $datum_reg;         // NIvK (datum registrace)
28     var $kod;           // pomocná stavová proměnná
29
30     //function uzivatel();              // inicializační konstruktor
31     //function g_email();               // vrátí emailovou adresu
32     //function zvys_pocitadlo();            // zvyšuje počítadlo přihlášení k obchodu
33     //function registrace();            // nová registrace
34     //function prihlasit($u_jmeno);         // přihlášení uživatele
35     //function odhlasit();              // odhlášení
36     //function oprava_reg($pole,$puvodni_data); // oprava registračních údajů
37     //function pristupy();              // logování posledních přístupů uživatele
38         //function g_jpa_email();           // vrátí jméno,příjmení,adresu a email
39                             // (pro účely serializace dat objednávek)
40
41     function uzivatel() {
42         $this->sid=session_id();
43         $this->stav=FALSE;
44         $orx=FALSE;$res_x=FALSE;
45         // vyjímečný případ (obnova registračních údajů)
46         if ((!empty($_GET['sub']))&&(!empty($_GET['uz']))) {
47             // SFBUG ** (nepoužito ereg())
48             $k=(htmlspecialchars($_GET['uz'])==$_GET['uz'])?TRUE:FALSE;
49             $GLOBALS['obnova_reg']=(($_GET['sub']=="obnova")&&$k)?TRUE:FALSE;
50             if ($GLOBALS['obnova_reg']) {
51                 $res_x=mysql_query("SELECT uzivatel,email,predesly_pristup,kod FROM
52                     uzivatele WHERE sid='docasne_irelevantni' AND kod='z' AND
53                     uzivatel='".$k."'");    // SFBUG *?* (co když bude 'uzivatel...'
54                                 //na začátku SQL-dotazu)
55                 if (!$res_x) { mysql_chyba(NULL,"Nepodařilo se vybrat z databáze údaje o
56                     uživateli, který se snaží obnovit registrační údaje, když zapomněl
57                     heslo."); }
58                 if (mysql_num_rows($res_x))
59                     $orx=TRUE;
60             }
61         }
62         $res=mysql_query("SELECT uzivatel,email,predesly_pristup,
63             kod FROM uzivatele WHERE sid='".$this->sid."' AND kod='p'");
64         if (!$res) { mysql_chyba(NULL,"Nepodařilo se zjistit uživatele."); }
65         if ((!mysql_num_rows($res))&&(!$orx)) {
66             // nepřihlášený uživatel, končíme v této třídě
67             return FALSE;
68         }
69         if (!$orx) {
70             list($this->uzivatel,$this->email,$this->predesly_pristup,
71             $this->kod)=mysql_fetch_row($res);
```

```php
        } else {
            list($this->uzivatel,$this->email,$this->predesly_pristup,
            $this->kod)=mysql_fetch_row($res_x);
            // jde o obnovu reg.údajů, uměle později nastavíme v '_in_registrace.php',
            // že je uživatel přihlášený
        }
        $GLOBALS['uz_online']=TRUE;
        $this->zvys_pocitadlo();
        $this->pristupy();
        return TRUE;
    }

    function pristupy() {
        $res=mysql_query("UPDATE uzivatele SET predesly_pristup=".$GLOBALS['time']."
            WHERE sid='".$this->sid."'");
        if (!$res) { mysql_chyba(NULL,"Nepodařilo se přepsat předešlý přístup uživatele"); }
    }

    function g_email() {
        return $this->email;
    }

    function g_jpamt_email() {
        $res=mysql_query("SELECT jmeno,prijmeni,adresa,mesto,telefon FROM uzivatele WHERE
            sid='".$this->sid."' AND kod='p'");
        if (!$res) {mysql_chyba(NULL,"Nepodařilo se zjistit registrační údaje uživatele."); exit;}
        if (!mysql_num_rows($res))
            return array("jmeno"=>"","prijmeni"=>"","adresa"=>"","mesto"=>"","telefon"=>"",
                "email"=>"");
        list($_j,$_p,$_a,$_m,$_t)=mysql_fetch_row($res);
        $_e=$this->g_email();
        return array("jmeno"=>$_j,"prijmeni"=>$_p,"adresa"=>$_a,"mesto"=>$_m,"telefon"=>$_t,
            "email"=>$_e);
    }

    function zvys_pocitadlo() {
        $res=mysql_query("UPDATE uzivatele SET pocitadlo=pocitadlo+1 WHERE sid='".$this->sid."'");
        if (!$res) { mysql_chyba(NULL,"Nezvýšilo se počítadlo přihlášení uživatele."); }
    }

    // jako parametr se sem vkládají hodnoty z registračního formuláře (pole $_POST)
    function registrace($pole) {
        $res=mysql_query("REPLACE INTO uzivatele VALUES('".session_id()."','".$pole['u_jmeno'].
            "','".$pole['jmeno']."','".$pole['prijmeni']."','".md5($pole['heslo'])."','".
            $GLOBALS['time'].",0,'".$pole['email']."','".$pole['adresa']."','".$pole['mesto'].
            "','".$pole['telefon']."','".date("d.m.Y")."','r')");
        if (!$res | !mysql_affected_rows()) {
            mysql_chyba("Nezdařila se registrace uživatele zřejmě díky chybě v databázi.",
                "Nevložil se údaj při přechodném kroku registrace do tabulky
                'uzivatele'.");
        }
    }

    function prihlasit($u_jmeno) {
        $res=mysql_query("UPDATE uzivatele SET sid='".session_id()."',kod='p' WHERE
            uzivatel='".$u_jmeno."'");
        if (!$res | !mysql_affected_rows()) {
            mysql_chyba(NULL,"Nepodařilo se přihlásit uživatele.");
        }
        // zvýšíme počítadla přístupů
        $dt="UPDATE pocitadla SET kolik=kolik+1 WHERE co='prihlaseni'";
        $dt.=($GLOBALS['dnes'])?" OR co='prihlaseni_dnes'":"";
        $res=mysql_query($dt);
        if (!$res) { mysql_chyba("Nepodařilo se zvýšit počítadla přihlášení."); }
        if (!$GLOBALS['dnes']) {
            $res=mysql_query("UPDATE pocitadla SET kolik=kolik+1 WHERE co='prihlaseni_dnes'");
            if (!$res) { mysql_query("Nezdařilo se vynulovat počítadlo dnešních přihlášení.");}
        }
    }

    function odhlasit() {
```



```php
        $res=mysql_query("UPDATE uzivatele SET kod='' WHERE sid='".session_id()."'");
        if (!$res | !mysql_affected_rows()) { mysql_chyba(NULL,"Nepodařilo se odhlásit
            uživatele."); }
    }

    function oprava_reg($pole) {
        $res=mysql_query("REPLACE INTO uzivatele VALUES('".session_id()."','".$GLOBALS['uz_jmeno'].
            "','".$pole['jmeno']."','".$pole['prijmeni']."','".md5($pole['heslo'])."','".
            $GLOBALS['time'].",0,'".$pole['email']."','".$pole['adresa']."','".
            $pole['mesto']."','".$pole['telefon']."','".date("d.m.Y")."','t')");
        if (!$res | !mysql_affected_rows()) {
            mysql_chyba("Nezdařila se úprava registrace uživatele zřejmě díky chybě v databázi.
            ","Nevložil se údaj při přechodném kroku úpravy registračních údajů v tabulce
            'uzivatele'.");
        }
    }
}

?>
```

```php
<?

/* >>>  _in_katalog_vyrobku.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//***********  implementace internetového obchodu  ************
//**************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ***********************
//************************************************************

//************************************
//  Implementace katalogu výrobků
//************************************

// bez parametru se zobrazí jednoduchá tabulka, kde jsou jednotlivé skupiny výrobků

// pokud je v jakémkoliv parametru v URL zjištěn nedostatek, volá se defaultní fce zobraz_skupiny(),
// která zobrazí základní skupiny výrobků

$parametr_katalogu=(empty($_GET['sub']))?NULL:$_GET['sub'];
if ($parametr_katalogu<>"seznam")
    $parametr_katalogu=NULL;

if (!$parametr_katalogu) {

    zobraz_skupiny();

} else {

    if ($parametr_katalogu=="seznam") {
        // zobrazení všech výrobků v jedné tabulce
        if (!empty($_GET['gid'])) {
            // SFBUG ***
            $res_skupina=mysql_query("SELECT * FROM skupiny WHERE gid=".$_GET['gid']);
            if (!$res_skupina) { mysql_chyba(NULL,"Nepodařilo se vybrat danou skupinu
                výrobků z databáze."); }
            if (!mysql_num_rows($res_skupina))
                zobraz_skupiny();
            else
                list($aksk_gid,$aksk_nazev,$aksk_ngid)=mysql_fetch_row($res_skupina);

            // *** SFBUG ***
            $res_sznm=mysql_query("SELECT id FROM vyrobky WHERE gid=".$_GET['gid']);
            //$res_sznm=mysql_query("SELECT * FROM vyrobky WHERE gid=".$_GET['gid']);
            if (!$res_sznm) { mysql_chyba(NULL,"Nezdařilo se zjistit výrobky patřící
                do skupiny"); }
            if (mysql_num_rows($res_sznm)) {
?>
<table width="600" align="center" cellspacing="0" cellpadding="0" border="1" class="skupiny">
    <th width="550" colspan="6" height="20" align="center" bgcolor="#94bac5" class="nadpis"><?
        echo $aksk_nazev; ?></th>
    <tr  align="center" bgcolor="#62757b">
        <td width="50"> </td>
        <td width="150">Název zboží</td>
        <td width="225">Popis</td>
        <td width="75">Cena bez DPH</td>
        <td width="75">Cena s DPH</td>
        <td width="25">Do košíku</td>
    </tr>
<?
                // vypíšeme jednotlivé položky výrobků
                for ($a=0;$a<mysql_num_rows($res_sznm);$a++) {
                    list($vr_id)=mysql_fetch_row($res_sznm);
                    $vyrobek=new vyrobek($vr_id);
                    $vyrobek->vypis_polozku_tabulky();
                    unset($vyrobek);
                }
?></table>
<?
            } else {
                # výrobky neexistují
                echo "\n<p align=\"center\">Výrobky v této sekci neexistují.</p>\n";
                zobraz_skupiny();
            }
        } else {
            zobraz_skupiny();
        }
    } else {

    }
}

function zobraz_skupiny() {

    $res_gid=mysql_query("SELECT * FROM skupiny");
    if (!$res_gid) { mysql_chyba(NULL,"Nepodařilo se vybrat jednotlivé skupiny výrobků."); }
    $pocet_skupin=mysql_num_rows($res_gid);
?>
<table width="400" cellspacing="0" class="skupiny" border="1" cellpadding="0" align="center"
bgcolor="#cccccc">
  <tbody><?

    for($a=0;$a<$pocet_skupin;$a++) {
        list($gr_d[$a],$gr[$a],$gr_nd[$a])=mysql_fetch_row($res_gid);
?>
        <tr>
            <td width="100" height="100"><a href="<? echo $_SERVER['PHP_SELF'];
            ?>?m=katalog&sub=seznam&gid=<? echo strtolower($gr_d[$a]);
            ?>"><img src="grafika/<? echo strtolower($gr[$a])."_obrazek_skupiny.jpg";
            ?>" width="100" height="100" alt="<? echo $gr[$a]; ?>"></a></td>
            <td width="300" height="100"><div align="center"><a href="<?
            echo $_SERVER['PHP_SELF']; ?>?m=katalog&sub=seznam&gid=<?
            echo strtolower($gr_d[$a]); ?>"><? echo $gr[$a]; ?></a></div></td>
        </tr>
<?
    }

?>
  </tbody>
</table>
<?

