

6 Bezpečnost online systémů a platebních systémů

- **Cíle výuky modulu**
- Popsat klíčové aspekty bezpečnosti e-commerce
- Identifikovat klíčové bezpečnostní hrozby v prostředí e-commerce.
- Popsat, jak technologie pomáhá chránit bezpečnost zpráv posílaných přes internet.
- Identifikovat nástroje používané k bezpečné komunikaci přes Internet, pro ochranu komunikačních kanálů a sítí, serverů a klientů.
- Diskutovat o významu politik, postupů a právních předpisů při tvorbě zabezpečení.
- Popsat vlastnosti tradičních platebních systémů.
- Vysvětlit hlavní platební mechanismy e-commerce.
- Popsat vlastnosti a funkce elektronické fakturace a platebních systémů.

Úvodní otázky k diskuzi

- Co je útok DDoS?
- Co jsou botnety? Proč se používají v DDoS útocích?
- Jaké procento počítačů patří botnetům? Jaké procento spamu je odesláno z botnetů?
- Může něco udělat pro zastavení DDoS útoky?



Obr. 1 – Ilustrace útoku DoS

Příklad ilustrující, jak jsou vytvořeny botnety a použity k odesílání nevyžádané pošty

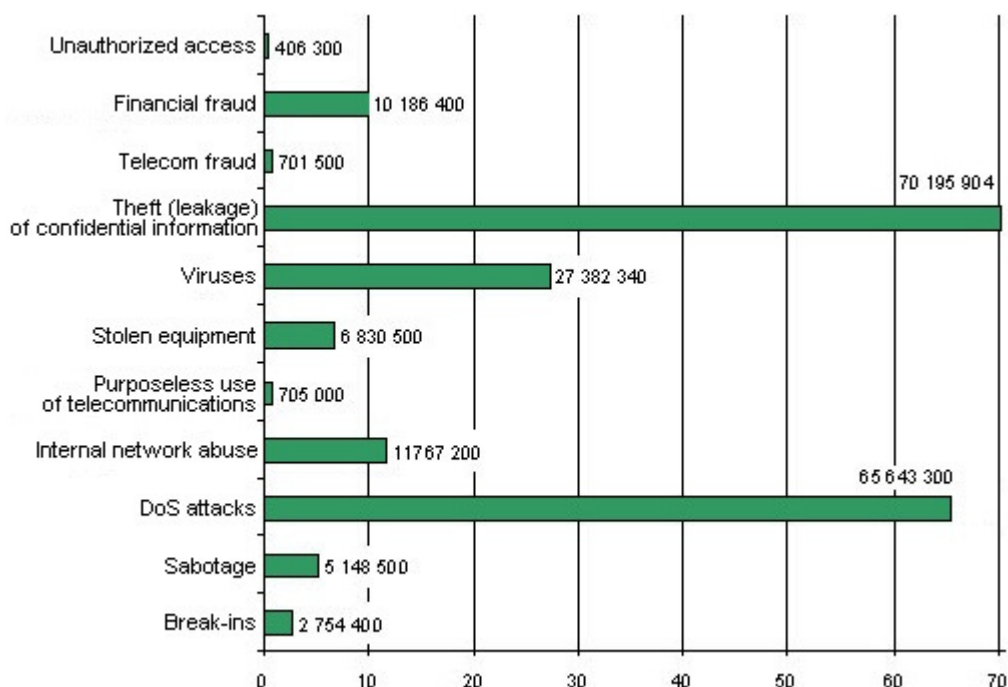
1. Botnet operátor posílá viry nebo červy, které infikují počítače běžných uživatelů
2. Bot na infikovaném počítači se uloží do části operačního systému command-and-control (C & C) server (často do IRC serveru, ale v některých případech na webový server). Pozn. IRC server (Internet Relay Chat server) – umožňuje komunikaci v reálném čase po internetu (chat).
3. Spammer nakoupí přístup k botnetům od operátora.
4. Spammer posílá instrukce prostřednictvím IRC serveru infikovaným počítačům, aby je přiměl rozesílat nevyžádanou poštu poštovním serverům.

Bezpečné prostředí e-commerce

Celková velikost a ztráty počítačové z kriminality nejsou úplně jasné, ne všechny firmy přiznávají, že byly terčem útoku.

Průzkum Computer Security Institute v roce 2008: 49% firem, které odpověděly na otázky, zaznamenalo porušení bezpečnosti v posledním roce. Průměrná ztráta byla 288.000 dolarů. Rozvíjí se Ilegální ekonomika. Ukradené informace jsou uloženy na serverech ilegální ekonomiky.

Typy útoků proti počítačovým systémům



Obr. 2 - Typy útoků proti počítačovým systémům

Ilegální ekonomika

Tab. 1 – položky ilegální ekonomiky

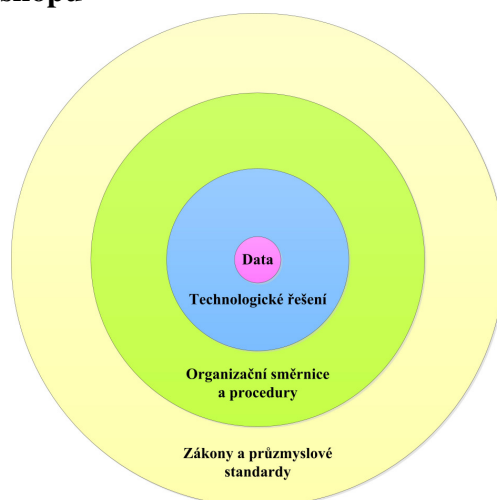
Overall Rank 2009 2008		Item	Percentage 2009 2008		Range of Prices
1	1	Credit card information	19%	32%	\$0.85-\$30
2	2	Bank account credentials	19%	19%	\$15-\$850
3	3	Email accounts	7%	5%	\$1-\$20
4	4	Email addresses	7%	5%	\$1.70/MB-\$15/MB
5	9	Shell scripts	6%	3%	\$2-\$5
6	6	Full identities	5%	4%	\$0.70-\$20
7	13	Credit card dumps	5%	2%	\$4-\$150
8	7	Mailers	4%	3%	\$4-\$10
9	8	Cash-out services	4%	3%	\$0-\$600 plus 50%-60%
10	12	Website administration credentials	4%	3%	\$2-\$30

Goods and services advertised on underground economy servers

Co znamená, že systém e-commerce je dobře zabezpečen?

