10 BEZPEČNOST E-BUSINESS

RYCHLÝ NÁHLED KAPITOLY

Elektronické podnikání a obchodování je závislé na informačních a komunikačních technologiích a zejména Internetu. Internet vytváří komunikační prostředí, které nabízí pro prodejce a zákazníky celou řadu užitečných možností, které ovšem přinášejí užitek za předpokladu, že jsou v rámci jeho využívání dodržována jistá pravidla vycházející zejména z oblasti zabezpečení počítačových sítí a zásad chování uživatelů v „otevřeném" prostředí Internetu. Nedodržení pravidel může v konečném důsledku vést nikoliv k bezproblémovému nákupu, ale ke ztrátě nejen finanční, ale i například újmě v oblasti osobní roviny. Cílem této kapitoly je prezentovat vybrané oblasti počítačové bezpečnosti z hlediska chování uživatelů a detailně popsat princip elektronického resp. digitálního podpisu jakožto prostředku pro identifikaci zákazníka v internetových obchodech.

CÍLE KAPITOLY

- Představit možná rizika elektronického obchodování a způsob jejich řízení.
- Prezentovat pravidla chování uživatelů v počítačových sítích resp. Internetu v návaznosti na elektronické obchodování.
- Detailně popsat princip elektronického resp. digitálního podpisu.

KLÍČOVÁ SLOVA KAPITOLY

Bezpečnost e-business a e-commerce. Řízení rizik v e-business a e-commerce. Zabezpečení dat. Elektronický podpis.

10.1 Rizika elektronického obchodování a jejich řízení

Elektronické obchodování přináší celou řadu výhod pouze za předpokladu vyvarování se chyb, kterých se může tvůrce, implementátor, provozovatel a posléze i uživatel elektronického obchodu dopustit. Existuje celá řada rizik, která se musí dobře zmapovat a identifikovat. Pokud rizika známe, můžeme je korigovat, potažmo minimalizovat. V této souvislosti hovoříme o tzv. Řízení rizik.

ŘÍZENÍ RIZIK

Řízení rizik lze definovat jako identifikaci, analýzu a ekonomickou kontrolu těch rizik, která mohou ohrozit aktiva podniku nebo jeho schopnost produkovat příjmy.

Jestliže dojde ke správné identifikaci a nadefinování rizik a zúčastněné subjekty budou své elektronické obchodní aktivity vytvářet a realizovat s vědomím, že daná rizika existují, dojde k jednoznačné minimalizaci jejich vlivu a můžeme konstatovat, že řízené riziko přestává být rizikem. Za rizika jsou posléze považovány nové skutečnosti a stavy, které jsou neočekávané, a které se musí posléze průběžně minimalizovat nebo lépe zcela eliminovat.

SAMOSTATNÝ ÚKOL

Vyhledejte na internetu články a odkazy týkající se rizik elektronického obchodování a elektronického podnikání. Uveďte základní oblasti rizik a způsoby jejich řešení a prevence.

10.2 Bezpečnost na Internetu

VYBRANÉ ZDROJE

1) http://www.bezpecnyInternet.cz/
2) http://www.bezpecnyInternet.cz/pokrocily/nakupovani-pres-Internet/rady.aspx
3) http://www.jaknaInternet.cz/page/1179/bezpecnost-pocitace/

10.3 Elektronický & digitální podpis

Elektronický podpis se stal nezbytným prvkem mnoha systémů. V roce 2000 došlo k vytvoření právní podpory, kdy v platnost vešel zákon č. 227/2000 Sb. O elektronickém podpisu.

ELEKTRONICKÝ PODPIS

Dle zákona č. 227/2000 o elektronickém podpisu je elektronický podpis definován jako: Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

DIGITÁLNÍ PODPIS

Digitální podpis je spojením klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka.

Na závěr je nutné uvést, že digitální podpis sám o sobě nepotvrzuje identitu uživatele nebo systému. Ta je garantována důvěryhodnou třetí stranou - certifikační autoritou. Vydává důvěryhodný certifikát uživateli na základě znalosti jeho identity.