}

?>
<p> </p>
```

_in_katalog_vyrobku.php Příloha č.1

```php
<?
/* >>>  _in_nakupni_kosik.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//**********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 ******************
//*****************  (licence GNU/GPL) ************************
//************************************************************

//**************************************
//  Obsluha nákupního košíku
//**************************************

// na této stránce se objeví, co všechno má zákazník v košíku a umožní mu měnit množství
// zároveň i vypíše už i konečnou cenu všech výrobků a umožní zásilku objednat

// princip manipulace s košíkem
// POST --> zákazník mění počty zboží
// GET  --> zákazník přidává druh zboží do košíku

// cenové proměnné

$cel_cena_bez_dph=0;$cel_cena_s_dph=0;$cel_dph_1=0;$cel_dph_2=0;$cel_dph=0;

// nejdříve zkontrolujeme, zda jsou předané hodnoty v pořádku

function ks_hlavicka() {

?>

<html>
<body>
<head><title>Nákupní košík</title></head>
<center>
<?

}

# je užívatel on-line ?
if (!$GLOBALS['uz_online']) {
    echo "<p> </p><p align=\"center\"><span style=\"font-size: 15px; font-weight: bolder\">Nejste
        přihlášen či registrován. Nemůžete tedy pracovat s košíkem.</span></p>";
    return;
}

$ks=0;
$ks_p=0;
if ((!empty($_POST['vyr_id'])) || (!empty($_POST['pocet']))) $ks+=3;
if (!empty($_GET['v'])) $ks++;
if ($ks<1) {
    if (je_prazdny_kosik())
        return;
        #   else
        #       kosik_chyba();
}
if ($ks==3) $ks_p=1;

if ($ks_p<>1) {

    $nk_pridat=FALSE;$nk_vyhodit=FALSE;
    if (empty($_GET['sub'])) {
        // implicitně zobrazíme obsah košíku
        $res_nk=zjisti_nakupni_kosik();
        vypis_nakupni_kosik_plus($res_nk);
    } else {
        if (($_GET['sub']!='pridat') && ($_GET['sub']!='obnovit') && ($_GET['sub']!='zmenit') &&
            ($_GET['sub']!='vyhodit') && ($_GET['sub']!='vysypat')) kosik_chyba();

        // teď se rozhodneme, co chceme vlastně dělat s košíkem, buď zobrazíme normální seznam
```



```php
        // zboží s odkazy, jak popř. měnit množství, či zobrazíme formulář, ve kterém už lze
        // množství měnit

        if ($_GET['sub']=='pridat') $nk_pridat=TRUE;
        if ($_GET['sub']=='vyhodit') $nk_vyhodit=TRUE;

                // pokud chceme vysypat košík
        if ($_GET['sub']=='vysypat') {
            vysyp_kosik();
            return;
        }

        if (($_GET['sub']=='pridat') || ($_GET['sub']=='obnovit') || ($_GET['sub']=='vyhodit')) {
            // normální seznam
            if ($nk_pridat) {
                // nemáme správné parametry
                if (empty($_GET['v'])||empty($_GET['p'])) kosik_chyba();
                if (!(is_numeric($_GET['v'])&&is_numeric($_GET['p']))) kosik_chyba();
            }

            // teď už je vše v pohodě, můžeme zobrazit hlavičku
            ks_hlavicka();

            // pokud chce zákazník přidat výrobek do koše, informujeme ho
            // o úspěchu či neúspěchu
            if ($nk_pridat) {
                $vyrobek_nk=new vyrobek($_GET['v']);
                if ($vyrobek_nk->id==-1) { // výrobek neexistuje
?>
<p> </p>
<p align="center"><span style="font-size: 15px; font-weight: bolder">Daný výrobek neexistuje, nelze
ho přidat do košíku.</span></p>
<?
                    } else {
                    // vytvoříme záznam v databázi (pokud už zákazník urč. výrobek
                    // přidal, ignoruje se to)
                    $res_nk_p=mysql_query("REPLACE INTO kosiky
                        VALUES('','".$GLOBALS['uz_jmeno']."',$vyrobek_nk->id,1)");
                    if (!$res_nk_p) { mysql_chyba("Nepodařilo se vložit výrobek
                        do košíku."); }
                }
            }

            if ($nk_vyhodit) {      // vyhození výrobku z koše
                if (!empty($_GET['v'])) {
                    if (is_numeric($_GET['v'])) {
                        $res_nk_v=mysql_query("DELETE FROM kosiky WHERE
                            ident=".$_GET['v']." AND uzivatel='".
                            $GLOBALS['uz_jmeno']."'");
                        if (mysql_affected_rows()) {
                            echo "<p> </p>\n<p align=\"center\">
                            Výrobek byl vyřazen z košíku.</p>\n<p> </p>";
                        } else {
                            echo "<p> </p>\n<p align=\"center\">
                            Výrobek v košíku už není.</p>\n<p> </p>";
                        }
                    }
                }
            }

            // nakonec zobrazíme celý obsah košíku (výrobky budou řazeny zřejmě chronologicky)
            $res_nk=zjisti_nakupni_kosik();

            // a teď vše vypíšeme do tabulky()
            vypis_nakupni_kosik_plus($res_nk);

        } elseif($_GET['sub']=='zmenit') {
            // umožníme změnu množství nějakého výrobku vypsáním formuláře
            $res_nkz=zjisti_nakupni_kosik();
            vypis_nakupni_kosik_plus($res_nkz,TRUE);
        } else {
```

```
141             // sem by to nikdy nemělo dojít
142             exit;
143         }
144 
145          }
146 } else {
147     // zpracováváme POST, tj. například úpravu množství z formuláře
148     if (!is_numeric($_POST['vyr_id']) || !is_numeric($_POST['pocet'])) {
149         echo "<p> </p><p align=\"center\"><span style=\"font-size: 15px; font-weight: bolder\">
150             Při zpracování dat z košíku došlo k chybě.</span></p>";
151         return;
152     } else {
153             $res_nk_post=mysql_query("UPDATE kosiky SET pocet=".$_POST['pocet']." WHERE uzivatel='".
154             $GLOBALS['uz_jmeno']."' AND ident=".$_POST['vyr_id']);
155         $vysl_r=mysql_affected_rows();
156         if (!$vysl_r) {
157             echo "<p> </p><p align=\"center\"><span style=\"font-size: 15px; font-weight:
    bolder\">
158                 Nezdařila se aktualizace informací o obsahu košíku.</span></p>";
159         } else {
160             $res_nk=zjisti_nakupni_kosik();
161             vypis_nakupni_kosik_plus($res_nk);
162         }
163     }
164 }
165 
166 
167 function ks_ukoncit() {
168 ?>
169 
170 </center>
171 </body>
172 </html>
173 
174 <?
175 }
176 
177 function kosik_chyba() {
178     ks_hlavicka();
179     echo "<p align=\"center\"><span style=\"font-size: 15px; font-weight: bolder\">
180         Došlo k závažné chybě při manipulaci s košíkem.</span></p>";
181     ks_ukoncit();
182     echo "\n<p> </p>";
183     exit;   // nemá smysl pokračovat
184 }
185 
186 function zjisti_nakupni_kosik() {
187     $res_nk=mysql_query("SELECT kod,ident,id,pocet,nazev,cena,dph,sklad FROM kosiky LEFT JOIN
188         vyrobky ON (kosiky.ident=vyrobky.id) WHERE kosiky.uzivatel='".$GLOBALS['uz_jmeno'].
189         "' ORDER BY kosiky.kod ASC");
190     if (!$res_nk) { mysql_chyba("Nezdařilo se zjistit obsah košíku. Informujte nás."); }
191     return $res_nk;     // vrátíme handle dotazu
192 }
193 
194 function vysyp_kosik() {
195     $res=mysql_query("DELETE FROM kosiky WHERE uzivatel='".$GLOBALS['uz_jmeno']."'");
196     if (!$res) { mysql_chyba("Nepodařilo se vysypat košík."); }
197     je_prazdny_kosik(); // zobrazí informaci, že je košík prázdný
198 }
199 
200 function je_prazdny_kosik() {
201     $res=mysql_query("SELECT * FROM kosiky WHERE uzivatel='".$GLOBALS['uz_jmeno']."' ORDER BY kod
    ASC");
202     if (!$res) { mysql_chyba("Nezdařilo se zjistit obsah košíku. Informujte nás."); }
203     if (!mysql_num_rows($res)) {
204         echo "<p> </p><p align=\"center\"><span style=\"font-size: 15px; font-weight: bolder\">
205             Košík je prázdný.</span></p>";
206                 aktualizace_tmp_objednavky(NULL,TRUE);
207         zobrazit_objednavky();
208         return TRUE;
209     }
```



```
210     return FALSE;
211 }
212 
213 # vypíše obsah košíku, popř. formulář s možností měnit množství + vytvoří dočasný záznam objednávky
214 function vypis_nakupni_kosik_plus($result,$zmena=FALSE) {
215     echo "<p align=\"right\"><a href=\"".$_SERVER['PHP_SELF']."?m=nak_kosik&sub=vysypat\">
216         Vysypat košík</a></p>\n";
217     $pocet=mysql_num_rows($result);
218         if (je_prazdny_kosik())
219         return;
220 
221     global $cel_cena_bez_dph;
222     global $cel_cena_s_dph;
223     global $cel_dph_1;
224     global $cel_dph_2;
225 
226         global $uz_pole;    // data o uživateli
227 
228     // serializovaná data košíku pro případné potvrzení objednávky
229     // (formát vysvětlen na konci implementace funkce)
230 
231     $data_obj=$GLOBALS['uz_jmeno']."\n";
232     $data_obj.=$uz_pole['jmeno']."\n";
233     $data_obj.=$uz_pole['prijmeni']."\n";
234     $data_obj.=$uz_pole['email']."\n";
235     $data_obj.=date("d.m.Y H:i")."\n";
236     $data_obj.=$uz_pole['adresa']."\n";
237     $data_obj.=$uz_pole['mesto']."\n";
238     $data_obj.=(string)$uz_pole['telefon']."\n\n";
239 
240     if ($zmena) {
241         echo "<form action=\"".$_SERVER['PHP_SELF']."?m=nak_kosik\" method=\"post\"
242             enctype=\"application/x-www-form-urlencoded\">";
243     }
244 
245 ?><table width="550" cellspacing="0" class="skupiny" border="1" cellpadding="0" align="center"
    bgcolor="#cccccc">
246 <th colspan="8" height="20" align="center" bgcolor="#94bac5" class="nadpis"> Obsah košíku </th>
247 <tr align="center" bgcolor="#62757b">
248     <td width="50">ID</td>
249     <td width="150">Název zboží</td>
250     <td width="75">Cena bez DPH</td>
251     <td width="75">DPH</td>
252     <td width="75">Cena s DPH</td>
253     <td width="35">Sklad</td>
254     <td width="30">Počet</td>
255     <td width="70">Vyhodit z košíku</td>
256 </tr>
257 <?  echo " <tr align=\"center\">\n";
258     for ($a=0;$a<$pocet;$a++) {
259         list($_kod,$_ident,$_id,$_pocet,$_nazev,$_cena,$_dph,$_sklad)=mysql_fetch_row($result);
260         $_vyr_t=new vyrobek($_id);
261 
262                 $cel_cena_bez_dph+=number_format($_cena,2)*$_pocet;
263         $cel_cena_s_dph+=number_format($_vyr_t->celkova_cena(),2)*$_pocet;
264         if ($_dph==1)
265             $cel_dph_1+=number_format($_vyr_t->dph(),2)*$_pocet;
266         elseif ($_dph==2)
267             $cel_dph_2+=number_format($_vyr_t->dph(),2)*$_pocet;
268         else
269             // DPH se neplatí (osvobozeno nebo není předmětem)
270 
271         $tmp=NULL;
272         $tmp=(string)$_id."&+&".(string)$_nazev."&+&".(string)$_pocet."&+&".(string)$_cena."&+&";
273                 $data_obj.=$tmp;
274         $data_obj.=(!$_dph)?0:(($_dph==1)?(string)(100*$GLOBALS['snizena_sazba_dph']):
275             (string)(100*$GLOBALS['zakladni_sazba_dph']));
276         $data_obj.="&+&".(string)number_format($_vyr_t->dph(),2);
277         $data_obj.="&+&".(string)number_format($_vyr_t->celkova_cena(),2)."\n";
278         $data_obj.="\n";
279 
```