- K dosažení nejvyššího stupně bezpečnosti je třeba:
 - Nové technologie
 - Organizační zásady a postupy
 - Průmyslové standardy a právních normy
 - Postupy vyplývající z best practice
- Další faktory
 - Časová hodnota peněz
 - Náklady na bezpečnost vs. případné ztráty
 - Bezpečnost je nutno posuzovat s ohledem na nejslabší článek

Bezpečnostní prostředí e-shopu



Pohled zákazníka a obchodníka na různé dimenze bezpečnosti e-commerce

Tab. 2 - Pohled zákazníka a obchodníka na různé dimenze bezpečnosti e-commerce

Dimenze	Pohled zákazníka	Pohled obchodníka
Integrita	Nebyla informace, kterou jsem odeslal nebo přijal změněna?	Nebyla data na webové stránce změněna bez autorizace?
Nepopření	Může druhá strana později popřít, že měla něco udělat?	Může zákazník popřít svoji objednávku?
Autentizace	S kým jednám? Jak si mohu být jistý, že to je ta osoba, za kterou se prohlašuje být	Jaká je reálná identita zákazníka?
Důvěrnost	Může někdo jiný než mnou označený příjemce číst mé zprávy?	Jsou zprávy nebo důvěrná data přístupné pro někoho jiného než je autorizovaná osoba?
Soukromí	Mohu kontrolovat užití informací o mě přenášené e-commerce obchodníkovi?	Jaký užitek může být z osobních dat uložených jako výsledek e-commerce transakce? Nejsou tato data využívány nedovoleným způsobem (porušení zákona o ochraně osobních údajů)
Dostupnost	Mohu přistupovat ke stránce?	Je webová stránka funkční?

Rozpor mezi bezpečností a jinými prvky e-commerce

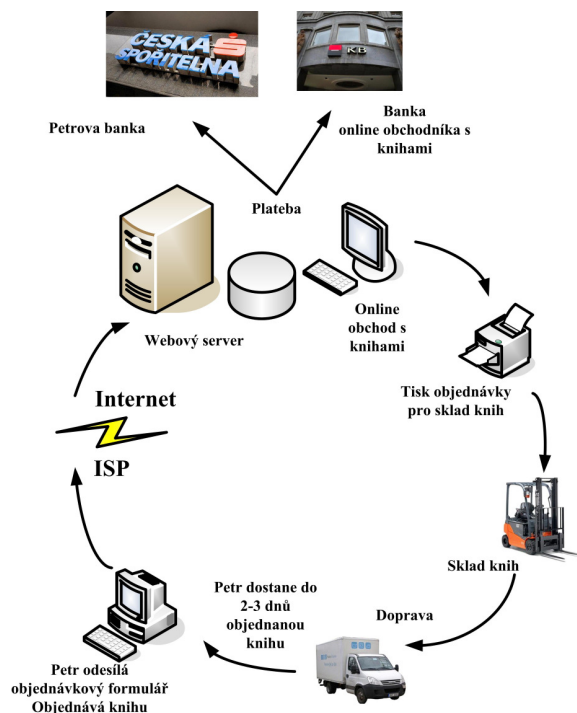
- Bezpečnost versus snadnost použití
 - Pokud je přidáno více bezpečnostních opatření, pak použití webové stránky může být obtížnější, případně pomalejší (potřeba složité autentizace apod.)
- Bezpečnost versus touha jednotlivců jednat anonymně

Bezpečnostní hrozby v prostředí e-commerce

Tři klíčové body zranitelnosti:

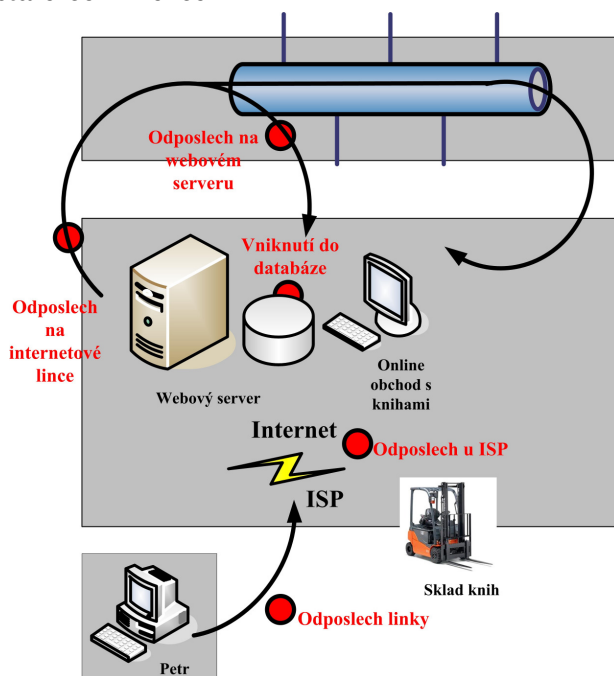
1. Klient
2. Server
3. Komunikační spoje

Typické transakce v e-commerce



Obr. 4 -Typické transakce v e-commerce

Možná zranitelná místa e-commerce



Obr. 5 - Zranitelná místa prostředí e-commerce

Bezpečnostní rizika (viz obrázek 3):

Tab. 3 - Bezpečnostní rizika

Oblast e-commerce	Bezpečnostní rizika
Komunikace přes internet	Odposlech Měnění zpráv Krádež a podvody
Vlastní prostředí e-commerce (ISP, obchodník, banky)	Útoky typu DoS Hacking Útok pomocí zlovolných kódů (malware) – viry, trojské koně, spyware Krádež a podvod Odposlech linek Vandalismus
Klient (obchodní partner, koncový uživatel)	Útok pomocí zlovolných kódů (malware) – viry, trojské koně, spyware Odposlech linek Fyzická ztráta nebo odcizení počítače

Nejčastější bezpečnostní hrozby v prostředí e-commerce

- Škodlivý kód
 - Viry
 - Červy
 - Trojské koně
 - Boty, bolety
- Nežádoucí programy
 - Parazitní programy prohlížeče
 - Adware
 - Spyware

Nejčastější bezpečnostní hrozby

- Phishing
 - Podvodný online pokus o získání důvěrných informací
 - Sociální inženýrství, podvody prováděné pomocí e-mailu, falšování legitimní webové stránky
 - Použití informací ke spáchání podvodného jednání (např. po získání přístupu k cizímu účtu), odcizení identity
- Hacking a cybervandalism

- Hackeři vs. crackers
- Cybervandalism: záměrně přerušení činnosti, znehodnocení, zničení webové stránky
- Druhy hackerů: white hats, black hats, grey hats (white hats – penetrační testování připojení na internet na objednávku, cíle je objevení chyb; black hat – nedovolené činnosti)

Nigerijský dopis – přijde vám e-mail, který tvrdí, že přes váš účet je třeba přeposlat miliony dolarů a že za to obdržíte několik procent z celé částky (dost peněz). Je jen potřeba sdělit informace o vašem účtu. Tyto podvodníci se zajímají o informace o vašem běžném účtu.

