Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Systémy pre elektronický obchod - funkcionalita a bezpečnosť

(diplomová práca)

Autor: Stanislav Miklík

Školiteľ: doc. RNDr. Daniel Olejár, PhD.

Bratislava, 2006

Zadanie:

Cieľom diplomovej práce je analyzovať funkcionalitu a bezpečnostné aspekty systému umožňujúceho realizáciu elektronického obchodu medzi obchodníkmi a koncovými klientami. Predpokladá sa, že systém bude prevádzkovať tretia strana (poskytovateľ služby).

Úlohou diplomanta je podrobnejšie popísať procesy, ktoré v takomto systéme prebiehajú, analyzovať možné hrozby a odhadnúť riziká z nich vyplývajúce a navrhnúť opatrenia, ktoré by znížili identifikované riziká na prijateľnú úroveň. Má vytvoriť bezpečnosný model systému v podobe Protection Profile podľa štandardu ISO/IEC 15408. Keďže bezpečnosť systému závisí aj od prevádzky, o ktorej je možné na úrovni modelu prijať len predpoklady, diplomant by mal požiadavky na prevádzku premietnuť do opatrení podľa štandardu ISO/IEC 17799.

Čestne prehlasujem, že som túto diplomovú prácu vypracoval samostatne s použitím uvedenej literatúry pod odborným vedením vedúceho diplomovej práce.

Ďakujem vedúcemu diplomovej práce doc. RNDr. Danielovi Olejárovi, PhD. za vedenie, odbornú pomoc a užitočné prípomienky, Michalovi Pokornému za morálnu podporu a všetkým ostatným, ktorí prispeli k dokončeniu tejto diplomovej práce.

Abstrakt:

V tejto práci sme podali čitateľovi základný prehľad o systémoch pre elektronický obchod. Analyzovali sme základné modely elektronického obchodu, ich účastníkov a vzťahy medzi nimi. Uviedli sme možné príklady použitia takýchto systémov v praxi.

Ďalej sme sa venovali hlavnej časti tejto práce - bezpečnostným aspektom elektronického obchodu. Čitateľa sme uviedli do základov kryptografie a informačnej bezpečnosti. Taktiež sme predstavili štandard Common Criteria, podľa ktorého sme nakoniec vybudovali bezpečnostný model pre množinu systémov elektronického obchodu typu B2C. Úroveň bezpečnosti sme postavili na úroveň EAL 3, čo ešte neznamená nutnosti zásadne meniť existujúce dobré zvyklosti pri návrhu a vývoji systémov. Uvedený model sme doplnili aj o zásady správnej prevádzky a správy pre komplexnejšej pohľad na bezpečnosť, ktoré sme vypracovali na základe štandardu ISO/IEC 17799.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Časť I

Úvod

V dnešnej dobe je naše počínanie vo veľkej miere späté s použitím informačných technológií. A vplyv informačných technológií sa čím ďalej, tým viac rozširuje do mnohých oblastí života. Jednou z nich je aj obchodovanie a jeho informačná podoba - elektronický obchod.

V minulosti mohli využívať elektronický obchod len veľké spoločnosti, ktoré používali vlastné systémy a súkromné siete. S rozvojom internetu a zlepšovaním výkonu a dostupnosti výpočtovej techniky sa elektronický obchod stal dostupný stredným a malým podnikateľom a taktiež aj koncovým zákazníkom. Rozvoj elektronického obchodu je však podmienený istými faktormi a to najmä technickými, technologickými, právnymi a bezpečnostnými.

K technickým faktorom určite patrí dostupnosť telekomunikačnej infraštruktúry, ktorá sa v súčastnosti u nás dá pokladať za celkom dobrú. Keďže elektronický obchod sa vyvíja rôznymi smermi a využíva rôzne technológie, je potrebná pre lepšiu integráciu systémov istá štandardizácia. V súčastnosti existujú viaceré štandardy, ale mnohé systémy využívajú aj vlastné protokoly. Pre širšie uplatnenie v spoločnosti je nutné pre elektronický obchod vytvoriť aj legislatívne prostredie. V tejto oblasti sa deje pokrok, či už vo forme direktív Európskej únie, ako aj vo forme prijímaných zákonoch SR.

Nevyhnutnou podmienkou pre fungovanie elektronického obchodu je otázka bezpečnosti a s ňou súvisiaca otázka dôvery používateľov k systémom elektronického obchodu. Jednak je nutné zabezpečiť dôvernosť detailov obchodu, ktoré môžu byť predmetom obchodného tajomstva, ale môže ísť taktiež o osobné údaje alebo iné údaje, ktoré by mali zostať utajené. V neposlednom rade však ide aj o korektné fungovanie prebiehajúceho obchodovania. Vzhľadom na špecifiká digitálneho sveta treba osobitne riešiť otázky pôvodu údajov (kto zadal objednávky, ...), zachovania integrity (sú tieto údaje nezmenené?) a ďalšie. Preto sa v diplomovej práci budeme zaoberať otázkami bezpečnosti systémov elektronického obchodu.

Najprv sa pozrieme na elektronický obchod ako taký, podáme prehľad rôznych modelov elektronického obchodu. Keďže možnosti elektronického obchodovania sú veľmi široké, zameriame na obchodovanie medzi zákazníkom a obchodníkom. Pri skúmaní otázok bezpečnosti zvolíme všeobecnejší model fungovania systému pre elektronický obchod, pre ktorý potom zostavíme bezpečnostný model. Prostriedok pre zostavenie tohto modelu nám poskytnú Common Criteria vo forme profilu ochrany. Keďže Common Criteria slúžia na popis informačných požiadaviek na systém, tento model ešte doplníme pomocou neinformačných požiadaviek podľa štandardu BS 7799 Správa informačnej bezpečnosti (ISO 17799 a ISO 27001), ktorý poskytuje

skôr manažérsky prístup k prevádzke systému.