10.4 Certifikační autorita

Jestliže chceme získat certifikát, musíme si vybrat nějakou certifikační autoritu a požádat o jeho vydání.

CERTIFIKAČNÍ AUTORITA

Certifikační autorita (zkratka CA) je 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.

Činnost certifikační autority by se dala přirovnat k činnosti notáře při ověřování klasického podpisu. Je zde ovšem jedna zásadní odlišnost - zatímco notář musí ověřit každý jednotlivý podpis, certifikační autorita neověřuje vlastní podpis, ale data pro vytváření digitálního podpisu, skutečných podpisů potom můžete pomocí těchto dat vytvořit libovolné množství. Jinak je ovšem postup analogický - certifikační autorita stejně jako notář musí zkontrolovat totožnost podepisující se osoby (respektive žadatele o certifikát), zajistit, že se skutečně podepisuje daná osoba (u klasického podpisu se osoba podepíše přímo před notářem, v případě digitálního podpisu musí prokázat vlastnictví daného páru klíčů), provést záznam potřebných údajů (do databáze, respektive do knihy), a následně vydá certifikát obsahující všechny potřebné údaje (notář připojí k dokumentu razítko, kde údaje vyplní) podepsaný svým soukromým klíčem (respektive vlastnoručním podpisem v případě notářského ověření).

Na rozdíl od notářského ověření podpisu, které je víceméně jednorázovým úkonem, je zde ovšem ještě jedna odlišnost. Protože digitální podpis se dá pomocí certifikátu (respektive s ním svázaného soukromého klíče) vytvářet opakovaně po celou dobu platnosti certifikátu, vzniká mezi certifikační autoritou a držitelem certifikátu obchodní vztah, který je také zpravidla podepřen uzavřením smlouvy, ze které pro obě strany vyplývají jisté povinnosti. Certifikační autorita na základě toho poskytuje další servis, jako například zneplatňování certifikátů a zveřejňování jejich seznamů, vydávání následných certifikátů a podobně. Držitel certifikátu se potom zavazuje, že poskytne certifikační autoritě přesné a pravdivé informace, bude ji informovat o případných změnách těchto údajů, bude chránit svůj soukromý klíč a, v případě jeho kompromitace, požádá certifikační autoritu o zneplatnění certifikátu.

10.4.1 Zneplatněné certifikáty

Kromě vlastního vydávání a správy certifikátů poskytuje certifikační autorita další důležitou službu, a sice udržování a publikování tzv. seznamu zneplatněných certifikátů, neboli CRL (Certificate Revocation List). Jedná se o seznam certifikátů, u kterých byla předčasně ukončena jejich platnost. Předčasné ukončení platnosti (neboli zneplatnění) certifikátu může mít několik příčin, například změnu údajů uvedených v certifikátu, ale nejzávažnější příčinou je kompromitace soukromého klíče. Pokud k takové události dojde, hrozí riziko zneužití klíče (laicky řečeno "zfalšování" podpisu) a pochopitelně snahou držitele certifikátu je toto riziko co nejvíce eliminovat. Proto je důležité, aby byl certifikát uveden v seznamu zneplatněných certifikátů co nejdříve od okamžiku, kdy držitel certifikátu o zneplatnění požádá. V praxi je většinou CRL publikován v pravidelných intervalech, bez ohledu na to, jestli byl nějaký certifikát zneplatněn, či nikoli. Protože si tento seznam musí příjemci digitálně podepsaných zpráv pravidelně stahovat a instalovat, musí být také seznam zneplatněných certifikátů neustále dostupný, zpravidla na webu certifikační autority (měl být dostupný dvěma na sobě nezávislými způsoby).

SAMOSTATNÝ ÚKOL

Vyhledejte na internetu odkazy na konkrétní certifikační autority a porovnejte jejich nabídky a možnosti využití.

10.5 Základní pojmy z kryptologie

Pro správné pochopení principu digitálního podpisu je nutné představit základní pojmy z oblasti kryptologie (viz tabulka 13).