Nejčastější bezpečnostní hrozby (pokračování)

- • Podvod s kreditní kartou/krádeže
 - Strach z ukradení informací o kreditní kartě odrazuje od on-line nákupů
 - Hackeři se zaměřují na servery online obchodů, využívat data k získání úvěru pod falešnou identitou
 - Online společnosti v tomto smyslu jsou rizikovější než běžné offline kamenné obchody
- Umísťování falešného obsahu: zkreslování sebe sama pomocí falešných e-mailových adres
- Pharming: spoofing webu
 - Přesměrování odkazu z řádných webových stránek na nové falešné webové stránky
- Spam/nevyžádané webové stránky

Nejčastější bezpečnostní hrozby

- Odmítnutí služby (Denial of Services - DoS)
 - Hackeři zahltí webovou stránku neúčinnými zprávami
- Distribuované odepření služby (DDoS) útok
 - Hackeři používají více počítačů k útoku na cílové síť
- Odposlouchání
 - Odposlouchávací program, který monitoruje informace přicházející po síti
- Zaměstnanci
- Špatně navržený server a klientský software

Technologické řešení

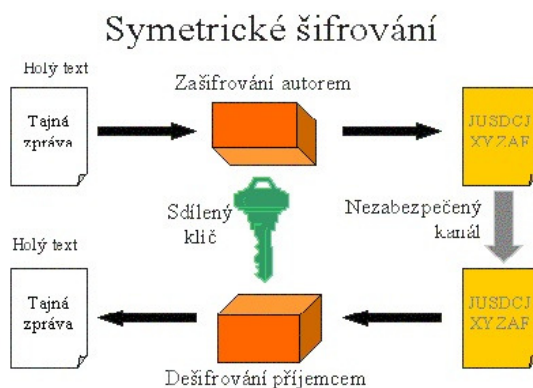
- Ochrana internetové komunikace (šifrování)
- Zabezpečení komunikačních kanálů (SSL, S-HTTP, VPN - tunelování)
- Ochrana sítě (firewall, IDS – intrusion detection systém – detekce průniku)
- Ochrana serverů a klientů (řízení přístupu, autentizace)

Šifrování

- Šifrování
- Transformace dat na šifrovaný text čitelný pouze odesílatelem a příjemcem
- Zabezpečuje uložené informace a přenos informací
- Poskytuje 4 z 6 klíčových dimenzí zabezpečení elektronického obchodování:
 1. Integritu zprávy
 2. Neodvolatelnost
 3. Ověření pravosti
 4. Důvěrnost

Symetrické šifrování

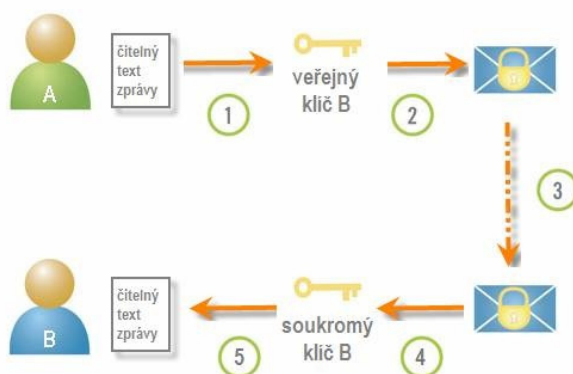
- Odesílatel a příjemce používají stejný digitální klíč pro šifrování a dešifrování zpráv
- Vyžaduje jinou sadu klíčů pro každou transakci
- Síla šifrování
 - Délka binárního klíče používaný k šifrování dat
- Advanced Encryption Standard (AES)
 - Nejvíce použitý typ symetrického šifrování
 - Používá 128 -, 192 - a 256-bitové šifrovací klíče
- Další standardy používají klíče až 2048 bitů



Obr. 5 – Symetrické šifrování

Šifrování s veřejným klíčem

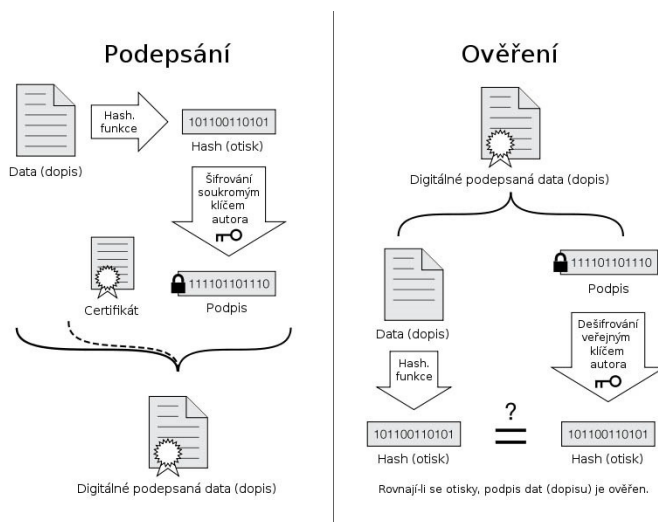
- Používá dvě matematicky související digitální klíče
 1. Veřejný klíč (šířený)
 2. Soukromý klíč (utajovaný vlastníkem)
- Oba klíče slouží k šifrování a dešifrování zpráv
- Klíčem, kterým zašifrujeme zprávu, nemůžeme tuto zprávu dešifrovat
- Odesílatel používá veřejný klíč příjemce k zašifrování zprávy. Příjemce používá svůj soukromý klíč k dešifrování této zprávy.