Diplomová práca je delená do nasledujúcich kapitol:

Kapitola 1 definuje pojem elektronického obchodu, popisuje jeho históriu a súčasný stav.

Kapitola 2 popisuje modely elektronického obchodu, účastníkov a pre jednotlivé typy modelov popisuje typické prípady použitia.

Kapitola 3 uvádza čitateľa do problematiky informačnej bezpečnosti a popisuje základné pojmy z tejto oblasti.

Kapitola 4 poskytuje základy kryptografie a ukazuje možné využitie kryptografických prvkov pri riešení problémov informačnej bezpečnosti.

Kapitola 5 sa zaoberá ochranou informačných systémov a približuje nám Common Criteria ako štandardizovaný prístup k riešeniu otázok bezpečnosti.

Kapitola 6 presnejšie popisuje model systému, ktorý sme zvolili pre vytvorenie bezpečnostného modelu. Popisuje účastníkov systému a ich interakcie so systémom.

Kapitola 7 predstavuje vlastný bezpečnostný model systému pre elektronický obchod vo forme profilu ochrany podľa Common Criteria.

Kapitola 8 popisuje pravidlá bezpečnej správy a prevádzky systému.

Táto práca je primárne venovaná dvom základným skupinám ľudí: obchodníkom a informatikom. Obchodníci musia vedieť vyjadriť požiadavky na informačné riešenie, aby vyjadrili svoje organizačné potreby. Musia si byť vedomí možných rizík a potreby priebežného udržiavania bezpečnosti systému. Taktiež by mali vedieť posúdiť, či ponúkaný produkt spĺňa ich bezpečnostné potreby. Pri nich nemôžeme predpokladať znalosti kryptografie ani informačnej bezpečnosti. Aj preto v diplomovej práci uvádzame základné pojmy z kryptografie a informačnej bezpečnosti v rozsahu potrebnom na pochopenie bezpečnostných požiadaviek na systém a posúdenie navrhnutých riešení. Tieto časti si nerobia nárok na úplnosť a čitateľa, ktorý by mal záujem o podrobnejšie poznatky odkazujeme na literatúru uvedenú v bibliografií.

Informatik - analytik alebo vývojár musí vedieť identifikovať bezpečnostné požiadavky na systém. Pri návrhu a implementácií systému musí zohľadniť bezpečnostné funkcie a požiadavky definované v bezpečnostnom modeli. U neho sa už predpokladá istá znalosť kryptografie a informačnej bezpečnosti.

Pri písaní tejto práce sme sa museli vyrovnať s problémom, že pre danú oblasť v dnešnej dobe neexistuje kompletná slovenská terminológia, prípadne je nejednotná. Preto sme sa snažili nájsť vhodné slovenské ekvivalenty a v prípadoch, keď to bolo nemožné alebo je bežne používaná anglická terminológia, sme ostali pri pôvodných výrazoch. Takisto sme neprekladali zaužívané skratky. Kvôli kompletnosti a prehľadnosti je k práci pripojený slovník používaných pojmov.

Časť II

Elektronický obchod

Kapitola 1

Úvod k elektronickému obchodu

V dnešnej dobe sa čoraz viac rozmáha elektronický obchod. Umožňuje nám nakupovať vo virtuálnom obchode bez toho, aby sme museli navštíviť obchod fyzicky. Vzdialenosti sa stávajú čoraz menej dôležité. Tovar si bežne môžme objednať na dobierku alebo ho zaplatíme pomocou kreditnej karty. Ale nie je to len tovar, za ktorý platíme, cez internet si môžme objednať aj rôzne služby, dokonca niekedy platíme za prístup k informáciám. Elektronický obchod sa však nevzťahuje len na koncového zákazníka. Takisto umožňuje obchodovať navzájom obchodníkom, umožňuje automatizovať niektoré procesy prebiehajúce v rámci spoločnosti aj medzi spoločnosťami; napr. v prípade novej objednávky automaticky doobjednať potrebný tovar či sledovať proces výroby a informovať zákazníka o stave vybavenia. Čo všetko vlastne zahŕňa elektronický obchod?

Zatiaľ neexistuje všeobecne uznávaná definícia elektronického obchodu. Napríklad definícia kanadskej vlády je taká široká, že zahŕňa akékoľvek transakcie uskutočňované elektronicky. My pre účely tejto diplomovej práce budeme rozumieť pod týmto pojmom nasledovné:

Elektronický obchod je výmena alebo spracovávanie obchodných informácií pomocou počítačov spojených v sieti.

Pod túto definíciu teda môžme zahrnúť nielen nákup tovaru, ale už aj marketing a reklamu, čo je vlastne poskytovanie informácií o tovaroch a službách, zisťovanie potrieb zákazníkov, vykonávanie prieskumov trhu atď. Ďalšími príkladmi sú fakturácie či elektronické platby. Elektronický obchod sa väčšinou vykonáva v prostredí siete internet, ale samozrejme hovoríme aj o elektronickom obchode uskutočňovanom aj v privátnych sieťach.