```
?>
 <tr align="center">
  <td width="50"><? echo $_kod."/".$_ident; ?></td>
  <td width="150"><? echo $_nazev; ?></td>
  <td width="75"><? echo number_format($_cena,2)," Kč\n"; ?></td>
  <td width="75"><? echo number_format($_vyr_t->dph(),2)," Kč\n"; ?></td>
  <td width="75"><? echo number_format($_vyr_t->celkova_cena(),2)," Kč\n"; ?></td>
  <td width="35"><? echo ($_sklad)?"ano":"ne"; ?></td>
<?
        if (!$zmena || empty($_GET['v'])) {
?>
    <td width="40"><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=nak_kosik&sub=zmenit&v=<?
        echo $_ident; ?>"><? echo $_pocet; ?></a></td><? // uvádí odkaz na změnu množství ?>
<?
    } else {
            // formulářový prvek umožňující měnit množství
        // (zobrazujeme pouze u jednoho
        // výrobku, především kvůli snadnější implementaci, bylo by však lepší vytvořit
        // obecnější formulář pro tento účel umožňující měnit množství všech výrobků, aby
        // zákazník nemusel při změně množství u několika výrobků stále klikat na jednotlivé
        // odkazy a vracet se zpět)
        if (!is_numeric($_GET['v']) || $_GET['v']!=$_ident) {
            ?><td width="40"><a href="<? echo $_SERVER['PHP_SELF'];
                ?>?m=nak_kosik&sub=zmenit&v=<? echo $_ident; ?>"><? echo $_pocet;
                ?></a></td><? // nesouhlasí parametr ?>
<?      } else {
            echo "<td width=\"40\" align=\"center\" class=\"mnozstvi_zvyraz\">\n";
            echo "<input type=\"text\" class=\"pocet_input\" name=\"pocet\"
                value=\"".$_pocet."\">(".$_pocet.")\n";
            // *** SFBUG *** (vyr_id)
                    echo "<input type=\"hidden\" name=\"vyr_id\" value=\"".$_ident."\">\n";
                    echo "</td>\n";
        }
       }
?>   <td width="70"><a href="<? echo $_SERVER['PHP_SELF']."?m=nak_kosik&sub=vyhodit&v=".$_ident;
    ?>">vyhodit</a></td>
<?
    echo " </tr>";

    // zobrazujeme u všech výrobků (když nechceme, odkomentujeme následující řádek a pak
    // řádek o 20 pozic níže)
    // zobrazíme mezisoučet, pokud u daného výrobku máme větší množství kusů (pro přehlednost)
//  if ($_pocet>1) {
?>
 <tr align="center" bgcolor="yellow">
  <td colspan="2">Celkem tento výrobek: </td>
  <td><? echo number_format($_cena*$_pocet,2)," Kč\n"; ?></td>
  <td><? echo number_format($_vyr_t->dph()*$_pocet,2)," Kč\n"; ?></td>
  <td><? echo number_format($_vyr_t->celkova_cena()*$_pocet,2)," Kč\n"; ?></td>
  <td colspan="3">( sazba DPH: <?
    if (!$_vyr_t->dph)
        echo "osvobozeno";
    elseif ($_vyr_t->dph==1)
        echo 100*$GLOBALS['snizena_sazba_dph'];
    else {
        echo 100*$GLOBALS['zakladni_sazba_dph'];
    }
  ?> %)</td>
  </tr>
<?
//  }
}
?>
</table>
<?

    if ($zmena) {
        echo "\n<p align=\"right\"><input type=\"submit\" name=\"zmenit\" value=\"
            Potvrdit změnu množství\"></p>";
        echo "\n</form>";
    }
```

_in_nakupni_kosik.php Příloha č.1

```

    // zobrazíme celkové údaje (cena, DPH, ...)

?>
<p> </p>
<center>
<table width="400" style="font-size: 14px">
 <th colspan="2" style="font-weight: bolder; font-size:16px">Údaje o ceně</th>
 <tr>
  <td colspan="2"><br> <br></td>
 </tr>
 <tr>
  <td>Celková cena bez DPH:</td>
  <td><? echo number_format($cel_cena_bez_dph,2); ?> Kč</td>
 </tr>
  <tr>
   <td>DPH se sníženou sazbou <? echo $GLOBALS['snizena_sazba_dph']*100; ?>% :</td>
   <td><? echo number_format($cel_dph_1,2); ?> Kč</td>
 </tr>
  <tr>
   <td>DPH se základní sazbou <? echo $GLOBALS['zakladni_sazba_dph']*100; ?>% :</td>
   <td><? echo number_format($cel_dph_2,2); ?> Kč</td>
 </tr>
  <tr>
   <td>Daň z přidané hodnoty celkem:</td>
   <td><? echo number_format($cel_dph_1+$cel_dph_2,2); ?> Kč</td>
 </tr>
  <tr>
   <td>Celková cena včetně DPH:</td>
   <td><? echo floor($cel_cena_s_dph); # zaokrouhlení na koruny dolů (zvyklost lepších podniků)?>
Kč</td>
 </tr>
  <tr>
   <td>Manipulační poplatek:</td>
   <td><? echo $GLOBALS['manipulacni_poplatek']; ?> Kč</td>
 </tr>
  <tr>
   <td>Poštovné:</td>
   <td><? echo $GLOBALS['postovne']; ?> Kč</td>
 </tr>
  <tr>
   <td>Cena celkem:</td>
   <td style="color: red; font-weight:bolder; font-size:16px"><? echo floor($cel_cena_s_dph+
    $GLOBALS['manipulacni_poplatek']+$GLOBALS['postovne']); ?> Kč</td>
 </tr>

</table>
</center>
<?
        $data_obj.=(string)$GLOBALS['postovne']."\n";
    $data_obj.=(string)$GLOBALS['manipulacni_poplatek']."\n";
    $data_obj.=(string)floor($cel_cena_s_dph+$GLOBALS['postovne']+$GLOBALS['manipulacni_poplatek']);

    echo "<br><br><center><a href=\"",$_SERVER['PHP_SELF'],"?m=objednavka\" target=\"_blank\"><span
    style=\"font-size: 20px; text-decoration: underline\">Objednat ...</span></a></center>";

    // tato funkce (už nestandardně dlouhá oproti všem předpokladům :-), ještě vytvoří dočasný záznam
v tabulce
    // objednávek se stavem objednávky "0" (nepotvrzeno); jiné stavy jsou ">1" (potvrzena a pracuje
se na ní)
    // a stav "-1" už znamená "vyřízeno"

    // formát serializovaných dat v tabulce "objednavky" (sloupec "data")

    // [uzivatelske_jmeno]              \n
    // [jmeno]                  \n
    // [prijmeni]                   \n
    // [email]                  \n
    // [d.m.Y  h:i:s]                           \n      // datum a čas objednávky
    // [adresa]                                     \n
    // [mesto]                  \n
```

```
419     // [telefon]                        \n
420     //                      \n
421     //
    [id_vyrobku]&+&[nazev_vyrobku]&+&[pocet]&+&[cena_bez_dph]&+&[sazba_dph]&+&[dph]&+&[cena_s_dph]  \n
422     //                      \n
423     // [postovne]                \n
424     // [manipulacni_poplatek]           \n
425     // [celkova_cena]               \n
426
427     // ********* doplnit do databáze objednávku *********
428
429     aktualizace_tmp_objednavky($data_obj);
430     zobrazit_objednavky();  // minulé a aktivní objednávky (neumožňujeme ale uživateli
431                 // stornovat objednávky, ani je prohlížet)
432 }
433
434 function aktualizace_tmp_objednavky($data_obj=NULL,$delete=FALSE) {
435         if ($delete) {
436         $res=mysql_query("DELETE FROM objednavky WHERE uzivatel='".$GLOBALS['uz_jmeno']."' AND
    stav=0");
437         $text= "Nezdařilo se vymazat dočasný záznam o objednávce.";
438         if (!$res) { mysql_chyba(NULL,$text); }
439         return;
440     }
441
442         $res_ob=mysql_query("SELECT * FROM objednavky WHERE uzivatel='".$GLOBALS['uz_jmeno']."' AND
    stav=0");
443     if (!$res_ob) { mysql_chyba(NULL,"Nepodařilo se zjistit, zda existují data košíku v objednávkové
444         tabulce"); }
445     if (mysql_num_rows($res_ob)) {
446             $res_obb=mysql_query("UPDATE objednavky SET data='".$data_obj."' WHERE uzivatel='".
447             $GLOBALS['uz_jmeno']."' AND stav=0");
448         if (!$res_obb) { mysql_chyba(NULL,"Nezdařila se aktualizace košíku v tabulce
449             objednávek."); }
450     } else {
451         $res_obb=mysql_query("INSERT INTO objednavky VALUES ('".$GLOBALS['uz_jmeno']."','".
452             $data_obj."',0)");
453         if (!$res_obb) { mysql_chyba(NULL,"Nepodařilo se vložit obsah košíku do tabulky
454             objednávek."); }
455     }
456 }
457
458 function zobrazit_objednavky() {
459     $res=mysql_query("SELECT uzivatel FROM objednavky WHERE uzivatel='".$GLOBALS['uz_jmeno']."'
460         AND stav<>0");
461         if (!$res) { mysql_chyba(NULL,"Nepodařilo se získat informace o dřívějších objednávkách
462         zákazníka."); }
463     $res_n=mysql_num_rows($res);
464     echo (!$res_n)?"":"\n<br><p align=\"center\">(Počet vyřizovaných objednávek: ".$res_n.")</p>";
465 }
466
467 ?>
468
469
```