Obr. 6 – Asymetrické šifrování

Digitální podpis

- Hashovací funkce:
 - Matematický algoritmus, který produkuje číslo pevné délky, který nazýváme otisk (hash)
- Hash zprávy zašleme příjemci spolu se zprávou, Hash slouží k ověření integrity
- Odesílatel spočítá hash zprávy.
- Hash a šifrovanou zprávu zašifruje odesílatel veřejným klíčem příjemce
- Celý šifrovaný text i hash příjemce dešifruje soukromým klíčem
 - -vytváření digitálního podpisu-ověření pravosti, neodvolatelnost

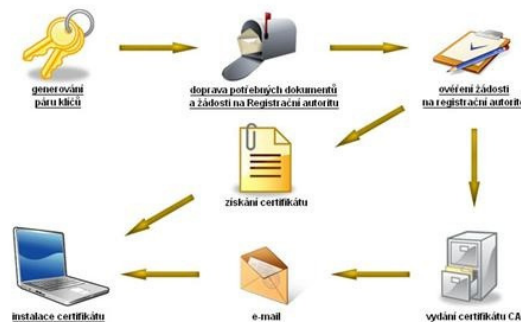


Obr. 7 – digitální podpis

Infrastruktura veřejného klíče (Public Key Infrastructure - PKI)

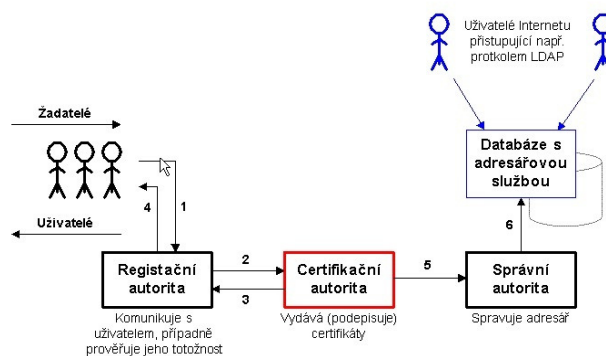
- Digitální certifikát obsahuje:
 - Název předmětu / firmy
 - Předmět veřejný klíč

- Digitální sériové číslo certifikátu
- Datum ukončení platnosti, datum vydání
 - Digitální podpis certifikační autority (důvěryhodná třetí strana), který vydává osvědčení
- Public Key Infrastructure (PKI):
 - CA (Certification Authority) a digitální certifikát, postupy, které jsou přijímány všemi stranami



Obr. 8 – princip PKI

Získání digitálního certifikátu



Obr. 9 - Získání digitálního certifikátu

Certifikační autorita

Certifikační autorita (zkratka CA) je v asymetrické kryptografii subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI (Public Key Infrastructure) tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na základě principu přenosu důvěry tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.

Na Internetu působí mnoho komerčních certifikačních autorit, které obvykle mají své veřejné klíče umístěny přímo ve webových prohlížečích a dalších programech, čímž mohou uživatelé zjednodušit rozhodování o míře důvěry webových serverů, ke kterým se připojuje (ale též digitálně podepsaných e-mailů i jiných dat). Existují též bezplatné certifikační autority nebo takové, které se řídí zákony daného státu, vnitřními předpisy organizace a podobně. Majitel veřejného klíče musí proto při žádosti o vydání digitálního certifikátu důvěryhodným způsobem certifikační autoritu přesvědčit, že jím poskytnuté údaje odpovídají skutečnosti a tomu, co uvedl ve svém veřejném klíči. Může tak například učinit:

- Fyzická osoba - přeložením občanského průkazu zástupci certifikační autority.
- Právnická osoba - předložením ověřeného výpisu z obchodního rejstříku,

Po ověření a porovnání výše uvedených údajů vydá certifikační autorita digitální certifikát, který ověřené údaje obsahuje. Důležitou součástí digitálního certifikátu je elektronický podpis, kterým lze snadno ověřit jeho autentičnost. Pokud by byly údaje v digitálním certifikátu změněny, kryptografické ověření digitálního podpisu by změnu odhalilo.

Meze šifrovací řešení

- Je třeba uchovávat v tajnosti soukromý klíč
 - PKI může být kompromitován zaměstnanci, osobami, které se podílejí na chodu PKI
- Není zaručeno, že ověřený počítač obchodníka je bezpečný
- CA mohou být neregulované, samy se vydávají za autority

Zabezpečení komunikačních kanálů

- Secure Sockets Layer (SSL):
 - Zřizuje bezpečnou dohodnutou komunikaci klient-server
- HTTPS:
 - Poskytuje - komunikace orientovanou na zabezpečené zprávy. Je to protokol navržený pro použití ve spojení s http
- Virtuální privátní síť (VPN):
 - Umožňuje vzdáleným uživatelům bezpečně přistupovat k vnitřní síti přes Internet pomocí Point-to-Point Tunneling Protocol (PPTP)

Komunikace SSL

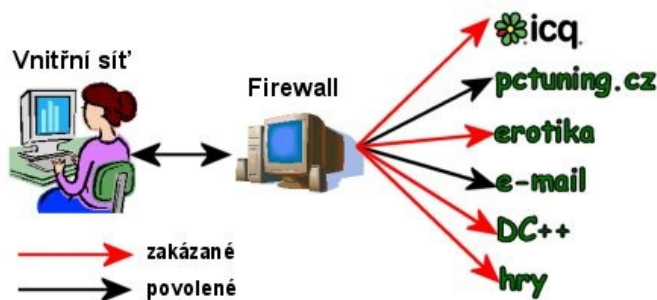
Komunikace SSL probíhá následovně:

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informace a hlavně certifikátu serveru.
3. Podle přijatého certifikátu si klient ověří autentifikaci serveru. Certifikát také obsahuje veřejný klíč serveru.

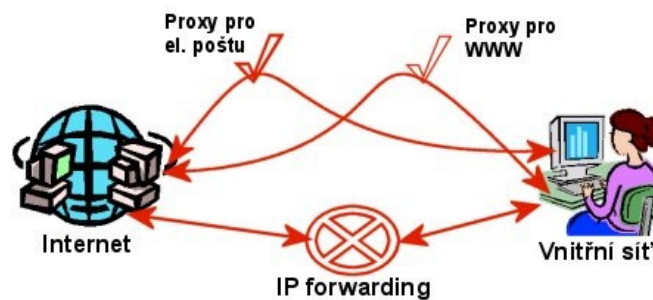
4. Na základě doposud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak i server, tak i klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tím končí.
7. Je dohodnuté zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od teď komunikují přes šifrované spojení. Po dobu první fáze ustanovení bezpečného spojení si klient a server dohodnou kryptografické algoritmy, které budou používat pro výměnu klíčů.