V čom spočíva úspech elektronického obchodu? Veľkou výhodou elektronického obchodu je, že rozširuje pôsobisko obchodovania na národnú či medzinárodnú úroveň. Umožňuje nájsť lepšie ponuky, získať lepší výber, spoločnostiam nájsť nových zákazníkov, lepších dodávateľov. Ďalej umožňuje znížiť administratívne náklady na tvorbu, spracovanie, distribúciu a uskladňovanie informácií, ktoré predtým boli v papierovej podobe. Napríklad náklady na vydanie elektronickej platby sú nižšie ako vydanie papierového šeku. Vykonávanie obchodov a iných transakcií je umožnené v ľubovoľnom čase, nielen v rámci otváracích hodín. Navyše elektronický obchod umožňuje zrýchlenie obratu skrátením časov potrebných na uskutočňovanie transakcií. Významným prísom je zníženie zásob možnosťou použitia ťahového typu manažmentu. V ťahovom systéme sa po prijatí objednávky spustí proces objednania potrebných komponentov a následne sputstí výroba. Pri vhodnom prepojení systémov elektronický obchod umožňuje zefektívnenie výrobných ale aj iných procesov. Výhodou elektronického prostredia je aj jeho interaktivita, ktorá umožňuje rýchlejšiu dostupnosť želaných informácií alebo aj mierenejšiu reklamu. Toto umožnilo zmenu klasickej reklamy mierenej na čo najväčšie masy na tzv. "win to win strategy", kde aj obchodník môže podať mierenejšiu reklamu bez straty potenciálnych zákazníkov a aj zákazník dostane presnejšie a lepšie informácie a služby.

Hoci pojem elektronický obchod sa začal v širšej miere používať len nedávno, korene elektronického obchodu sa dajú datovať už do 60.-tych rokov 20.-teho storočia.[1] V tom čase išlo o veľké počítačové systémy a súkromné siete, ktoré mohli využívať len veľké spoločnosti. Tieto systémy sa používali na spracovanie a výmenu obchodných informácií. Práve potreba výmeny týchto informácií viedla k vyvinutiu formátu EDI (*Electronic Data Interchange*). EDI slúži na výmenu obchodných informácií pomocou dohodnutých štandardných správ medzi aplikáciami. Výmena týchto dát je nezávislá na použitej prenosovej vrstve a vyžaduje minimálnu ľudskú intervenciu.

Existuje viacero štandardov EDI, ale jediný medzinárodný štandard je UN/ EDIFACT (*United Nations/ Electronic Data Interchange For Administration, Commerce, and Transport*), ktorý bol schválený ako štandard ISO 9735. Tieto štandardy predpisujú, ktoré informácie sú pre konkrétny dokument (správu) povinné resp. nepovinné. Tieto dáta sú interpretované tzv. prekladacím softvérom, ktorý prekladá tieto spoločné štandardné správy na

[1] Ak nerátame použitie telegrafov a telefónov napríklad pri obchodovaní na burze, aj keď na tieto sa nevzťahuje naša definícia.

vlastné dokumenty a naopak. Význam týchto informácií musí byť dohodnutý.

EDI je stále používaný dátový formát v mnohých elektronických transakciách, aj keď čím ďalej sa rozmáha formát XML(*Extensible Markup Language*), ktorý síce zaberá viacej miesta, ale je pre ľudí ľahšie čitateľný.

Postupom času sa počítače stávali dostupnejšie a internet umožňoval globálnu konektivitu za dostupnú cenu, menil sa aj ráz využitia počítačov. Predtým pri využívaní súkromných sietí nebola až taká dôležitá otázka bezpečnosti, keďže tieto siete boli kontrolované buď priamo spoločnosťami, ktoré ich využívali, alebo aspoň známou spoločnosťou - prevádzkovateľom.

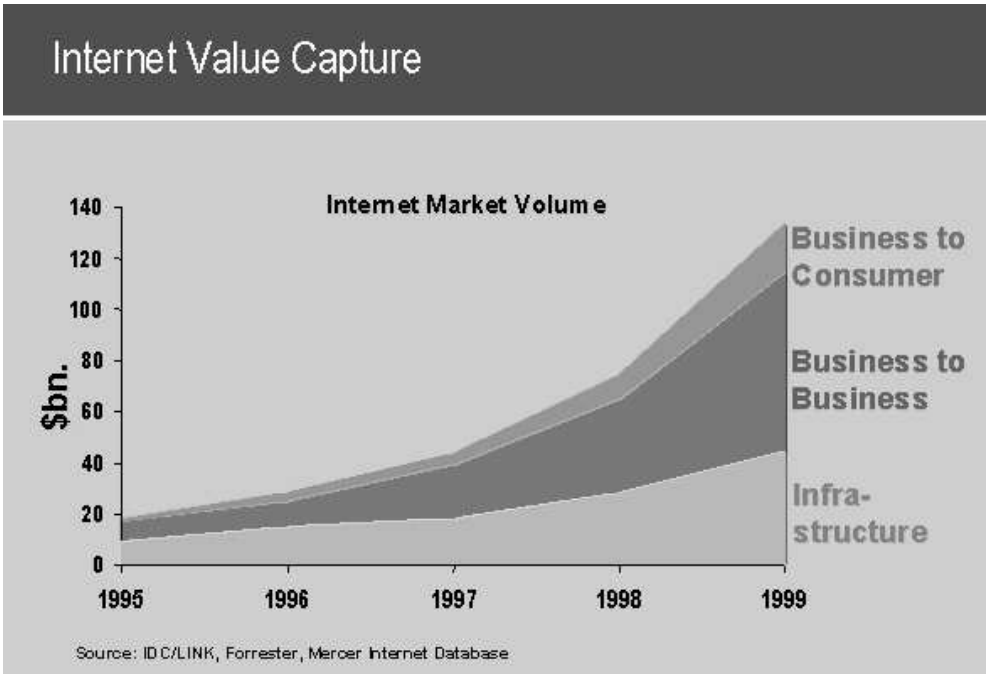
Veľký krok v elektronickom obchode znamenalo vyvinutie protokolu SSL (*Secure Sockets Layer*) v roku 1994 firmou Netscape. Pôvodne tento protokol bol vyvinutý na zabezpečenie spojenia medzi prehliadačom a webovým serverom, ale neskôr začal byť používaný aj pre iné služby ako sú FTP alebo TELNET. Protokol SSL slúžil ako základ pre protokol TLS (*Trasport Layer Security*),ktorý je definovaný v RFC 2246.