Tabulka 13: Základní pojmy z kryptologie

Pojem	Charakteristika
Kryptologie	Věda o šifrování (je v ní obsažena kryptografie a kryptoanalýza).
Kryptografie	Zabývá se metodami šifrování dat.
Kryptoanalýza	Zabývá se metodami umožňujícími šifrované zprávy neautorizovaně dešifrovat.
Šifrování	Proces, při kterém dochází k převedení obecně srozumitelného textu na zašifrovaný text (jeho obsah nelze přímo určit).
Dešifrování	Proces opačný k šifrování.
Otevřený text	Původní nezašifrovaný text.
Šifrovaný text (šifra)	Zašifrovaný text
Šifrovací (dešifrovací) algoritmus	Funkce, obecně sestavená na matematickém základě, podle které se provádí vlastní šifrování a dešifrování zpráv.
Šifrovací klíč	Binární informace, která slouží jako jednoznačný podmíněný vstupní parametr při šifrování a dešifrování zpráv. Obecně má předem určený počet bitů.

ŠIFROVÁNÍ

Jestliže označíme C jako šifru, P otevřený původní text, E (D) šifrovací (dešifrovací) algoritmus a K klíč, pak můžeme šifru obecně vyjádřit jako funkci ve tvaru:

C = E(P) resp. C = E(K, P) - šifrování
P = D(C) resp. P = D(K, C) - dešifrování
přičemž musí platit, že P = D(E(P))

10.5.1 Požadavky na šifrovací algoritmus

- Zprávy by se zašifrováním neměly zvětšovat.
- Algoritmus šifrování musí čím jak nejvíce zamezit možnosti prolomení šifry, nicméně jeho implementace by měla být co nejjednodušší.
- Algoritmus by v žádném případě neměl být omezující (např. počet znaků a typy znaků).
- Množství práce vynaložené na šifrování a dešifrování by mělo být úměrné požadovanému stupni utajení.
- Chyby při šifrování by se neměly příliš šířit a ovlivňovat následující komunikaci.

10.5.2 Šifrovací & dešifrovací klíč

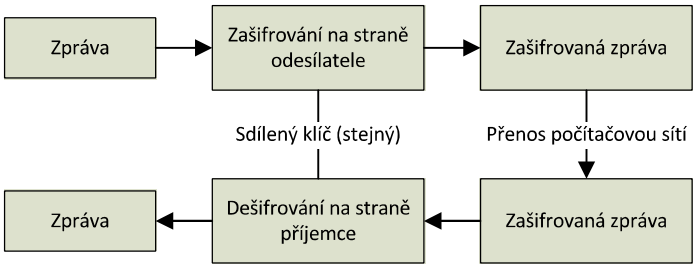
Jedním z nejdůležitějších prvků, od kterého se odvíjí bezpečnost šifrovacího systému z hlediska přenosu zašifrovaných dat, je klíč. Prakticky všechny jeho parametry a stadia od generace přes distribuci až po délku platnosti jsou velice důležité. Jakékoliv podcenění důležitosti klíče a z toho vyplývající nutnosti jeho ochrany může mít za následek plné porušení požadované bezpečnosti systému. Klíč můžeme do jisté míry považovat za jakési "vstupní heslo" šifrovacího (dešifrovacího) algoritmu.

10.6 Typy šifrování

Z hlediska použitých šifrovacích algoritmů a potřebných klíčů hovoříme o šifrování se symetrickým klíčem a šifrování s asymetrickým klíčem. Symetrickému šifrování se taky často říká šifrování s tajným klíčem, asymetrickému šifrování s veřejným klíčem.

10.6.1 Šifrování s tajným klíčem

Při symetrické kryptografii komunikující partneři používají stejný kryptografický klíč (obrázek 15).