Ochrana sítě

- Firewall
 - Hardware nebo software, který filtruje pakety
 - Zabraňuje, aby se některé pakety nedostaly do sítě na základě bezpečnostní politiky
 - Dvě hlavní metody:
 1. Paketové filtry
 2. Aplikační brány
- Proxy servery (proxy)
 - Software servery, které zajišťuje veškerou komunikaci pocházející z internetu nebo je posílána do internetu



Obr. 10 – Princip firewallu



Obr. 11 – Princip proxy serveru

Ochrana serverů a klientů

- Vylepšení bezpečnosti operačního systém
 - Aktualizace, opravy
- Anti-virus software
 - Nejjednodušší a nejlevnější způsob, jak zabránit ohrožení integrity systému
 - Vyžaduje denní aktualizací

Bezpečnostní politiky, obchodní procesy a veřejné zákony

- US firmy a organizace utratí 12% IT rozpočtu na zabezpečení hardware, software, služby 120 mld. USD v roce 2009)
- Řízení rizik zahrnuje
 - Technologie
 - Efektivní bezpečnostní politiky
 - Veřejné zákony a jejich aktivní prosazování

Bezpečnostní plán: bezpečnostní politiky

- Hodnocení rizik
- Bezpečnostní politika
- Plán implementace bezpečnostních opatření
 - Bezpečnost organizace
 - Kontrola přístupu
 - Ověřovací procedury, včetně biometrických údajů
 - Autorizační politiky, řídicí systém pro autorizaci
- Bezpečnostní audit

V ideálním případě firma zavede systém řízení bezpečnosti informací dle ISO/IEC 27001.

Systém řízení bezpečnosti informací (Information Security Management System - ISMS) je dokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. Pojem primárně zavedla

norma ISO/IEC 17799 (mezinárodní norma převzatá z Britského standardu BS 7799-1:1999), publikovaná Mezinárodní organizací pro normalizaci (ISO) v roce 2000. Novější revidovaná verze je součástí nové řady norem týkající se bezpečnosti informací ISO 27000.

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována.

ISMS může být zaveden pro organizační složku společnosti, informační systém nebo jeho část, případně může zahrnovat celou organizaci. Zavedení systému řízení bezpečnosti informací (ISMS) je strategickým rozhodnutím vedení společnosti. Tento systém začínají hojně využívat všechny organizace bez ohledu na velikost či obor činnosti, pro které jsou informace a informační technologie klíčovou součástí podnikatelských procesů, nebo které spravují citlivá data svých klientů a mají potřebu efektivně a komplexně zajistit jejich bezpečnost.



Obr. 12 – Životní cyklus ISMS

Platební systémy

Druhy platebních systémů

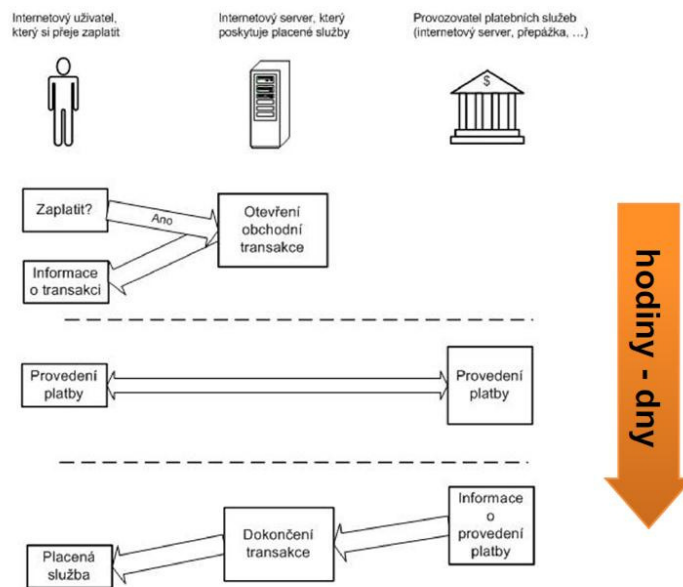
- Hotovost
 - Nejčastější formou platby, pokud jde o počet transakcí
 - Okamžitě převoditelné na jiné formy hodnot bez zprostředkování
- Platební karta
 - Platební karty asociací (VISA, Master Card)
 - - Vydávající banky
 - - Zpracovatelská centra

Typy platebních systémů (platí pro Českou republiku)

- Klasické offline metody (dobírka, převodem)
- Online platba kartou (Platební karty asociací - VISA, Master Card)
- Platební tlačítka různých bank

- Mikroplatby (nejvíce jsou využívány služby elektronické peněženky)
- Mobilní platby (m-platby)
- Online uzavření splátky
- Platba na terminálech Sazka
- Zahraniční platební systémy (PayPal)

Klasické offline metody (dobírka, převodem)



Obr. 13 – Princip off-line platebních metod (ET NETERA a.s.)

Dobírka

Česká pošta, PPL, DPL, vlastní dovoz, ..

Stále nejpobulárnější platební metoda

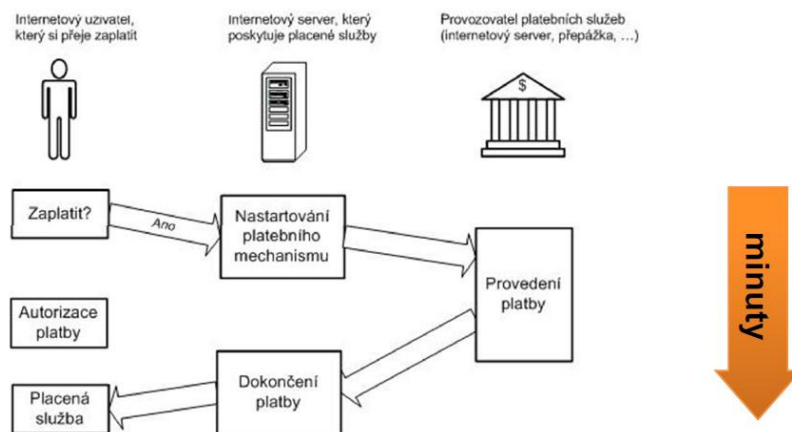
- Dle našich statistik až 70% transakcí, APEK uvádí 80%
- Náklady typicky 50 – 100 Kč, lze je ale přenést na zákazníka
- Lidé dobírce věří, platí až za doručení