Do tých časov sa elektronický obchod nemohol vo veľkom rozvíjať na internetových stránkach, pretože nebola zaručená bezpečnosť spojenia. Nedalo sa zaručiť súkromie osobných údajov, takže elektronický obchod bol obmedzený na ponúkanie tovaru. Práve zavedenie protokolu SSL umožnilo ďalší rozvoj na internete a prispel aj k väčšiemu zapojeniu obyčajných ľudí do elektronického obchodovania, keďže predtým išlo najmä o obchodovanie medzi spoločnosťami. A naozaj už v roku 1995 začali na internete svoju prevádzku dva veľké internetové obchody: *Amazon.com* a *eBay*. Amazon.com začal s predajom kníh, ďalej však rozšíril svoju ponuku o predaj hudobných CD, DVD, softvéru, nábytku a iných druhov tovaru. Spoločnosť eBay prevádzkuje online aukcie, kde ľudia môžu predávať a nakupovať tovar.

V roku 1996 bol vytvorený protokol SET (*Secure electronic transaction*), ktorý slúži na zabezpečenie transakcií kreditných kariet. Bol vyvinutý spoločnosťami Mastercard a Visa v spolupráci s ďalšími spoločnosťami. Používateľ protokolu SET obdrží tzv. elektronickú peňaženku (digitálny certifikát). Pri vykonávaní a overovaní transakcie sa na zaručenie súkromia a dôvernosti používa kombinácia certifikátov nákupcu, obchodníka a banky. Tento protokol sa však nepresadil a to najmä kvôli nutnosti inštalovať softvér (elektronickú peňaženku), zložitosti a cene.

Úspech elektronického obchodu je značne ovplyvnený úspechom internetu. Internet je obrovská, lacná celosvetová sieť spájajúca milióny účastníkov, ktorá takto vytvára veľký obchodný priestor. Koncom 90.-tych rokov za-

znamenal elektronický obchod exponenciálny nárast, ale tento nárast nebol samozrejme udržateľný. Napriek skľudneniu rastu sa opäť očakáva zvyšovanie objemu investícií do elektronického obchodu.



Obrázok 1.1: Objem internetového trhu. Zdroj: [11]

V súčasnej dobe má už skoro každá firma svoju prezentáciu na internete. Informujú o tom, kde ich možno nájsť, prezentujú oblasť, v ktorej pôsobia, zväčša predstavia svoje produkty. Niektoré ponúkajú už aj podrobnejší zoznam svojich produktov či služieb už aj s konkrétnymi podmienkami. Vzniklo aj mnoho elektronických obchodov ponúkajúcich rôzne druhy tovarov. Tento trend bol umožnený relatívne lacnými možnosťami webhostingu, ktorý je ponúkaný mnohými na to špecializovanými spoločnosťami. Tieto spoločnosti tiež zväčša aj ponúkajú vytvorenie stránky pre svojich zákazníkov - firmy. Rozvoj elektronického obchodu viedol dokonca k rozšíreniu ponúk vytvorenia stránok až k možnosti vytvorenia vlastného systému pre elektronický obchod podľa predvytvorených šablón. Tieto sú potom voliteľne rozšíriteľné o rôzne druhy platobných systémov.

V prípade elektronického obchodovania medzi dvomi obchodníkmi hrá naďalej dôležitú úlohu EDI. Ale aj tu nastáva posun k novým technológiám.

Medzi jednu z týchto technológií určite patrí XML a na nej postavené technológie SOAP (*Simple Object Access Protocol*), webovské služby a UDDI (*Universal Description, Discovery and Integration*). Webovské služby sú množina technológií, ktoré poskytujú platformovo nezávislé protokoly pre výmenu dát medzi aplikáciami. UDDI je štandard, ktorý umožňuje popisovanie, zverejňovanie a vyhľadávanie webovských služieb.

Ďalší rozvoj elektronického obchodu sa musí vyrovnať s niekoľkými bariérami. K technickým bariéram patrí nedostatok široko akceptovaných a používaných štandardov. Rozvoj elektronického obchodu je taktiež podmienený rozvinutosťou a dostupnosťou telekomunikačnej infraštruktúry. Dôležitý fakt je aj integrácia existujúcich obchodných systémov s možnosťami elektronického obchodu, možnosťou je aj nahradenie zastaraných systémov novými.

Z netechnických bariér sem patria vysoké náklady na zavedenie a vývoj týchto systémov. Nevyhnutnou podmienkou na širšie používanie elektronického obchodu je dostatočná legislatíva. Je nutné zavedenie istých pravidiel pre právnu záväznosť akcií vykonaných prostredníctvom elektronického obchodu (napríklad keď si niekto objedná tovar elektronicky, aby nemohol potom odoprieť jeho zaplatenie). Ďalšou otázkou je bezpečnosť a súkromie, najmä v oblasti obchodu so zákazníkmi treba zamedziť možnosti zneužitia osobných údajov. Bezpečnosť a ochrana súkromia v elektronickom obchode je úzko spätá s potrebou prekonať nedôveru používateľov. Pri snahe použiť elektronický obchod na nadnárodnej úrovni začína dôležitú rolu hrať aj jazyk a kultúrne rozdiely.