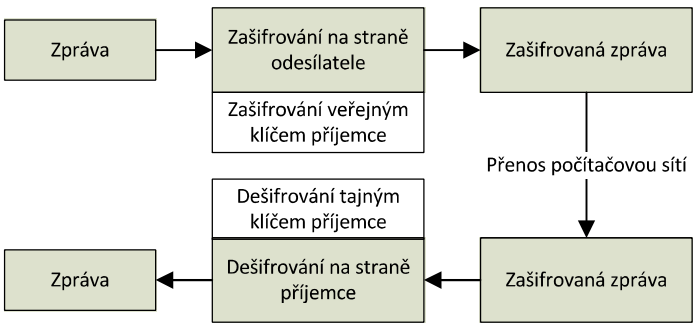


Obrázek 15: Šifrování s tajným klíčem (symetrické)

10.6.2 Šifrování s veřejným klíčem

Při asymetrické kryptografii se klíče komunikujících partnerů liší. Klíče jsou navzájem neodvoditelné, čili ze znalosti jednoho klíče nemůžeme vypočíst druhý. Zpráva se jedním klíčem zašifruje. Dešifrování stejným klíčem už není možné. To se provede až druhým klíčem. Tento způsob šifrování zajišťuje mnohem vyšší bezpečnost než je u symetrického šifrování.

Příkladem aplikace je kryptografie s veřejným klíčem a soukromým klíčem. Jeho princip spočívá v tom, že každý uživatel má pro svou potřebu dva klíče. Jeden zveřejní a druhý je tajný, přičemž veřejný klíč slouží k šifrování a tajný je dešifrovací. Musí se samozřejmě jednat o jednoznačně vygenerovanou dvojici klíčů, přičemž tajný klíč uživatele není odvoditelný z veřejného klíče. Samotný postup při zasílání zpráv pak vypadá tak, že odesílatel zašifruje text pomocí veřejného klíče příjemce a odešle jej. Příjemce pak zprávu dešifruje pomocí svého tajného klíče (obrázek 16).



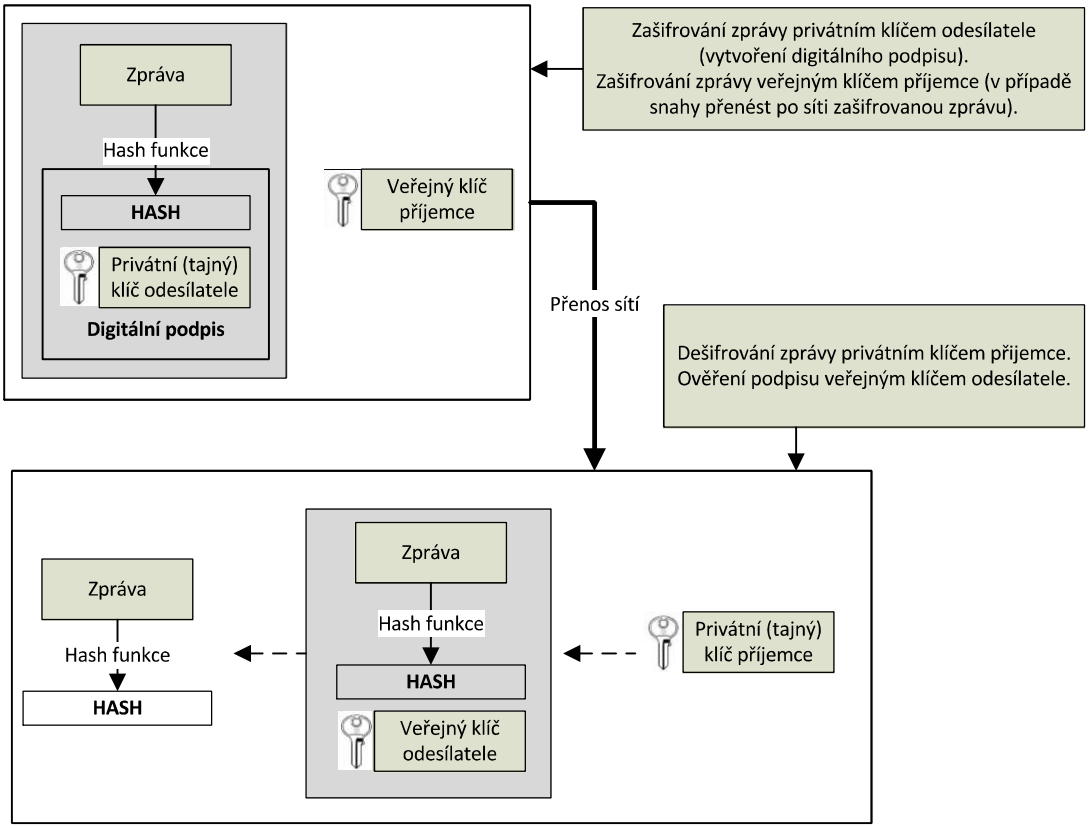
Obrázek 16: Šifrování s veřejným klíčem (asymetrické)