Platba převodem

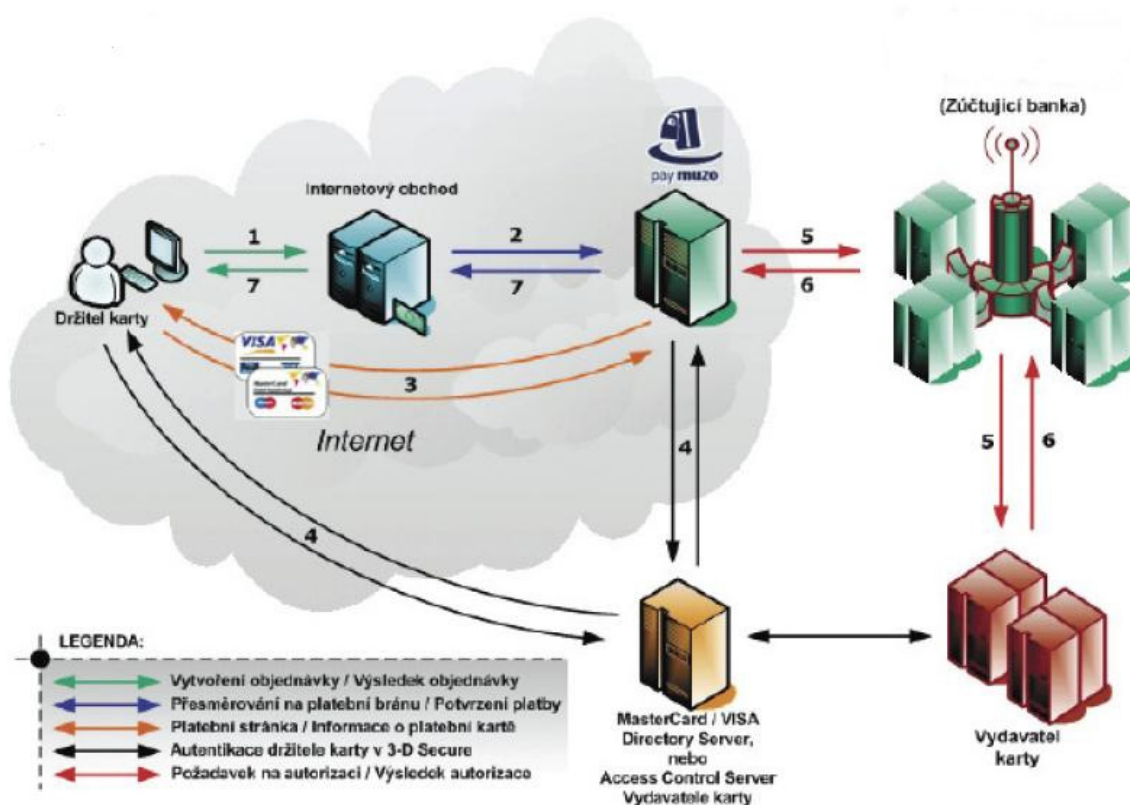
- Druhá nejpobulárnější metoda s cca. 15% podílem
- Elektronický obchod uživateli sdělí číslo účtu a variabilní symbol, zákazník pošle peníze převodem z účtu nebo jiným způsobem
- Výhoda je: nulové náklady pro obchodníka, malé pro nakupujícího
- Problém: zákazník má šanci si nákup rozmyslet, nenakupuje IHNE

- Většinou se čeká s expedicí objednaného zboží, až jsou peníze na účtu obchodníka – to je určitá komplikace, čekání

Online platební metody



Obr. 14 – Princip on-line platebních metod (ET NETERA a.s.)



Obr. 15 – Princip platby kartou na internetu (PayMUZO)

Platba kartou

V ČR provozuje:

- PayMUZO (www.globalpaymentsinc.com)
- Česká Spořitelna (http://www.csas.cz/banka/content/inet/internet/cs/sc_1585.xml), jiné banky

Z pohledu obchodníka

- Vysoké transakční náklady – typicky 1,5-4%
- Peníze nejsou na účtu ihned, online je jen potvrzení transakce

Z pohledu zákazníka

- Strach ze zneužití (byť v případě 3D Secure neoprávněný)
- Problematika karet s blokováním nákupem na internetu

Platební tlačítka

Princip:

- Po implementaci do webové stránky elektronického obchodu mají možnost zákazníci přímo a jednoduše platit za objednané služby/zboží z jejich účtu v dané bance většinou prostřednictvím stávajících služeb elektronického bankovníctví dané banky.
- Zákazník musí mít účet u určité banky, jejíž platební tlačítko je implementováno do webové stránky elektronického obchodu.
- Zákazník je po jednoduchém kliknutí na interaktivní ikonu (platební tlačítko) reprezentující dané funkcionality služby okamžitě přesměrován na webové stránky elektronického bankovníctví dané banky. Zde si zákazník zvolí svou službu pro zaplacení částky a po standardním bezpečnostním postupu přihlášení již jednoduše zrealizuje svou platbu.
- Platbu dokončí a vrací se do elektronického obchodu

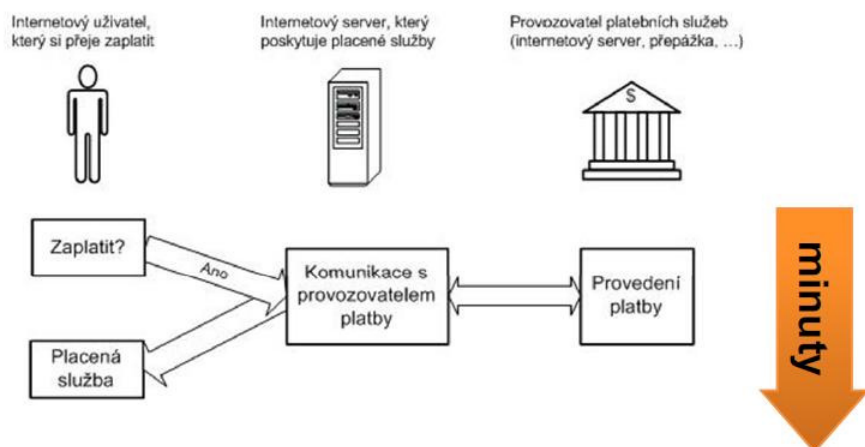
Výhody:

- Nižší transakční náklady (1%) – odpadá karetní asociace
- Rychlý převod peněz

Nevýhody:

- Některé banky vyžadují zřízení účtu
- Prozatím málo používané uživateli (jednotky procent)
- Problémy s přihlášením do online bankovníctví - certifikáty

Mikroplatby



Obr. 16 – Princip on-line platebních metod (ET NETERA a.s.)