V tejto kapitole sme stručne načrtli, čo to je elektronický obchod, povedali niečo o jeho histórií a o predpokladoch jeho ďalšieho rozvoja. V nasledujúcej kapitole povieme , v akých podobách prebieha elektronický obchod.

Kapitola 2

Modely

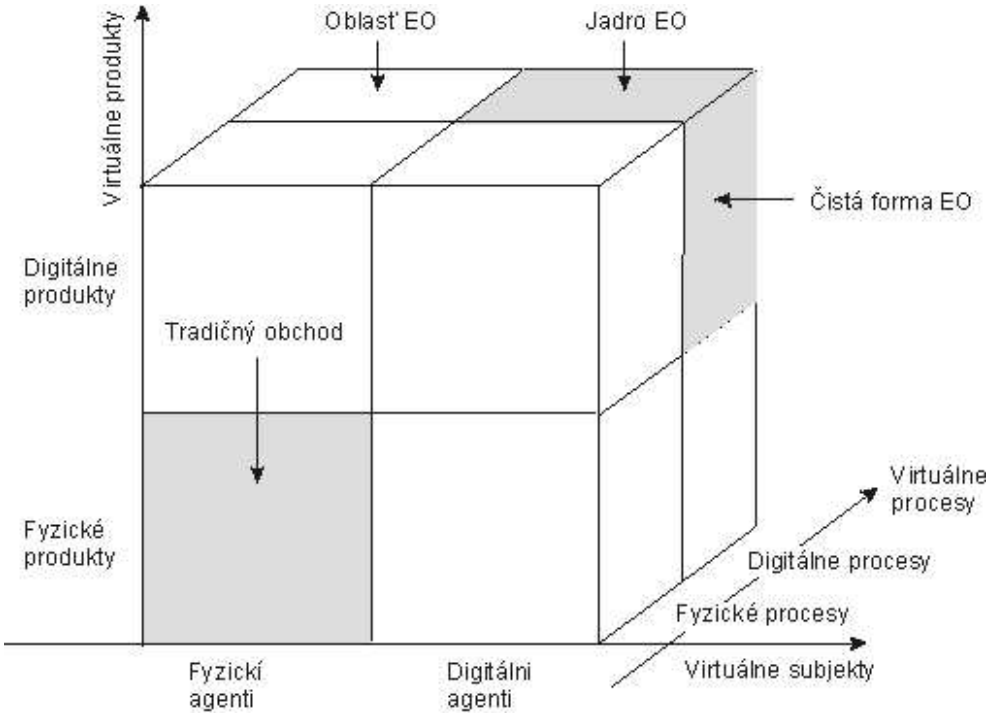
V tejto kapitole rozvinieme spôsoby fungovania elektronického obchodu, popíšeme základné typy účastníkov, vzťahy a možné prebiehajúce procesy medzi nimi.

Elektronický obchod môže nadobúdať rôzne podoby, ktoré závisia od stupňa digitalizácie predaného produktu alebo služby, procesu a spôsobu doručenia alebo sprostredkovania. V knihe *The economics of electronic commerce* [27] vytvorili autori model, ktorý vysvetľuje možné konfigurácie na základe troch dimenzií : produkty, agenti, ktorí ich predávajú ale aj jednotlivé procesy môžu byť fyzické alebo digitálne (viď obr.2.1). V tradičnom obchode sú všetky fyzické, v čistom elektronickom obchode sú zas všetky dimenzie digitálne. Ostatné časti "matice"sú hybridné formy elektronického obchodu.

Nákup klasického (nedigitálneho) tovaru nie je čistá forma elektronického obchodu, lebo pri nej dochádza k fyzickému doručeniu daného tovaru. Príkladom čistej formy elektronického obchodu môže byť napríklad stiahnutie programu zo stránky, pričom zaplatíme pomocou internetu.

Ďalšie delenie elektronického obchodu, ku ktorému sa dostávame, je podľa účastníkov tohto obchodu. Vo všeobecnosti máme tri rôzne typy účastníkov:

- **obchodník** (**B** - *business*) Môže ísť o malého obchodníka, ale aj o veľkú spoločnosť, ktorá sa snaží niečo predať, ale tak isto dobre sa môže snažiť aj niečo nakúpiť.
- **zákazník** (**C** - *customer/citizen*) Zväčša ide o fyzickú osobu, ktorá si chce niečo kúpiť alebo získať nejakú službu (niektoré služby sú poskytované aj zadarmo).



Obrázok 2.1: Dimenzie elektronického obchodu. Zdroj: [27]

- **vláda** (**G** - *goverment*) Ide o vládu alebo iné štátne úrady a orgány verejnej správy, ktoré realizujú transakcie medzi sebou, vo vzťahu ku komerčnej sfére (napr. verejné obstarávanie, dane) a k občanovi.

Hoci ľubovoľná kombinácia je podľa definície možná, najviac sa hovorí o elektronických obchodoch typu **B2B** (*business-to-business*) alebo **B2C** (*business-to-customer*). V rámci snáh štátu o digitalizáciu procesov sa zvykne tiež hovoriť o **G2C** (goverment-to-citizen).