```
1  <?
2
3  /* >>> _in_prihlaseni.php << */
4
5  //************************************************************
6  //*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
7  //**********  implementace internetového obchodu  ************
8  //**************** @ Tomáš Psika, 2003-2004 *******************
9  //******************  (licence GNU/GPL) ***********************
10 //************************************************************
11
12 //*************************************
13 //     Přihlášení uživatele
14 //*************************************
15
16 $parametr_prihlaseni=(empty($_GET['sub']))?NULL:$_GET['sub'];
17 if ($parametr_prihlaseni!="odpoved")
18     $parametr_prihlaseni=NULL;
19
20 if (!empty($GLOBALS['uz_jmeno'])) {
21 ?>
22 <p align="center">Už jste přihlášen jako '<? echo $GLOBALS['uz_jmeno']; ?>'. Není možné se přihlásit
   znovu. Pokud se potřebujete odhlásit, klikněte <a href="?m=odhlaseni">zde</a>.</p>
23 <?
24     return;
25 }
26
27 if (!$parametr_prihlaseni) {
28 ?>
29 <p align="center">
30 <form action="?m=prihlaseni&sub=odpoved" method="POST" enctype="application/x-www-form-urlencoded">
31 Vaše přihlašovací <u>j</u>méno:    <input type="text" name="u_jmeno" size="20"
   maxlength="20" accesskey="j">
32 <br><br>
33 <u>H</u>eslo:             
34                
35         
36 <input type="password" name="heslo" size="20" maxlength="20">
37 <br><br>
38 <input type="submit" name="prihlas" value="Přihlásit se !"
   accesskey="p">             
39 <input type="reset" name="clean" value="Vyčistit pole !" accesskey="v">
40 </form>
41 </p>
42
43 <?
44 } else {
45     // lehké bezpečnostní opatření před idioty nebo útočníky
46     $o_uzivatel=htmlspecialchars($_POST['u_jmeno'],ENT_QUOTES);
47     $o_heslo=htmlspecialchars($_POST['heslo'], ENT_QUOTES);
48     if (($o_heslo!=$_POST['heslo'])||($o_uzivatel!=$_POST['u_jmeno'])||
49         (ereg("[^a-zA-Z0-9_.!?áÁčČďĎéěÉĚíÍňŇóÓřŘšŠťŤúůÚŮýÝžŽ@. -]+",$_POST['heslo'])||
50         (ereg("[^a-zA-Z0-9_.!?áÁčČďĎéěÉĚíÍňŇóÓřŘšŠťŤúůÚŮýÝžŽ@. -]+",$_POST['u_jmeno']))||
51         (ereg("[-]{2,}",$_POST['heslo']))||(ereg("[-]{2,}",$_POST['u_jmeno'])))) {
52             // tady bychom mohli přidat logování těchto událostí
53             echo "<p align=\"center\">Došlo k chybě při přihlašování. Byly vyplněny
54                 špatné údaje. Prosím zkuste to znovu a používejte zejména normální
55                 znaky české abecedy a písmena.</p>";
56             return;
57     }
58     $res=mysql_query("SELECT uzivatel FROM uzivatele WHERE uzivatel='".$o_uzivatel."'
59         AND heslo='".md5($o_heslo)."'");
60     if (!$res) { mysql_chyba(NULL,"Došlo k chybě při získávání informace, zda existuje určitý
61         uživatel."); }
62     $res_n=mysql_num_rows($res);
63     if (!$res_n) {
64         echo "<p align=\"center\">Bylo zadáno špatné uživatelské jméno či heslo. Zkuste to prosím
65          znovu <a href=\"".$_SERVER['PHP_SELF']."?m=prihlaseni\"<u>zde</u></a>.</p>";
66     } else {
67         // úspěšné přihlášení, informujeme o tom tabulku 'uzivatele'
68         global $uzivatel;
```

```
69          //$uzivatel=new uzivatel();
70          $uzivatel->prihlasit($o_uzivatel);
71          echo "<p align=\"center\">Byl jste úspěšně přihlášen jako <font color=\"red\">'".
72              $o_uzivatel."'</font>.</p>";
73      }
74  }
75
76  if ($parametr_prihlaseni<>"odpoved") {
77
78
79  ?>
80  <br>
81  <p align="right">     Pokud jste náhodou zapomněli heslo, klikněte <a
    href="<?
82      echo $_SERVER['PHP_SELF']; ?>?m=registrace&sub=zapomenute_heslo">zde</a>.</p>
83  <?
84
85  }
86
87  ?>
88
```



```
1  <?
2  /* >>> _in_odhlaseni.php <<< */
3
4  //*************************************************************
5  //*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
6  //**********  implementace internetového obchodu  *************
7  //***************** @ Tomáš Psika, 2003-2004 *******************
8  //******************  (licence GNU/GPL) ************************
9  //*************************************************************
10
11 //************************************
12 //     Odhlášení uživatele
13 //************************************
14
15 if (!empty($GLOBALS['uz_jmeno'])) {
16     global $uzivatel;
17     $uzivatel->odhlasit();
18 ?>
19 <p align="center">Odhlášení proběhlo úspěšně.</p>
20 <?
21 } else {
22 ?>
23 <p align="center">Nejste přihlášen, proto se nemůžete samozřejmě odhlásit.</p>
24 <?
25 }
26
27 ?>
28
```

```php
<?
/* >>>  _in_o_podniku.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//***********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//*************************************
//     Informace o podniku
//*************************************

?>
<blockquote><p>     Informace o podniku</p></blockquote>

```



```php
<?

/* >>> _in_registrace.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//***********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//*************************************
//     Registrace uživatele
//*************************************

$parametr_registrace=(empty($_GET['sub']))?NULL:$_GET['sub'];
if (!($parametr_registrace=="potvrzeni" || $parametr_registrace=="uprava" ||
    $parametr_registrace=="kontrola" || $parametr_registrace=="potvrzeni_upravy_registrace" ||
    $parametr_registrace=="zapomenute_heslo" || $parametr_registrace=="zaslani_hesla" ||
    $parametr_registrace=="obnova"))
        $parametr_registrace=NULL;

// zobrazení základního formuláře pro registraci a základních informací
if (!$parametr_registrace) {

if ($GLOBALS['uz_online']) {
?>
<blockquote><p>      Jste již přihlášen, pokud chcete opravit své registrační údaje, klikněte <a href="?m=registrace&sub=uprava">zde</a>.</p></blockquote>
<br><br>
<?
}
?>
<blockquote><p>     Registrace je velmi jednoduchá, stačí zadat některé základní osobní údaje a údaje o adrese, na kterou má být
objednávané zboží odesláno. Samozřejmě je nutné zadat emailovou adresu, aby Vám mohlo být posláno heslo, pokud ho zapomenete a dále pak heslo, kterým se
prokážete při návštěvě obchodu. Všechny údaje by měly být uvedeny, aby bylo možné poslat objednané zboží na dobírku.</p></blockquote>
<form action="<? echo $_SERVER['PHP_SELF']; ?>?m=registrace&sub=kontrola" method="POST" enctype="application/x-www-form-urlencoded">
<br><br>
<u>J</u>méno:        <input type="text" name="jmeno" size="20" maxlength="20" accesskey="j">
<br><br>
<u>P</u>říjmení:       <input type="text" name="prijmeni" size="20" maxlength="20" accesskey="p">
<br><br>
Přih<u>l</u>ašovací jméno:  <input type="text" name="u_jmeno" size="20" maxlength="20" accesskey="l">
<br><br>
<u>H</u>eslo:         <input type="password" name="heslo" size="20" maxlength="20" accesskey="h">
<br><br>
<u>E</u>mailová adresa:       <input type="text" name="email" size="20" maxlength="50" accesskey="e">
<br><br>
A<u>d</u>resa:         <input type="text" name="adresa" size="50" maxlength="100" accesskey="d">
<br><br>
<u>M</u>ěsto:            <input type="text" name="mesto" size="28" maxlength="30" accesskey="m">
<br><br>
<u>T</u>elefon:         <input type="text" name="telefon" size="20" maxlength="20" accesskey="t">
<br><br>
<input type="submit" name="reg" value="Registrovat !" accesskey="s">
</form>
<?
} elseif ($parametr_registrace=="kontrola") {
    if (!empty($_POST['reg'])) {        // ** SFBUG **
```

```
59          // proparsujeme všechny hodnoty poslané POSTem
60          // navíc zkontrolujeme velikost jednotlivých polí, obrana proti útoku přehráním
61          // !! nekontrolujeme validitu dat poslaných formulářem (umožníme uživateli napsat cokoliv,
    třeba si bude
62          // obchod jen zkoušet, dáme mu možnost vše opravit, až bude chtít)
63          $pars_e=kontrola_reg_udaju();
64          if ($pars_e) {
65              echo "<p align=\"center\">Zřejmě jste zadal při registraci špatné údaje. Používejte
    prosím základní
66                  alfanumerické znaky při vyplňování formuláře.</p>";
67          } else {
68              // kontrolujeme pouze, zda je ve formuláři správně zadáno uživatelské
69              // jméno a heslo
70              if (empty($_POST['u_jmeno']) | empty($_POST['heslo'])) {
71                  echo "<p align=\"center\">Nezadal jste ani ty nejzákladnější údaje
72                      při registraci, tj. uživatelské jméno a heslo. Vraťte se zpět
73                      a vyplňte alespoň tyto údaje. Nebo klikněte
74                      <a href=\"?m=registrace\">sem</a>.</p>";
75                  return;
76              }
77              // neexistuje nám už takový uživatel se zadaným jménem ?
78              $res=mysql_query("SELECT sid FROM uzivatele WHERE uzivatel='".$_POST['u_jmeno'].
79                  "' AND kod<>'r'");
80              if (!$res) { mysql_chyba(NULL,"Nepodařilo se nám zjistit, jestli už neexistuje
81                  registrovaný uživatel se zadaným jménem."); }
82              if (mysql_num_rows($res)) {// takový uživatel existuje, dáme to vědět uživateli
83                  echo "<p align=\"center\">Uživatel se zadaným uživatelským jménem v obchodě
84                      už existuje, zvolte si prosím jiné uživatelské jméno.</p>";
85                  return; // vracíme se
86              }
87              // pokud jsou údaje v pořádku, také si je uložíme do tabulky s uživateli
88              // (ve formě přechodných dat)
89              $uz_tmp=new uzivatel();
90              $uz_tmp->registrace($_POST);
91              echo "<p align=\"center\">Teď můžete potvrdit všechny zde vypsané údaje nebo se
92                  vrátit zpět a své údaje opravit.</p><br>\n<b>Zadané údaje:</b>\n<br><br>
93                  Jméno:      ".$_POST['jmeno']."<br>\n
94                  Příjmení:    ".$_POST['prijmeni']."<br><br>\n
95                  <font color=\"red\">Uživatelské jméno:</font> ".$_POST['u_jmeno'].
96                  "<br><br>\n<font color=\"red\">Emailová adresa:</font>   
97                   ".$_POST['email']."<br><br>\nAdresa:   ".
98                  $_POST['adresa']."<br>\nMěsto:    ".$_POST['mesto'].
99                  "<br><br>\nTelefon:  ".$_POST['telefon']."<br><br>\n
100                 <form action=\"".$_SERVER['PHP_SELF']."?m=registrace&sub=potvrzeni\"
101                 method=\"POST\"  enctype=\"application/x-www-form-urlencoded\">\n<input
102                 type=\"submit\"  name=\"reg_kontrola\" value=\"Potvrdit údaje\"
103                 accesskey=\"p\">\n </form>";
104         }
105     } else {        // ** SFBUG ** start
106             echo "<p align=\"center\">Nejsou žádné údaje ke kontrole registrace.</p>";
107     }           // ** SFBUG ** end
108 } elseif ($parametr_registrace=="potvrzeni") {
109     // provede se již konečný zápis do databáze a potvrdíme úspěšnost registrace
110     if (!empty($_POST['reg_kontrola'])) {       // ** SFBUG **
111         $res=mysql_query("UPDATE uzivatele SET kod='' WHERE sid='".session_id()."'");
112             if (!$res) { mysql_chyba(NULL,"Nezdařilo se potvrzení registračních informací
113                 v databázi během dokončování registrace."); }
114                 echo "<p align=\"center\">Jste úspěšně registrován v obchodě, můžete se
115                 přihlásit a nakupovat. Děkujeme za Váš zájem o naše výrobky.</p>";
116         } else {        // ** SFBUG ** start
117             echo "<p align=\"center\">Nejsou žádné údaje k potvrzení registrace.</p>";
118         }           // ** SFBUG ** end
119 } elseif ($parametr_registrace=="uprava") {
120         // zákazníkovi vypíšeme, kde bude mít formulář a po pravé straně v závorkách uvedeny
121         // starší hodnoty
122         if (!$GLOBALS['uz_online']) {
123             echo "<p align=\"center\">Nejste přihlášen jako žádný uživatel, nemůžete
124                 tedy měnit své registrační údaje. Pokud jste zapomněl heslo a nemůžete
125                 se přihlásit, klikněte <a href=\"?m=registrace&sub=zapomenute_heslo\">
126                 zde</a></p>";
127         } else {
```