Princip

- Uživatel má účet na internetu dobíjený jiným způsobem (elektronická peněženka)
- Vhodné spíše pro menší platby v řádech stokorun

Elektronická peněženka

Elektronická peněženka je určena pro mikroplatby i makroplatby a funguje vlastně podobně jako bankovní účet, ovšem jde o on-line elektronický platební systém a platební transakce jsou tedy neporovnatelně rychlejší a obvykle i výrazně levnější. Jako nejznámější elektronické peněženky, z nichž všechny jsou k dispozici i v české lokalizaci, je možné uvést celosvětově známý a velmi oblíbený PayPal, dále pak Moneybookers, GoPay, PayPay či česká PaySec od ČSOB, mPeníze od mBank. Pro fungování elektronických peněženek v České republice byl zcela přelomový rok 2002, který přinesl platnost nového zákona č. 124/2002 Sb., jež stanovil, že platební systémy a tedy i elektronické peněženky smí provozovat v České republice pouze držitelé bankovní licence, což se poté stalo důvodem zániku některých elektronických peněženek u nás.

Na elektronickou peněženku je možno převést finanční prostředky z jiné elektronické peněženky, dále převodem peněz z bankovního účtu (a to na stanovený bankovní účet pod variabilním symbolem identifikující konkrétní elektronickou peněženku), či platební kartou přes platební bránu. Peníze z elektronické peněženky je potom možno odeslat na jinou elektronickou peněženku či bankovní účet. Z účtu elektronické peněženky lze platit na platební bráně přesměrované při objednávce přímo ze stránek internetových obchodů, dále je umožněno účet elektronické peněženky ovládat přes webové rozhraní služby či u některých poskytovatelů elektronických peněženek (např. PayPal či PayPay) i pomocí příkazů v SMS zprávách, či pomocí e-mailu. Některé elektronické peněženky nabízejí dokonce možnost napojení na bankovní účet zákazníka a strhávání požadované částky přímo z jeho bankovního účtu. Příkladem budiž elektronická peněženka PayPal, která umožňuje napojit účet

elektronické peněženky na platební kartu zákazníka a při platbě částku strhnout z jeho platební karty, resp. bankovního účtu.

Nízké poplatky i možnost realizovat makroplatby tedy tuto platební metodu umožňuje využít nejen pro placení v rámci vztahu B2C, ale i B2B.

Pro a proti systému Elektronické peněženky:

Pro hovoří nulové či velmi nízké poplatky pro obchodníka za přijímání plateb elektronickou peněženkou a v podstatě neomezený platební rozsah.

Proti použití hovoří vyšší požadavky na kapacitu datového přenosu. Tento argument však také v poslední době mizí.

(<http://www.internetprovsechny.cz/clanek.php?cid=228>)

Příklad:

PaySec (<https://www.paysec.cz/>)

- Uvádí přes 15 tisíc aktivních klientů
 - Platby mezi uživateli využívá 20% klientů
 - Průměrná platba u obchodníka se pohybuje kolem 350 Kč
 - Týdenní obrat systému je 1,5 mil. Kč
 - Platby 200-500kč, primárně jízdenky apod.
- Penženka i platba je anonymní (do 25tis Kč)
- Nulové transakční náklady pro uživatele
- Řada problémů se spuštěním (bezpečnost, propagace, ...)

GoPay (<https://www.gopay.cz/>)

Platební terminály Sazka.cz

(Manum SuperCASH)

SuperCASH je nový platební kanál, který slouží ke zprostředkování hotovostních plateb mezi obchodníkem a zákazníkem jeho internetového obchodu. Využívá síť terminálů společnosti SAZKA, a.s. Je dostupný na mnoha místech v ČR i 24 hodin denně.

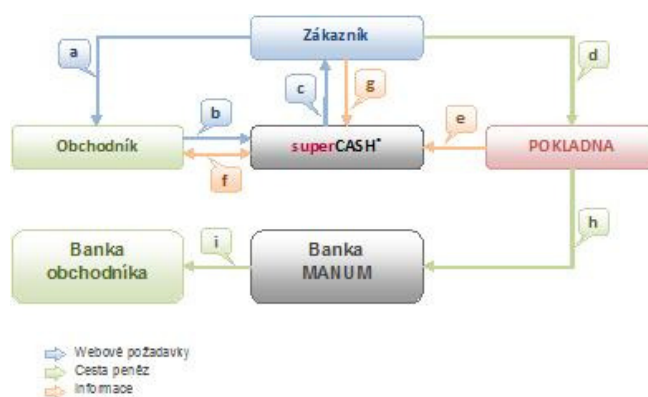
Výhody služby superCASH

- Rychlost. Informace o provedené úhradě je zasílána do 10 minut.
- Dostupnost. Přes 7000 platebních míst dostupných i o víkendech a 24/7
- Bezpečnost. Veškeré přenosy šifrovány.
- Anonymita. Zákazník nikde nezadává svá osobní data.
- Cena. Nižší náklady na zprostředkování platby než je na trhu obvyklé.
- Jednoduchost. Jednoduchá implementace do stávajícího systému obchodníka.