Elektronický obchod medzi dvoma obchodníkmi môže nadobúdať najrôznejšie podoby. Všetko závisí len od toho, na akej forme komunikácie sa dohodnú. Môžu používať buď proprietárne protokoly alebo aj štandardné ako je napríklad EDI. Pomocou nich sú schopní dosiahnuť poskytovanie mnohých služieb, automatizovanie výrobných procesov a pod. Tieto procesy a služby zahŕňajú obstarávanie, objednávanie, automatické dopĺňanie zásob a k nim zodpovedajúce procesy, ako je prijímanie objednávok, ich vybavovanie. S tým potom súvisia finančné procesy ako sú spracovanie platieb alebo vysta-

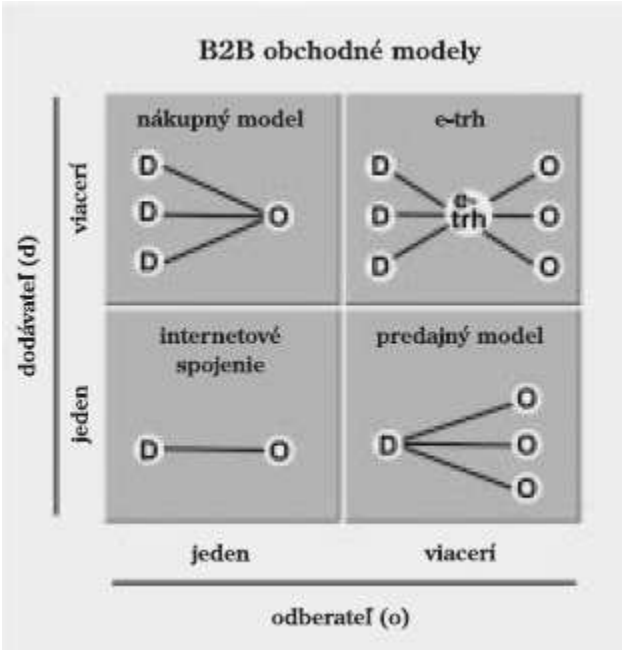
vovanie faktúr a ostatné prepojenia s dodávateľom. Toto všetko môže byť navzájom prepojené (napr. po prijatí objednávky vystav faktúru a pod.) a prepojené na systémy automatickej kontroly výrobkov a procesov.

Okrem toho je možná aj automatizovaná kontrola stavu plnenia, či už výroby, alebo v akom stave je vybavenie poskytnutia služby. Toto umožní odberateľov lepšie plánovanie vlastných úloh, prípadne ich automatické aktivovanie. Príkladom tohto je sledovanie polohy zásielky či transportovaného tovaru, prípadne automatické oznámenie po vykonaní colných úkonov.

Tieto procesy sa však dajú deliť ďalej. Napríklad obchodné modely sa členia aj podľa počtu odberateľov a dodávateľov, ktorí vystupujú vo vzájomných vzťahoch. Podľa počtu účastníkov dodávateľov ku odberateľom môžme tieto modely deliť do nasledovných skupín (viď. obr.2.2):

- **priame spojenie (1:1)** V prípade úzkeho prepojenia dvoch účastníkov, medzi ktorými je zvyčajne bližší vzťah.
- **nákupný model (n:1)** Základom tohto typu býva jeden silný odberateľ, ktorý má vyjednávaciu silu (napríklad obchodné reťazce)
- **predajný model (1:n)** Možným modelom je aliancia dodávateľov, ktorý si nekonkurujú ale dopĺňajú. Potom sa ich výdavky na predaj delia medzi viaceré subjekty.
- **e-trh (n:m)** Analógia s klasickými trhmi, kde sa stretáva ponuka s dopytom. Väčšinou je realizovaný nezávislým subjektom.

Obchodné procesy prebiehajúce medzi dvoma obchodníkmi môžu byť naozaj rozmanité. V prípade elektronického obchodovania medzi obchodníkom a zákazníkom je tento vzťah trochu iný. V záujme obchodníka je zabezpečiť dostupnosť jeho služieb alebo tovarov čo najširšej skupine zákazníkov. Keďže nie je reálne sa dohodnúť s každým zákazníkom na forme komunikácie, musí obchodník použiť formu dostupnú priemernému zákazníkovi. Toto obmedzenie však nie je až také veľké ako by sa na prvý pohľad zdalo. V drvivej väčšine prípadov komunikácia medzi zákazníkom a obchodníkom prebieha vo forme klient-server komunikácie. V dnešnej dobe sa čoraz častejšie začína uplatňovať princíp tenkého klienta, tj. klient slúži len na zobrazovacie účely a zvyšnú prácu spraví server. Najbežnejším príkladom tenkého klienta je webovský prehliadač, pričom webovský server buď priamo poskytuje zvyšnú logiku, alebo slúži ako sprostredkovateľ k ďalšiemu "biznis"serveru.



Obrázok 2.2: Modely B2B obchodov. Zdroj:[12]

Keďže webovský prehliadač má skoro každý, kto je pripojený do internetu, orientácia poskytovania služieb prostredníctvom internetových stránok je prirodzená. Tenký klient však vo všeobecnosti nepokrýva všetky možnosti. Napríklad webovský prehliadač nie je schopný prijať nevyžiadanú správu od servera. Čiže v prípade očakávanej notifikácie sa musí prehliadač pravidelne obracať na server, čo nemusí viesť k efektívnemu využívaniu prostriedkov. Takéto alebo iné nedostatky je možné riešiť prídavným softvérom, ale ten si už zákazník musí inštalovať.

Obchody medzi obchodníkom a zákazníkom sa dajú diferencovať podľa miery digitalizácie prebiehajúcich procesov súvisiacich s obchodom (ktoré všetky činnosti sa vykonávajú automatizovane v elektronickej podobe). Tieto služby môžme rozdeliť nasledovne:

- informačné
- komunikačné
- transakčné

Príkladom informačných služieb je napríklad poskytnutie informácií o ponúkaných tovaroch v elektronickej podobe (spravidla pomocou internetovej stránky). Ďalej je dnes už skoro samozrejmá prezentácia firmy ako takej na internete (kto sú, čo robia, kde ich možno nájsť). Výhodou tejto formy oproti klasickým formám prezentovania (napríklad brožúrky či letáky) je možná interaktivita s používateľom, ako aj možnosti vyhľadávania, odkazy a aj ďalšie elektronické formáty. Informácie poskytované obchodníkom nemusia mať len všeobecný charakter, určený pre celú verejnosť. Obchodník je schopný poskytovať aj konkrétne informácie pre konkrétnu skupinu zákazníkov (napríklad držitelia klubovej karty) alebo pre konkrétneho zákazníka (napr. stav účtu).