```
128             $res=mysql_query("SELECT * FROM uzivatele WHERE sid='".session_id()."' AND
129                 uzivatel='".$GLOBALS['uz_jmeno']."'");
130             if (!$res) { mysql_chyba("Nezdařilo se zjistit Vaše registrační údaje.","Nenašly
131             se registrační údaje z databáze při pokusu je upravit."); }
132             list($tmp_sid,$tmp_uzivatel,$tmp_jmeno,$tmp_prijmeni,$tmp_heslo,
133                 $tmp_predesly_pristup,$tmp_pocitadlo,$tmp_email,$tmp_adresa,$tmp_mesto,
134                 $tmp_telefon,$tmp_datum_registrace,$tmp_kod)=mysql_fetch_row($res);
135             // teď vypíšeme formulář i se starými údaji
136 ?>
137 <blockquote><p>     Zde můžete opravit své registrační údaje. Staré údaje
    jsou zobrazeny v závorkách napravo od jednotlivých polí, nové zadávejte do jednotlivých políček.
    Pokud nějakou položku neuvedete, vymaže starou hodnotu. Heslo musí být uvedeno.</p></blockquote>
138 <form action="<? echo $_SERVER['PHP_SELF']; ?>?m=registrace&sub=potvrzeni_upravy_registrace"
    method="POST" enctype="application/x-www-form-urlencoded">
139 <br><br>
140 <u>J</u>méno:       <input type="text" name="jmeno" value="<?
    echo $tmp_jmeno; ?>" size="20" maxlength="20" accesskey="j">     (<? echo
    (empty($tmp_jmeno))?'\'není uvedeno\'':$tmp_jmeno; ?>)
141 <br><br>
142 <u>P</u>říjmení:     <input type="text" name="prijmeni" value="<? echo
    $tmp_prijmeni; ?>" size="20" maxlength="20" accesskey="p">     (<? echo
    (empty($tmp_prijmeni))?'\'není uvedeno\'':$tmp_prijmeni; ?>)
143 <br><br>
144 Přih<u>l</u>ašovací jméno:  <input type="text" disabled name="u_jmeno" value="<? echo
    $tmp_uzivatel; ?>" size="20" maxlength="20"
    accesskey="l">     ('uživatelské jméno nelze změnit')
145 <br><br>
146 <u>H</u>eslo (nové):   <input type="password" name="heslo" size="20" maxlength="20"
    accesskey="h">     ( 'nezobrazuje se' )
147 <br><br>
148 <u>E</u>mailová adresa:      <input type="text" name="email"
    value="<? echo $tmp_email; ?>" size="20" maxlength="50"
    accesskey="e">     (<? echo (empty($tmp_email))?'\'není
    uvedeno\'':$tmp_email; ?>)
149 <br><br>
150 A<u>d</u>resa:      <input type="text" name="adresa" value="<? echo
    $tmp_adresa; ?>" size="50" maxlength="100" accesskey="d">     (<? echo
    (empty($tmp_adresa))?'\'není uvedeno\'':$tmp_adresa; ?>)
151 <br><br>
152 <u>M</u>ěsto:        <input type="text" name="mesto"
    value="<? echo $tmp_mesto; ?>" size="28" maxlength="30"
    accesskey="m">     (<? echo (empty($tmp_mesto))?'\'není
    uvedeno\'':$tmp_mesto; ?>)
153 <br><br>
154 <u>T</u>elefon:      <input type="text" name="telefon" value="<?
    echo $tmp_telefon; ?>" size="20" maxlength="20" accesskey="t">     (<? echo
    (empty($tmp_telefon))?'\'není uvedeno\'':$tmp_telefon; ?>)
155 <br><br>
156 <input type="submit" name="reg_uprava" value="Potvrdit úpravu registračních údajů !" accesskey="s">
157 </form>
158 <?
159         }
160 } elseif ($parametr_registrace=="potvrzeni_upravy_registrace") {
161         // potvrzení úpravy registračních údajů zákazníka
162         if ((!$GLOBALS['uz_online']) || (empty($_POST['heslo']))) {
163             echo "<p align=\"center\">Došlo k chybě během potvrzování nových registračních
164                 údajů. Možná nebylo uvedeno heslo. Nelze pokračovat.</p>";
165         } else {
166             if (!empty($_POST['reg_uprava'])) {
167                 // potvrdíme hodnoty v databázi a smažeme dočasnou položku v tabulce
168                 // nejdříve ale také zkontrolujeme, jestli nejsou zadány špatné údaje
169                 $pars_e=kontrola_reg_udaju();
170                 if (!$pars_e) {
171                     if (!empty($_POST['reg_uprava'])) {     // ** SFBUG **
172                         // pokud jsou údaje v pořádku, také si je uložíme
173                         // do tabulky s uživateli
174                         $uz_tmp=new uzivatel();
175                         $uz_tmp->oprava_reg($_POST);
176                         $res=mysql_query("UPDATE uzivatele SET kod='' WHERE
177                             sid='".session_id()."' AND uzivatel='".
178                             $GLOBALS['uz_jmeno']."'");
```

```
179                         if (!$res) { mysql_chyba(NULL,"Nezdařilo se potvrzení
180                             registračních informací v databázi během
181                             dokončování úpravy registrace."); }
182                         echo "<p align=\"center\">Úspěšně jste změnil své
183                             registrační údaje v obchodě, byl jste odhlášen,
184                             musíte se znovu přihlásit a pak teprve nakupovat.
185                             Děkujeme za Váš zájem o naše výrobky.</p>";
186                     } else {        // ** SFBUG ** start
187                         echo "<p align=\"center\">Nejsou žádné údaje k potvrzení
188                             úpravy registrace.</p>";
189                     }           // ** SFBUG ** end
190                 } else {
191                     echo "<p align=\"center\">Zadal jste při úprave registrace
192                         špatné údaje. Používejte prosím základní alfanumerické
193                         znaky při vyplňování formuláře. Zkuste to prosím
194                         znovu.</p>";
195                 }
196             } else {
197                 echo "<p align=\"center\">Nejsou žádné údaje k potvrzení úpravy Vaší
198                     registrace.</p>";
199             }
200         }
201 } elseif ($parametr_registrace=="zapomenute_heslo") {
202         // chování při zapomenutí hesla zákazníkem
203         // mechanismus funguje tak, že je na emailovou adresu nepřihlášeného uživatele je zasláno
204         // přechodné heslo, které je pak zpracováno skriptem a umožněno uživateli opravit své
205         // registrační údaje
206         if ($GLOBALS['uz_online']) {
207             echo "<p align=\"center\">Jste přihlášen, proč tedy chcete znát své heslo? To
208                 můžete udělat přímo <a href=\"?m=registrace&sub=uprava\">zde</a>. Pokud
209                 chcete obnovit heslo pro někoho jiného, nejdříve se prosím odhlašte a pak
210                 navštivte registraci, kde najdete odkaz na tuto stránku.</p>";
211         } else {
212 ?>
213 <p align="center">Na emailovou adresu, která byla zadána při registraci tohoto uživatele bude
    zasláno dočasné heslo, které použijete k úpravě svých registračních údajů.</p>
214 <p>
215 <form action="<? echo $_SERVER['PHP_SELF']; ?>?m=registrace&sub=zaslani_hesla" method="POST"
    enctype="application/x-www-form-urlencoded">
216 Vaše uživatelské jméno: <input type="text" name="uzivatel" size="20" maxlength="30">
217 <br><br>
218 <input type="submit" name="zaslani_hesla" value="Žádost o zaslání hesla emailem !">
219 </form>
220 </p>
221 <?
222         }
223 } elseif ($parametr_registrace=="zaslani_hesla") {
224         // zaslání nového dočasného hesla pro zadaného uživatele
225         if (!$GLOBALS['uz_online']) {
226             if (empty($_POST['zaslani_hesla'])||(empty($_POST['uzivatel']))) {// ** SFBUG **
227                 echo "<p align=\"center\">Došlo k chybě, nemá smysl pokračovat.</p>";
228             } else {
229                 if ((htmlspecialchars($_POST['uzivatel'])!=$_POST['uzivatel'])||
230                     (strlen($_POST['uzivatel'])>30)) {  // ** SFBUG **
231                     echo "<p align=\"center\">Došlo k chybě, nemá smysl
232                         pokračovat.</p>";
233                 } else {
234                     // zjistíme email z databáze
235                     $res_h=mysql_query("SELECT email FROM uzivatele
236                         WHERE uzivatel='".$_POST['uzivatel']."'");
237                     if (!$res_h) { mysql_chyba(NULL,"Nezdařila se akce pro uživatele,
238                     který zapomněl své heslo."); }
239                     if (mysql_num_rows($res_h)==1) {
240                         list($tmp_em)=mysql_fetch_row($res_h);
241                         if (empty($tmp_em)) {
242                             echo "<p align=\"center\">Nepodařilo se získat
243                             emailovou adresu uživatele. Asi jste ji
244                             neuvedl při registraci, což byla vážná
245                             chyba. Pokud chcete nadále toto uživatelské jméno
246                             v našem obchodě používat, kontaktujte nás.</p>";
247                             return;
```