Princip digitálního podpisu je postaven na šifrování s veřejným klíčem!

10.6.3 Princip digitálního podpisu

Princip elektronického podpisu ukazuje obrázek 17. Na straně odesílatele se nejprve ze zprávy vytvoří pomocí tzv. hash funkce (transformační funkce – jednosměrný algoritmus)

digitální vzorek zprávy (hash, digiset, kontrolní vzorek, …). Ten je pro každou zprávu jednoznačný a nezaměnitelný. Tento vzorek je podepsán soukromým (privátním, tajným) klíčem odesílatele a je připojen ke zprávě. Pokud chceme ještě zajistit šifrování zprávy během přenosu po síti, využijeme šifrování a zašifrujeme vše, co odesíláme veřejným klíčem příjemce. Tím zajistíme, že zprávu bude moci dešifrovat pouze příjemce, kterému je zpráva určena. Na straně příjemce dojde nejprve k dešifrování došlé zprávy privátním dešifrovacím klíčem. Tím příjemce dostane opět zprávu a k ní připojený zašifrovaný vzorek. Ze zprávy vytvoří pomocí stejné hash funkce kontrolní vzorek a došlý kontrolní vzorek se dešifruje veřejným klíčem odesílatele.



Obrázek 17: Princip digitálního podpisu

CO DIGITÁLNÍ PODPIS OVĚŘUJE?

Porovnáním obou vzorků si příjemce ověří:

- ***Autentičnost podepisující osoby* - zprávu mohl podepsat pouze ten, kdo má k deklarovanému veřejnému klíči odpovídající privátní klíč.**
- ***Integritu zprávy* - v době, která uplynula mezi podepsáním zprávy a ověřováním podpisu, nebyla tato zpráva modifikována.**
- ***Neodmítnutelnost odpovědnosti* - osoba, která tuto zprávu podepsala, nemůže svou činnost popřít, neboť její znalost privátního klíče je unikátní.**

- ***Časové ukotvení* - Elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu. Časové razítko vydává důvěryhodná třetí strana, a protože je součástí elektronického podpisu, lze ji ověřit stejným postupem, jako elektronický podepsaný dokument.**

VYBRANÉ ZDROJE

1) http://www.postsignum.cz/
2) https://www.digitalni-podpis.cz/
3) http://www.jaknainternet.cz/page/1249/elektronicky-podpis/
4) http://frankbold.org/poradna/kategorie/ruzne/rada/elektronicky-podpis-nebo-datova-schranka
5) http://www.ica.cz/Elektronicky-podpis

SHRNUTÍ KAPITOLY

Bezpečnost internetu je jednou z nejklíčovějších problematik současnosti. Elektronické podnikání a obchodování je rozsáhlým kyberprostředím, které v rámci internetu vytváří oblast, která je napadnutelná hackery, a proto je potřeba se touto problematikou zabývat. Důležité je dávat pozor, aby se elektronické obchodování nestalo „dírou“ do informačního systému podniku a na straně druhé je důležité, aby zůstaly chráněny osobní údaje běžných spotřebitelů. Podstatným prvkem je rovněž identifikace prodávajícího a kupujícího, která se dá zajistit digitálním podpisem.