Informačné služby zahŕňajú aj marketing. Firma nielen informuje o sebe, o svojich tovaroch a službách, ale snaží sa pomocou internetu aj vyhľadať zákazníkov, zisťovať ich potreby formou výskumov trhu alebo inak sa propagovať pomocou reklamy. Medzi najbežnejšie spôsoby reklamy na internete patria bannery, zaregistrovanie sa vo vyhľadávačoch alebo katalógoch a reklama pomocou elektronickej pošty. Bannery sú zväčša obrázky alebo iné multimediálne objekty (typu flash a pod.), pomocou ktorého sa dá dostať na reklamovanú stránku firmy alebo konkrétneho produktu. Ďalšou možnosťou je zaregistrovanie sa vo vyhľadávačoch alebo katalógoch, kde pri vyhľadaní alebo zobrazení témy sa na zvýhodnených miestach zobrazia odkazy danej firmy. Niektoré firmy zvyknú posielať novinky či iné informácie formou elektronickej pošty všetkým ľuďom, ktorý sa prihlásili na odberanie týchto informácií. Žiaľ vo veľkej miere sa rozmáha aj reklama formou nevyžiadanej pošty - spamu napriek tomu, že ide o nelegálnu činnosť.

Pri komunikačných službách už nastáva elektronická komunikácia medzi obchodníkom a zákazníkom(napr. dohoda o poskytnutí služieb, dohoda o kúpe tovaru), pričom následné procesy sa už vykonávajú tradičným spôsobom. Príkladom takejto komunikácie môže byť objednanie tovaru pomocou elektronickej pošty na základe údajov na internetovej stránke. Ďalšie kroky (platba, dodávka tovaru a iné) sa vykonávajú aj pomocou štandardných prostriedkov. Rozšírením tohto prípadu je použitie elektronických vozíkov, pomocou ktorých si zákazník popri prezeraní ponuky môže vybrať konkrétne produkty. Následne pomocou potvrdzovacieho formulára sa vygeneruje objednávka, ktorá sa zaregistruje a spracuje tradičnými postupmi. Zo strany obchodníka môže nastať interakcia vo forme potvrdenia prijatia objednávky či potvrdenia expedície tovaru. Navyše ku elektronickému obchodu môžme pridať aj podporu pre zákazníka.

Najvyššou formou automatizácie procesov sú tzv. transakčné služby. Pri nich prebieha automatizované spracovanie procesov spojených s obchodovaním. Samozrejme stupeň digitalizácie nemusí byť stopercentný (ako by to malo byť v čistej forme elektronického obchodu). Napríklad pri materiálnych produktoch ťažko zabezpečíme doručenie elektronicky. Možným scenárom je výber tovaru pomocou elektronického košíka, potvrdenie objednávacieho formuláru. Následne server overí platnosť údajov, zaregistruje objednávku a vyprodukuje sumár objednaných tovarov za posledné časové obdobie. V prípade prepojenia na vhodný B2B systém môže objednať daný tovar, ak nie je dostupný na sklade. Ak je tovar dostupný, informuje o tom zákazníka.

Okrem tradičných elektronických obchodov sa vyskytuje ešte aj model elektronických aukcií. Pri nich systém zvykne zabezpečiť automatický systém dražby spolu so zabezpečením vytvorenia zmluvy, platieb prípadne aj doručenia. Výhodou elektronických aukcií je efektívnosť ,nie je nutná fyzická účasť záujemov a samozrejme väčšia potenciálna účasť.

Dôležitou súčasťou mnohých transakčných systémov je subsystém - aplikácia na realizáciu elektronických platieb. Tieto môžu byť realizované spôsobmi:

- **Platby pomocou kreditných kariet** môžu byť realizované použitím protokolu SET. Pri použití protokolu SET obchodník nedostane číslo kreditnej karty, ale dostane len dáta, ktoré posunie banke, ktorá autorizuje transakciu a pošle autorizačné číslo obchodníkovi. Potom je schopný dokončiť transakciu. Taktiež zákazník dostane potvrdenie o transakcií.

- **Platby pomocou iných platobných systémov** sú realizované podobným spôsobom. Obchodník pre realizáciu platby presmeruje zákazníka na platobný systém, tam vyplní autorizačné údaje. Platobný systém overí vykonateľnosť transakcie (zväčša u banky zákazníka) a potvrdí obchodníkovi vykonanie transakcie. Výhodou je jednotné rozhranie pre klientov rôznych bánk a väčšia dôvera ako keby každý obchodník mal vlastný spôsob elektronických platieb. Niekedy tieto platobné systémy sú realizované samotnými bankami v rámci internet bankingu.

- **Platby pomocou elektronických peňazí** na rozdiel od predchádzajúcich riešení umožňujú zachovať anonymitu platcu. Záujemca si za normálne peniaze kúpi digitálne peniaze - balíček dát reprezentujúcich

peniaze. Pri platení zákazník presunie tieto peniaze na obchodníka (či už priamo, či len časť dát na základe protokolu), za ktoré si potom obchodník môže vybrať skutočné peniaze. Keďže skutočné peniaze nie sú viazané na osobu, strata týchto dát znamená stratu peňazí. V praxi sa tento prístup veľmi nepoužíva.