```
248                         }
249                         // vlastní zaslání hesla
250                         $text_emailu="Někdo (zřejmě Vy) si vyžádal obnovu ".
251                             "registračních údajů pro internetový obchod firmy".
252                             " ".$GLOBALS['firma']."\n\n\nUživatelské jméno: ".
253                             $_POST['uzivatel']."\nKlikněte na následující ".
254                             "odkaz sloužící k obnově registračních údajů: ".
255                             $GLOBALS['domenova_adresa'].$_SERVER['PHP_SELF'].
256                             "?m=registrace&sub=obnova&uz=".$_POST['uzivatel'].
257                             "&hash=".md5($_POST['uzivatel']."obnova__hesla".
258                             date("dmY")).".\n\n\nS pozdravem\n\nVáš ".
259                             "internetový obchod ".
260                             strtoupper($GLOBALS['firma']);
261                         if (mail($tmp_em,"Obnova registračních údajů pro ".
262                             "internetový obchod firmy ".$GLOBALS['firma'],
263                             $text_emailu)) {
264                                 echo "<p align=\"center\">Byly obnoveny
265                                 registrační údaje v našem obchodě,
266                                 po přečtení emailu klikněte na
267                                 odkaz v něm uvedený.</p>";
268                             // aktualizace databáze
269                             $ress=mysql_query("UPDATE uzivatele SET kod='z',
    sid='docasne_irelevantni' WHERE uzivatel='".$_POST['uzivatel']."'");
270                             if (!$ress) { mysql_chyba(NULL,"Nezdařilo se
271                                 aktualizovat kód a sid v tabulce uživatelů,
272                                 který má zajistit obnovu zapomenutého
273                                 hesla."); }
274                         } else {
275                             echo "<p align=\"center\">Během odesílání emailu
276                                 došlo k chybě.</p>";
277                         }
278                     } else {
279                         echo "<p align=\"center\">Nepodařilo se získat emailovou
280                             adresu uživatele. Nelze tedy pokračovat.</p>";
281                     }
282                 }
283             }
284         } else {
285             echo "<p align=\"center\">Došlo k chybě, nemá smysl pokračovat.</p>";
286         }
287 } elseif ($parametr_registrace=="obnova") {
288     // nejdříve zjistíme, zda máme v URI také proměnnou 'uz' a 'hash' (při opravě registračních
289     // údajů z emailu)
290         if ((empty($_GET['uz']))||(empty($_GET['hash']))) {
291             echo "<p align=\"center\">Došlo k chybě při obnově registračních údajů, nemá smysl
292             pokračovat.</p>";
293         } else {
294             // kontrolujeme hash
295             $hs_ok=md5($_GET['uz']."obnova__hesla".date("dmY"));
296             if ($hs_ok!=$_GET['hash']) {
297                 echo "<p align=\"center\">Došlo k chybě při obnově registračních
298                 údajů. Zkuste si odeslat dočasné heslo znovu.</p>";
299             } else {
300                 // rovnou už aktualizujeme databázi
301                 $res=mysql_query("SELECT kod FROM uzivatele WHERE uzivatel='".
302                     $_GET['uz']."'");
303                 if (!$res) { mysql_chyba(NULL,"Nezdařilo se získat kontrolní kód v tabulce
304                 uživatelů při obnovování registračních dat."); }
305                 $res_n=mysql_num_rows($res);
306                 if ($res_n==0) {
307                     echo "<p align=\"center\">Došlo k chybě a pravděpodobně nebudete
308                         moci upravit své registrační údaje. Kontaktujte nás o Vašem
309                         problému.</p>";
310                 } else {
311                     list($r_tmp)=mysql_fetch_row($res);
312                     if ($r_tmp=="p" | $r_tmp=="") {
313                         echo "Zdá se, že jste buď přihlášen nebo nebyla zjištěna
314                             žádost o úpravu registračních dat.";
315                     } elseif ($r_tmp=="z") {
316                         // tady bychom měli být vždy, když projde všechno v pořádku
317                         $rrr=mysql_query("UPDATE uzivatele SET kod='p',sid='".
```

```
318                             session_id()."' WHERE uzivatel='".$_GET['uz']."'");
319                         if (!$rrr) { mysql_chyba(NULL,"Nepodařilo se dočasně
320                             aktivovat přihlášení uživatele při pokusu o obnovu
321                             zapomenutého hesla uživatele."); }
322                         echo "<p align=\"center\">Došlo k úspěšnému přihlášení
323                             uživatele za účelem obnovy hesla. Klikněte <a
324                             href=\"?m=registrace&sub=uprava\">zde</a>, abyste
325                             mohli zadat nové heslo.</p>";
326                     } else {
327                         echo "<p align=\"center\">Došlo k chybě při obnově
328                             registračních dat. Nebyl zjištěn stav zákazníka
329                             v obchodě. Kontaktujte nás o Vašem problému.</p>";
330                     }
331                 }
332             }
333         }
334 } else {
335         // sem to už nemůže dojít
336 }
337
338 function kontrola_reg_udaju() {
339     $pars_e=FALSE;
340     $pole_velikosti=array(20,20,20,20,50,100,30,20);
341     $pole_uk=0;
342     foreach ($_POST as $tmp) {
343         if (($tmp!=htmlspecialchars($tmp))||
344             (ereg("[^a-zA-Z0-9_,!?áÁčČďĎéěÉĚíÍňŇóÓřŘšŠťŤúŮůŮýÝžŽ@. -]+",$tmp)||
345             (ereg("[-]{2,}",$tmp))))
346             $pars_e++;
347         if ($pole_uk<8 && strlen($tmp)>$pole_velikosti[$pole_uk])
348             $pars_e++;
349         $pole_uk++;
350     }
351     return $pars_e;
352 }
353
354 ?>
355
```



```
1  <?
2
3  /* >>> _in_standardni_zahlavi.php <<< */
4
5  //************************************************************
6  //*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
7  //**********  implementace internetového obchodu  ************
8  //***************** @ Tomáš Psika, 2003-2004 ******************
9  //******************  (licence GNU/GPL) ***********************
10 //************************************************************
11
12 //***************************************
13 //  Standardní záhlaví
14 //***************************************
15
16 ?>
17 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
18 <html><body>
19 <head>
20 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
21 <meta name="Author" content="Tomáš Psika">
22 <meta name="description" lang="cs" content="Internetový obchod, e-shop, e-commerce, e-business">
23 <meta name="Copyright" content="Tomas Psika, 2003/04">
24 <meta name="Resource-Type" content="document">
25 <meta name="Robots" content="all,follow">
26 <meta http-equiv="Content-Language" content="cs">
27 <meta http-equiv="Reply-to" content="tomas_psika@cbox.cz">
28 <meta name="Pragma" content="no-cache">
29 <meta name="Keywords" content="obchod, komerce, e-shop, internetový obchod, internet, e-komerce,
   e-commerce">
30 <? echo $this->napis_titulek(); ?>
31 <link rel="stylesheet" type="text/css" href="styl.css">
32 <!-- link rel="shortcut icon" href="favicon.ico" type="image/x-icon" -->
33 <script type="text/javascript" src="service.js"></script>
34 <script type="text/javascript">
35 <!--
36
37 preload_loga();
38 vratitstatus();
39
40 -->
41 </script>
42 </head>
43 <body bgcolor="white" text="black" link="black" alink="black" vlink="black">
44 <table width="764" cellspacing="0" class="hlavni_tabulka" cellpadding="0" align="center">
45   <tbody>
46     <tr>
47       <td><img src="grafika/logo_ok_adresa.jpg" alt="Adresa" width="764" height="22"
   border="0"></td>
48     </tr>
49     <tr>
50       <td><a href="<? echo $_SERVER['PHP_SELF']; ?>"><img src="grafika/logo_ok_hlavni_logo.jpg"
   alt="Hlavní logo" width="764" height="104" border="0"></a></td>
51     </tr>
52     <tr>
53       <td>
54         <table cellspacing="0" cellpadding="0" border="0">
55             <tr>
56                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=o_podniku"><img name="obr1"
   src="grafika/logo_ok_o_podniku.jpg" OnMouseOver="zamen('obr1','grafika/logo_ok_on_o_podniku.jpg')"
   OnMouseOut="zamen('obr1','grafika/logo_ok_o_podniku.jpg')" alt="O podniku" width="110" height="27"
   border="0"></a></td>
57                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=katalog"><img name="obr2"
   src="grafika/logo_ok_katalog_vyrobku.jpg"
   OnMouseOver="zamen('obr2','grafika/logo_ok_on_katalog_vyrobku.jpg')"
   OnMouseOut="zamen('obr2','grafika/logo_ok_katalog_vyrobku.jpg')" alt="Katalog výrobků" width="160"
   height="27" border="0"></td>
58                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=nak_kosik"><img name="obr3"
   src="grafika/logo_ok_nakupni_kosik.jpg"
   OnMouseOver="zamen('obr3','grafika/logo_ok_on_nakupni_kosik.jpg')"
   OnMouseOut="zamen('obr3','grafika/logo_ok_nakupni_kosik.jpg')" alt="Nákupní košík" width="145"
```

```
   height="27" border="0"></td>
59                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=registrace"><img name="obr4"
   src="grafika/logo_ok_registrace.jpg" OnMouseOver="zamen('obr4','grafika/logo_ok_on_registrace.jpg')"
   OnMouseOut="zamen('obr4','grafika/logo_ok_registrace.jpg')" alt="Registrace" width="125" height="27"
   border="0"></td>
60                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=prihlaseni"><img name="obr5"
   src="grafika/logo_ok_prihlaseni.jpg" OnMouseOver="zamen('obr5','grafika/logo_ok_on_prihlaseni.jpg')"
   OnMouseOut="zamen('obr5','grafika/logo_ok_prihlaseni.jpg')" alt="Přihlášení" width="120" height="27"
   border="0"></td>
61                 <td><a href="<? echo $_SERVER['PHP_SELF']; ?>?m=kontakt"><img name="obr6"
   src="grafika/logo_ok_kontakt.jpg" OnMouseOver="zamen('obr6','grafika/logo_ok_on_kontakt.jpg')"
   OnMouseOut="zamen('obr6','grafika/logo_ok_kontakt.jpg')" alt="Kontakt" width="104" height="27"
   border="0"></td>
62               </tr>
63           </table>
64         </td>
65       </tr>
66       <tr>
67 <td class="vlastni_obsah">
68       <table width="100%">
69       <tr>
70       <td align="left"><? echo $this->nadpis(); ?></td>
71       <td align="right"> <?
72
73 if ($GLOBALS['zobrazit_stav']) {
74
75     echo "(<span style=\"color:#aaaaaa; font-weight:bold\">";
76
77     if (empty($GLOBALS['uz_jmeno']))
78         echo "Nejste přihlášen";
79     else
80         echo "Přihlášen jako '".htmlspecialchars($GLOBALS['uz_jmeno'])."'";
81
82     echo "</span>)";
83 }
84
85 ?></td>
86       </tr>
87       </table>
88 <br><br>
89
90 <!-- ********************************** -->
91
```



```
1  <?
2  /* >>> _in_standardni_zapati.php <<< */
3
4  ///*************************************************************
5  //*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
6  //**********  implementace internetového obchodu  *************
7  //***************** @ Tomáš Psika, 2003-2004 *******************
8  //******************  (licence GNU/GPL) ************************
9  //*************************************************************
10
11 //***************************************
12 // Standardní zápatí
13 //***************************************
14
15 ?>
16 <br><br>
17 </td>
18 </tr>
19 <!-- ********************************** -->
20
21     <tr class="zapati">
22       <td width="764" height="25" align="right">&copy; Tomáš Psika, 2003-2004</td>
23     </tr>
24   </tbody>
25 </table>
26 </html>
27
```

```php
<?
/* >>>  _in_objednavka.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//***********  implementace internetového obchodu  ***********
//***************** @ Tomáš Psika, 2003-2004 ******************
//*****************  (licence GNU/GPL) ************************
//************************************************************

//**************************************************
//            Zpracování objednávky
//**************************************************

// zkontrolujeme všechny náležitosti objednávky (hlavně adresu pro odeslání dobírky)
// a hned vypíšeme celou závaznou objednávku

// tímto je už zboží objednáno, není třeba už nic potvrzovat

// vyzískání informací o možné objednávce z tabulky

if (empty($GLOBALS['uz_online'])) {
    echo "<p align=\"center\" style=\"font-size: 16px\">Nejste přihlášen, není tedy co objednávat.</p>";
    return;
}