Další

- Zcela anonymní platba do 99.999,- Kč
- Poplatek platí zákazník – 10kč
- Vhodné pro platby nad 100kč
- Do budoucna pravděpodobně nebudou terminály sazka jediným vstupem

Technické řešení služby superCASH



Obr. 17 – Princip metody

1. Obchodník nabízí zákazníkovi zboží. Zákazník přejde do nákupního košíku a zvolí Platba superCASH.
2. Zákazník je přesměrován na zabezpečené webové rozhraní systému superCASH.
3. Potvrzením obchodních podmínek superCASH získá zákazník informace potřebné k úhradě platby.
4. Zákazník si vybere vhodný typ a místo platby. Pokud se zákazník rozhodne platit přes terminál SAZKA, a.s., má na výběr z několika způsobů identifikace platby: Vytiskne si vygenerovaný čárový kód, který zpracuje obsluha terminálu. Sdělí obsluze numerickou hodnotu pod čárovým kódem (toto číslo si může nechat zaslat na mobilní telefon).
5. Systém SAZKA, a.s., do 10 minut od složení hotovosti, zašle zabezpečenou a šifrovanou informaci o úhradě do systému superCASH.
6. Systém superCASH neprodleně po obdržení informace o úhradě zašle zabezpečenou elektronickou cestou avízo obchodníkovi (datový soubor, email, SMS) a aktualizuje přístupná rozhraní, kde si může obchodník kdykoli zjistit stav pohledávek.
7. Dle stanovené smluvní lhůty generuje systém superCASH podklady pro přehled plateb, poplatků a stavu úhrad pro každého obchodníka. Podklady jsou pravidelně zasílány písemně či elektronicky. Tyto doklady obchodník zkontroluje, potvrdí jejich správnost a úplnost a zašle je zpět společnosti MANUM, s.r.o. Zákazník má kdykoli v průběhu celého procesu možnost kontrolovat stav své platby pomocí webového rozhraní systému superCASH.
8. Společnost MANUM, s.r.o. provede převod plateb na účet obchodníka ponížený o smluvní poplatky neprodleně po připsání finančních prostředků společností SAZKA, a.s. na účet MANUM, s.r.o.

Platby mobilem

M-platby - mobilní platby, umožňují zaplatit bezhotovostní a elektronickou cestou pomocí mobilního zařízení menší finanční částky, obvykle maximálně v rámci stovek korun českých, proto jsou také označovány i jako mikroplatby. V České republice existuje více řešení mobilních plateb, avšak většinou se jedná o systémy, které jsou k dispozici pouze v rámci mobilní sítě každého operátora zvlášť (např. M-platby od operátora T-Mobile jsou vázány na

zákazníky této sítě, stejně tak jako M-platby od Vodafone). Univerzálněji uplatnitelné ve většině mobilních sítí jsou pak v České republice hojně využívané tzv. prémiové SMS zprávy (označované též jako Premium SMS), tedy speciální SMS zprávy s vyšší tarifací od operátora, pomocí kterých je možné platit za výrobky či služby, a to obvykle v rozsahu 3-99 Kč. Prémiové SMS podporují v České republice všichni operátoři (tedy T-Mobile, Telefónica O2, Vodafone a od června 2010 i U:fon).

Tab. 4 – Přehled mobilních plateb

Metoda	Operátor	Limity (v Kč)	Poznámka
Premium SMS	Všichni	Max 99,-	Obchodník dostane typicky cca 30%
M-platby	T-Mobile	Max 700,-	Vysoká provize (desítky procent)
M-peněženka	Vodafone	Max 600,-	

Online splátka

Princip

Z e-shopu je zákazník přeměřován na rozhraní poskytovatele úvěru. Zde vyplní online žádost a dostane jednu z odpovědí:

- Úvěr povolen (minimum)
- Úvěr zamítnut
- Úvěr ve schvalování

Následně probíhá telefonní a jiná komunikace, podpis smlouvy. Po podpisu smlouvy sdělí poskytovatel úvěru výsledek elektronickému obchodu.

Poskytovatelé online úvěrů

Např. Cetelem (AURA Karta) nebo GE MoneyBank

Výhody:

- Nulové náklady pro obchodníka (zpravidla)
- U části sortimentu vyžadováno zákazníky (elektronika, ...)

Nevýhody:

- Nárůst administrativy
- Nárůst komunikace

Zahraniční platební metody

PayPall

- Jednoduchá implementace
- Automaticky lze platit i VISA/MasterCard kartou
- Poměrně vysoké poplatky

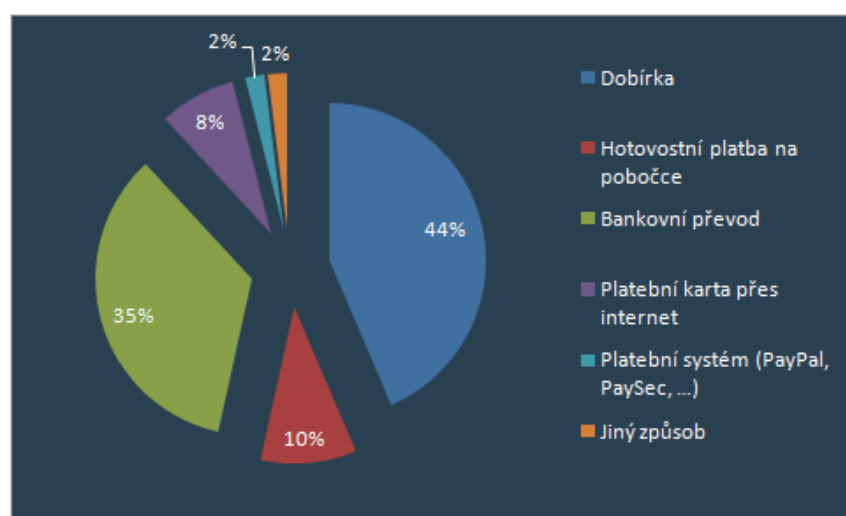
Jiné systémy

Peer-to-peer platební systémy (PaySec - není určen jen pro nákup u obchodníků, ale umožňuje okamžitý převod peněz mezi jeho uživateli (tzv. platby peer-to-peer))

A nakonec statistika:

Jak zákazníci v e-shopech nejčastěji nákup platí?

Z průzkumu vyplynulo, že i nadále je nejoblíbenějším způsobem úhrady zboží podle očekávání dobírka, kterou si vybírá nejvýznamnější část spotřebitelů (44%). Zároveň se ale potvrdilo, že zákazníci již běžně využívají i ostatní druhy plateb nabízených na trhu a hradí své nákupy také bankovním převodem (35%), kartou (8%) či prostřednictvím platebních systémů (2%). Zbývající část (10%) pak využívá internetu především k objednání zboží, které si pak osobně vyzvedne a uhradí v prodejnách e-obchodů.



Zdroj: APEK, Mediaresearch

Obr. 18 - Jaký je nejčastější způsob úhrady nákupu po internetu v ČR?