$res=mysql_query("SELECT data FROM objednavky WHERE uzivatel='".$GLOBALS['uz_jmeno']."' AND stav=0");
if (!$res) { mysql_chyba("Nepodařilo se zjistit obsah objednávky"); }
if (mysql_num_rows($res)) {
    list($data)=mysql_fetch_row($res);
    $obj_pole=objednavka_parse($data);
        // testujeme, zda máme všechna důležitá data
    if (empty($obj_pole['jmeno'])||empty($obj_pole['prijmeni'])||empty($obj_pole['adresa'])||
        empty($obj_pole['mesto'])||empty($obj_pole['email'])) {
?>
<p align="center" style="font-size:14px; color: red">Nelze obsah košíku objednat, protože nebyly při registraci uvedeny některé náležité údaje jako je email, adresa, město nebo celé jméno a příjmení. Ty jsou nutné pro zajištění zásilky (email pro informování o stavu vyřízení objednávky).</p>
<?
    return; // nelze pokračovat
}
    vypis_obsah_objednavky($obj_pole);
    objednej();
} else {
    echo "<p align=\"center\" style=\"font-size: 14px\">Není co objednávat, nenalezl se
        žádný obsah košíku.</p>";
    return;
}

// proparsuje všechna data uložená v databázi, formát dat viz _in_nakupni_kosik.php (konec souboru)
function objednavka_parse($data) {
    $vyrob=NULL;
    $temp=$data;
    $udaje=explode("\n",$temp);
    $ret['uz_jmeno']=$udaje[0];
        $ret['jmeno']=$udaje[1];
    $ret['prijmeni']=$udaje[2];
    $ret['email']=$udaje[3];
    $ret['datum']=$udaje[4];
    $ret['adresa']=$udaje[5];
    $ret['mesto']=$udaje[6];
    $ret['telefon']=$udaje[7];

    $a=1;
    while($a) {
        $udaje2[$a-1]=explode("&+&",$udaje[$a+8]);
        $vyrob[$a-1]['id']=$udaje2[$a-1][0];
        $vyrob[$a-1]['nazev']=$udaje2[$a-1][1];
        $vyrob[$a-1]['pocet']=$udaje2[$a-1][2];
        $vyrob[$a-1]['cena_bez_dph']=$udaje2[$a-1][3];
```



```php
        $vyrob[$a-1]['sazba_dph']=$udaje2[$a-1][4];
        $vyrob[$a-1]['dph']=$udaje2[$a-1][5];
        $vyrob[$a-1]['cena_s_dph']=$udaje2[$a-1][6];
        $vyrob[$a-1]['cel_cena']=$udaje2[$a-1][3]*$udaje2[$a-1][2];
        $vyrob[$a-1]['cel_dph']=$udaje2[$a-1][5]*$udaje2[$a-1][2];
        $vyrob[$a-1]['cel_cena_s_dph']=$udaje2[$a-1][6]*$udaje2[$a-1][2];
        if (count(explode("&+&",$udaje[$a+9]))<>7)
                    break;
        else
            $a++;
    }

    $ret['vyrobek']=$vyrob;
    $ret['postovne']=$udaje[count($udaje)-3];
    $ret['manipulacni_poplatek']=$udaje[count($udaje)-2];
    $ret['celkova_cena']=$udaje[count($udaje)-1];
    return $ret;    # tímto vrátíme dynamické složité třírozměrné smíšené pole :-)
}

function vypis_obsah_objednavky($ret) {
?>
<p align="center" style="font-size: 22px; font-weight: bolder: color: red">Objednávka (kupní smlouva)</p>
<p align="left" style="font-size: 14px">
Následující text potvrzuje Vaší objednávku u našeho podniku. Měly byste si jej uchovat pro případ reklamace či pro kontrolu.
<br><br>
Datum a čas objednávky: <? echo $ret['datum']; ?><br><br>
Identifikátor objednávky: <?
    //echo $GLOBALS['uz_jmeno'].str_replace(".","",str_replace(":","",$ret['datum']));
    echo $GLOBALS['uz_jmeno'].ereg_replace("(\.+)|( +)|(:+)","",$ret['datum']);
?>
<br><br><br><u>Kupující</u><br><br>
<table width="90%" style="font-size: 14px">
<tr>
 <td>Jméno a příjmení kupujícího: <? echo $ret['jmeno']." ".$ret['prijmeni']; ?></td>
<tr>
 <td>Adresa: <? echo $ret['adresa'].", ".$ret['mesto']; ?></td>
</tr>
</table>
<br><br>
<u>Prodávající</u><br><br>
<table width="90%" style="font-size: 14px">
<tr>
 <td>Jméno podniku: <? echo $GLOBALS['nazev_podniku']; ?></td>
</tr>
<tr>
 <td>Sídlo: <? echo $GLOBALS['sidlo']; ?></td>
</tr>
<tr>
 <td>IČO: <? echo $GLOBALS['ico']; ?></td>
</tr>
<tr>
 <td>DIČ: <? echo $GLOBALS['dic']; ?></td>
</tr>
</table>
</p>
<table width="100%" style="font-size: 12px; border-style: solid; border-width: 2px">
 <tr align="center">
  <td>Výrobek</td>
  <td>Cena bez DPH</td>
  <td>Sazba DPH</td>
  <td>DPH</td>
  <td>Cena s DPH</td>
  <td>Počet kusů</td>
  <td>Cena celkem bez DPH</td>
  <td>DPH celkem</td>
  <td>Cena celkem s DPH</td>
 </tr><br><br><?
    for ($a=0;$a<count($ret['vyrobek']);$a++) {
?>
```

```
 <tr align="center" bgcolor="lightblue">
  <td><? echo $ret['vyrobek'][$a]['nazev']; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['cena_bez_dph'],2)." Kč"; ?></td>
  <td><? echo $ret['vyrobek'][$a]['sazba_dph']." %"; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['dph'],2)." Kč"; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['cena_s_dph'],2)." Kč"; ?></td>
  <td><? echo $ret['vyrobek'][$a]['pocet']." ks"; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['cel_cena'],2)." Kč"; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['cel_dph'],2)." Kč"; ?></td>
  <td><? echo number_format($ret['vyrobek'][$a]['cel_cena_s_dph'],2)." Kč"; ?></td>
 </tr>
<?
    }
?>
</table>
<p> </p>
<table width="100%" align="left" style="color: red; font-size: 14px">
 <tr align="left">
  <td>Celková cena s DPH</td>
  <td><? echo number_format($ret['celkova_cena']-$ret['postovne']-$ret['manipulacni_poplatek'],2)."
Kč";
    ?></td>
 </tr>
 <tr align="left">
  <td>Poštovné</td>
  <td><? echo number_format($ret['postovne'],2)." Kč"; ?></td>
 </tr>
 <tr align="left">
  <td>Manipulační poplatek</td>
  <td><? echo number_format($ret['manipulacni_poplatek'],2)." Kč"; ?></td>
 </tr>
 <tr align="left">
  <td><p>Celková cena k zaplacení</p><p> </p></td>
  <td style="font-weight: bolder"><p><? echo number_format($ret['celkova_cena'],2)." Kč";
    ?></p><p> </p></td>
 </tr>
</table>
<?
}

function objednej() {
    $res=mysql_query("SELECT stav FROM objednavky WHERE uzivatel='".$GLOBALS['uz_jmeno']."'
        ORDER BY stav DESC");
    if (!$res) { mysql_chyba(NULL, "Nezjistilo se pořadové číslo objednávky u daného uživatele."); };
        list($stav)=mysql_fetch_row($res);
    $stav++;
    $res=mysql_query("UPDATE objednavky SET stav=".$stav." WHERE uzivatel='".$GLOBALS['uz_jmeno']."'
        AND stav=0");
    if (!$res) { mysql_chyba(NULL, "Nezdařilo se přidat další objednávku uživatele."); }

    echo "<center>Objednávka byla úspěšně zařazena do databáze.</center>";
}

?>
```



```
<?
/* >>> _in_uvodni_stranka.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//**********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 ******************
//******************  (licence GNU/GPL) ***********************
//************************************************************

// Skript vítající potenciálního zákazníka

?>

```

```php
<?
/* >>>  _in_kontakt.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//************************************
//  Kontaktní informace
//************************************

$info_email="info@xinerama.cz";

?>

```



```php
<?
/* >>> podnikove_udaje.php <<< */

//*************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//**********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//*************************************************************

//************************************************
//              Podnikové údaje
//************************************************

// globální proměnné

$nazev_podniku="Xinerama, s.r.o.";
$sidlo="Zd. Fibicha 154/2022, 154 02 Litoměřice";
$ico="8413244777";
$dic="657617657-577";

?>

```

```php
<?
/* >>> db.php <<< */

///************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//***********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//************************************************************

//***************************************
// Nastavení databáze a připojování atd.
//***************************************

function pripoj_se_k_databazi() {

    $db_host="localhost";   // z bezpečnostních důvodů definováno uvnitř fce
    $uzivatel="tomas";
    //$db=strtolower($GLOBALS['firma']);
    //$db="testshop";
    $db="xinerama";
    $db_heslo="hezkeheslo";

    $GLOBALS['db_tmp']=mysql_connect($db_host,$uzivatel,$db_heslo);
        if (!$GLOBALS['db_tmp']) {
            mysql_chyba("Chyba. Prosím zkuste obnovit stránku v prohlížeči.");
        }

        $dbaze_tmp=@mysql_select_db($db);
        if (!$dbaze_tmp) {
            mysql_chyba("Chyba. Omlouváme se, ale zřejmě nebude možné pokračovat. Zkuste přesto obnovit
        stránku v prohlížeči, možná budete mít štěstí.");
        }
}

// tahle fce se teoreticky nemusí volat, protože nepersistentní připojení
// k databázi končí během skriptu
function odpoj_se_od_databaze() {
    mysql_close($GLOBALS['db_tmp']);
}

?>
```



```php
<?

/* >>> dph.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ****************
//***********  implementace internetového obchodu  *************
//***************** @ Tomáš Psika, 2003-2004 *******************
//******************  (licence GNU/GPL) ************************
//************************************************************

//*************************************
//Globální proměnné týkající se sazeb DPH
//*************************************

$GLOBALS['snizena_sazba_dph']=0.05;
$GLOBALS['zakladni_sazba_dph']=0.22;

?>
```

```php
<?
/* >>> pausaly.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//**********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 ******************
//******************  (licence GNU/GPL) ***********************
//************************************************************

//*************************************************
//   Proměnné týkající se paušálních poplatků
//    za poštovné, manipulační poplatky apod.
//*************************************************

$manipulacni_poplatek=50;
$postovne=40;

?>
```



```php
<?
/* >>> podnikove_udaje.php <<< */

//************************************************************
//*************** Projekt UJEPFSE_DPL_TESTSHOP ***************
//**********  implementace internetového obchodu  ************
//***************** @ Tomáš Psika, 2003-2004 ******************
//******************  (licence GNU/GPL) ***********************
//************************************************************

//*************************************************
//              Podnikové údaje
//*************************************************

// globální proměnné

$nazev_podniku="Xinerama, s.r.o.";
$sidlo="Zd. Fibicha 154/2022, 154 02 Litoměřice";
$ico="8413244777";
$dic="657617657-577";

?>
```

Příloha č. 2

Struktura databázové části implementace obchodu

```sql
# phpMyAdmin SQL Dump
# version 2.5.2-rc1
# http://www.phpmyadmin.net
#
# Počítač: localhost
# Vygenerováno: Úterý 02. března 2004, 20:39
# Verze MySQL: 4.0.15
# Verze PHP: 4.3.3
#
# Databáze : `xinerama`
#

# --------------------------------------------------------

#
# Struktura tabulky `data`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:30
#

DROP TABLE IF EXISTS `data`;
CREATE TABLE `data` (
  `data` char(20) NOT NULL default '',
  `kolik` int(11) NOT NULL default '0',
  PRIMARY KEY  (`data`)
) TYPE=MyISAM;

#
# Vypisuji data pro tabulku `data`
#

INSERT INTO `data` VALUES ('posledni_pristup', 0);
INSERT INTO `data` VALUES ('server_on', 1);

# --------------------------------------------------------

#
# Struktura tabulky `kosiky`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:29
#

DROP TABLE IF EXISTS `kosiky`;
CREATE TABLE `kosiky` (
  `kod` int(11) NOT NULL auto_increment,
  `uzivatel` varchar(30) NOT NULL default '',
  `ident` int(11) NOT NULL default '0',
  `pocet` int(11) NOT NULL default '0',
  PRIMARY KEY  (`kod`),
  UNIQUE KEY `ident` (`ident`)
) TYPE=MyISAM AUTO_INCREMENT=25 ;

#
# Vypisuji data pro tabulku `kosiky`
#


# --------------------------------------------------------

#
# Struktura tabulky `objednavky`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:31
#

DROP TABLE IF EXISTS `objednavky`;
CREATE TABLE `objednavky` (
  `uzivatel` varchar(30) NOT NULL default '',
```



```sql
  `data` text NOT NULL,
  `stav` tinyint(1) NOT NULL default '0',
  PRIMARY KEY  (`uzivatel`,`stav`)
) TYPE=MyISAM;

#
# Vypisuji data pro tabulku `objednavky`
#


# --------------------------------------------------------

#
# Struktura tabulky `pocitadla`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:31
#

DROP TABLE IF EXISTS `pocitadla`;
CREATE TABLE `pocitadla` (
  `co` char(16) NOT NULL default '',
  `kolik` int(11) NOT NULL default '0',
  PRIMARY KEY  (`co`)
) TYPE=MyISAM;

#
# Vypisuji data pro tabulku `pocitadla`
#

INSERT INTO `pocitadla` VALUES ('pristupy', 0);
INSERT INTO `pocitadla` VALUES ('pristupy_dnes', 0);
INSERT INTO `pocitadla` VALUES ('prihlaseni', 0);
INSERT INTO `pocitadla` VALUES ('prihlaseni_dnes', 0);

# --------------------------------------------------------

#
# Struktura tabulky `skupiny`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:29
#

DROP TABLE IF EXISTS `skupiny`;
CREATE TABLE `skupiny` (
  `gid` smallint(6) NOT NULL auto_increment,
  `nazev` varchar(40) NOT NULL default '',
  `ngid` smallint(6) NOT NULL default '0',
  PRIMARY KEY  (`gid`)
) TYPE=MyISAM AUTO_INCREMENT=4 ;

#
# Vypisuji data pro tabulku `skupiny`
#

INSERT INTO `skupiny` VALUES (1, 'Knihy', 0);
INSERT INTO `skupiny` VALUES (2, 'CD', 0);
INSERT INTO `skupiny` VALUES (3, 'DVD', 0);

# --------------------------------------------------------

#
# Struktura tabulky `stranky`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:35
#

DROP TABLE IF EXISTS `stranky`;
CREATE TABLE `stranky` (
```

```
  `id` smallint(6) NOT NULL auto_increment,
  `param` varchar(10) NOT NULL default '',
  `titulek` varchar(35) NOT NULL default '',
  `skript` varchar(35) NOT NULL default '',
  `pocitadlo` int(11) NOT NULL default '0',
  PRIMARY KEY  (`id`)
) TYPE=MyISAM AUTO_INCREMENT=11 ;

#
# Vypisuji data pro tabulku `stranky`
#

INSERT INTO `stranky` VALUES (1, 'uvodni_str', 'Vítejte v obchodě firmy Xinerama',
'uvodni_stranka.php', 0);
INSERT INTO `stranky` VALUES (2, 'o_podniku', 'Informace o podniku', 'o_podniku.php', 0);
INSERT INTO `stranky` VALUES (3, 'katalog', 'Výrobkový katalog', 'katalog_vyrobku.php', 0);
INSERT INTO `stranky` VALUES (4, 'nak_kosik', 'Nákupní košík', 'nakupni_kosik.php', 0);
INSERT INTO `stranky` VALUES (5, 'registrace', 'Registrace zákazníka', 'registrace.php', 0);
INSERT INTO `stranky` VALUES (6, 'prihlaseni', 'Přihlášení zákazníka', 'prihlaseni.php', 0);
INSERT INTO `stranky` VALUES (7, 'kontakt', 'Firemní kontakty a reference', 'kontakt.php', 0);
INSERT INTO `stranky` VALUES (9, 'objednavka', 'Objednávka', 'objednavka.php', 0);
INSERT INTO `stranky` VALUES (8, 'odhlaseni', 'Odhlášení uživatele', 'odhlaseni.php', 0);
INSERT INTO `stranky` VALUES (10, 'admin_ace', 'Administrace obchodu', 'admin_ace.php', 0);

# --------------------------------------------------------

#
# Struktura tabulky `uzivatele`
#
# Vytvoření: Úterý 02. března 2004, 20:33
# Poslední změna: Úterý 02. března 2004, 20:33
#

DROP TABLE IF EXISTS `uzivatele`;
CREATE TABLE `uzivatele` (
  `sid` char(32) NOT NULL default '',
  `uzivatel` char(20) NOT NULL default '',
  `jmeno` char(20) NOT NULL default '',
  `prijmeni` char(20) NOT NULL default '',
  `heslo` char(32) NOT NULL default '',
  `predesly_pristup` int(11) NOT NULL default '0',
  `pocitadlo` mediumint(9) NOT NULL default '0',
  `email` char(50) NOT NULL default '',
  `adresa` char(100) NOT NULL default '',
  `mesto` char(30) NOT NULL default '',
  `telefon` char(100) NOT NULL default '',
  `datum_registrace` char(10) NOT NULL default '0',
  `kod` char(1) NOT NULL default '',
  PRIMARY KEY  (`sid`,`uzivatel`)
) TYPE=MyISAM;

#
# Vypisuji data pro tabulku `uzivatele`
#



# --------------------------------------------------------

#
# Struktura tabulky `vyrobky`
#
# Vytvoření: Úterý 02. března 2004, 20:29
# Poslední změna: Úterý 02. března 2004, 20:29
#

DROP TABLE IF EXISTS `vyrobky`;
CREATE TABLE `vyrobky` (
  `id` smallint(6) NOT NULL auto_increment,
  `nazev` varchar(50) NOT NULL default '',
  `gid` tinyint(4) NOT NULL default '0',
  `cena` float NOT NULL default '0',
```



```
  `dph` tinyint(1) NOT NULL default '2',
  `popis` text NOT NULL,
  `obrazek` varchar(50) NOT NULL default '',
  `sklad` tinyint(1) NOT NULL default '1',
  `rel` tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (`id`,`nazev`)
) TYPE=MyISAM AUTO_INCREMENT=2 ;

#
# Vypisuji data pro tabulku `vyrobky`
#

INSERT INTO `vyrobky` VALUES (1, 'PHP a MySQL rozvoj webových aplikací', 1, '455', 2, 'Autor: Luke
Welling, Laura Thomson\n\nKniha seznamuje čtenáře se základními aspekty tvoření moderních dynamických
webových aplikací, internetových obchodů apod.', 'we_php_a_mysql_rozvoj_webovych_aplikaci.png', 1, 1);

```

```sql
# SQL skript pro vytvoření databáze a práv nového uživatele 'tomas'

# odstranění uživatele 'tomas'
REVOKE ALL PRIVILEGES ON * . * FROM "tomas"@"%";
DELETE FROM `user` WHERE `User` = "tomas" AND `Host` = "%";

# vytvoření uživatele
GRANT USAGE ON * . * TO "tomas"@"localhost"IDENTIFIED BY "hezkeheslo"WITH MAX_QUERIES_PER_HOUR 0
MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 ;

# vytvoření databáze
CREATE DATABASE `xinerama`;

# přidělení práv novému uživateli k této databázi
REVOKE ALL PRIVILEGES ON `xinerama` . * FROM "tomas"@"localhost";
REVOKE GRANT OPTION ON `xinerama` . * FROM "tomas"@"localhost";

GRANT SELECT ,
INSERT ,
UPDATE ,
DELETE ,
CREATE ,
DROP ,
INDEX ,
ALTER ,
CREATE TEMPORARY TABLES ON `xinerama` . * TO "tomas"@"localhost";
```

Příloha č. 3

Ostatní soubory nutné pro funkčnost implementace obchodu

styl.css Příloha č.3

```css
body {
    font-family:sans-serif; font-size:12px;
    color:#000000;
    margin-top:20pt; margin-right:10pt; margin-bottom:20pt;  margin-left:10pt;
    scrollbar-face-color: #151515; scrollbar-highlight-color: #000000;
    scrollbar-shadow-color: #e08c44; scrollbar-3dlight-color: #000000; scrollbar-arrow-color: #00a24a;
    scrollbar-track-color: #202020;scrollbar-darkshadow-color: #e08c44
}

h3 {
    font-family:sans-serif; font-size:15px; font-weight:bold
}

.hlavni_tabulka {
    font-size:14px;
    border-style:solid; border-color: black; border-width: 2px
}

.nadpis {
    font-size:15px; font-weight:bold
}
.pocet_input {
    width: 30px
}
.mnozstvi_zvyraz {
    border: 2px red dashed
}
.skupiny {
    font-size:12px; font-family:sans-serif;
    border-width:medium; border-style:groove;
    border-color: darkRed darkMagenta darkRed darkMagenta;
}
.vlastni_obsah {
    padding-left:35px; padding-right:35px; padding-top: 15px; padding-bottom: 0px;
text-align:justify
}
.zapati {
    background-image: url(grafika/zapati.jpg); background-color: #a4d6e6
}

```

service.js Příloha č.3

```javascript
/* Různé doplňkové javascriptové funkce */

// obsluha stavového řádku

function vratitstatus()
{
    window.status="Vítejte v obchodě firmy Xinerama";
    return true;
}

// preload obrázků loga

function preload_loga() {
    obr1=new Image();
    obr1.src="grafika/logo_ok_on_o_podniku.jpg";

    obr2=new Image();
    obr2.src="grafika/logo_ok_on_katalog_vyrobku.jpg";

    obr3=new Image();
    obr3.src="grafika/logo_ok_on_nakupni_kosik.jpg";

    obr4=new Image();
    obr4.src="grafika/logo_ok_on_registrace.jpg";

    obr5=new Image();
    obr5.src="grafika/logo_ok_on_prihlaseni.jpg";

    obr6=new Image();
    obr6.src="grafika/logo_ok_on_kontakt.jpg";
}

// OnMouseOver a OnMouseOut efekt u obrázků

function zamen(nazev_obr,novy_obr)
{
  document.images[nazev_obr].src=novy_obr;
}

```