- **Platby pomocou elektronických šekov** je obdoba platieb klasickými šekmi. Platca elektronicky podpíše elektronickú podobu šeku. Spracovanie platby potom prebieha klasickým spôsobom.

Posledným spomínaným typom elektronického obchodu je elektronický obchod medzi vládou a občanom (G2C). Celkom dobre prepracovanou stránkou G2C je informovanie občana o zákonoch, jeho povinnostiach a právach, popis rôznych úkonov, zoznam a lokácia potrebných inštitúcií. Pomocou informačných portálov možno nájsť možnosti, ako sa zachovať v rôznych životných situáciách. Stránky vlády či konkrétnych štátnych inštitúcií umožňujú stiahnuť a v niektorých prípadoch aj podávať elektronické tlačivá. Následne je možné sledovať stav vybavenie, prípadne výsledok. V prípade finančných operácií sa aj v prípade G2C opäť dajú využiť platobné systémy. Pre právoplatnosť transakcií medzi občanom a orgánmi verejnej správy je niekedy nutné použitie právne podložených digitálnych podpisov (u nás sa nazýva zaručený elektronický podpis). Podobné vzťahy panujú aj medzi firmami a finančnými inštitúciami a vládou, kde je snaha o zavedenie elektronických procesov ako náhrada papierových z dôvodu zefektívnenia aj po stránke časovej aj finančnej.

V tejto kapitole sme ukázali troch základných účastníkov elektronického obchodu. Taktiež sme popísali typické príklady procesov bežiacich medzi nimi. Pri týchto obchodoch ide nielen o peniaze ale častokrát sa pri nich spracovávajú aj osobné údaje účastníkov. Aby bol človek ochotný používať systém pre elektronický obchod, musí mať záruky, že nepríjde o svoje peniaze ani nebudú zneužité údaje, ktoré poskytol systému. Dôvera v správne fungovanie týchto systémov sa zakladá na ich adekvátnom bezpečnostnom zaistení. Na bezpečnosť systémov elektronického obchodu sa pozrieme v nasledujúcich častiach.

Časť III

Bezpečnosť

Kapitola 3

Základy informačnej bezpečnosti

Použitie súkromných sietí pri proprietárnych systémoch umožňovalo prístup len vlastných zamestnancov, čo vylučovalo útok zvonku a za predpokladu korektného správania vlastných zamestnancov znamenalo relatívne vysokú úroveň bezpečnosti. Internet však nie je kontrolovaný jednou spoločnosťou a z toho dôvodu ho nepovažujeme za bezpečný. Pri elektronickom obchode sa cez internet prenášajú informácie, ktoré majú reálnu hodnotu a preto môžu byť záujmom potenciálnych útočníkov. Nutná podmienka dôvery účastníkov preto musí byť založená na bezpečnosti systémov elektronického obchodu.

V tejto časti povieme niečo o bezpečnosti ako takej a ako sa dosahuje. V tejto kapitole zavedieme základné pojmy z informačnej bezpečnosti.

IT produkty alebo systémy slúžia najmä na spracovávanie informácií. Vlastník týchto informácií očakáva, že tieto nebudú svojvoľne šírené ani modifikované. Tieto informácie alebo iné prostriedky, ktoré majú byť chránené sa nazývajú aj **aktíva**. Keď sa však pozeráme na systém, jeho fungovanie je ovplyvňované prostredím, v ktorom sa nachádza, a preto sa ním musíme zaoberať. Systém má plniť svoje ciele a napĺňanie týchto cieľov je dosahované procesmi, ktoré sa riadia určitými pravidlami. Potom potenciálna odchýlka od týchto pravidiel je **hrozba** pre tento systém.

Informačná bezpečnosť sa zaoberá práve chránením aktív pred hrozbami. Aktíva chránime najmä pred stratou dôvernosti, integrity alebo dostupnosti týchto aktív. V prípade ochrany osobných údajov hovoríme o zachovaní **súkromia**, vo všeobecnosti pod **dôvernosťou** rozumieme ochranu (ľubovoľných) informácií pred prezradením nechceným osobám. **Integrita** údajov znamená, že tieto údaje neboli zmenené (tj. okrem iného, že sú kompletné). U informáciách nás ešte môže zaujímať ich **autentickosť**,tj. či ich pôvod je

naozaj taký, ako sa predpokladá. Pri nakladaní s informáciami musíme overiť, či daný používateľ má právo vykonávať tieto akcie, či je **autorizovaný** na tieto činnosti. Overenie identity používateľa sa tiež nazýva **autentifikácia**.

Medzi hrozby môžme zaradiť chyby, zneužitie, krádeže, úmyselné poškodenia, počítačové útoky, záškodnícky kód (ako sú vírusy, červy a iné) či priemyselné a iné špionáže. Aj keď bezpečnosť kladie väčší dôraz na hrozby súvisiace so zlomyseľnou a inou ľudskou činnosťou, musí sa zaoberať aj inými hrozbami ako sú napríklad prírodné katastrofy, strata podpornej infraštruktúry, ktorá zahŕňa výpadky elektrickej energie, stratu konektivity ale aj dôvody, pre ktoré nebolo možné fyzicky zabezpečiť potrebné akcie zamestnancami (napríklad lokálna nedostupnosť kvôli prírodným podmienkam). Relevantné sú aj hrozby vyplývajúce z opotrebovania či poškodenia používaných súčastí.

Ochrana aktív je úlohou vlastníka, pretože za ne zodpovedá, spravuje ich a majú pre neho cenu. Pod cenou aktíva musíme chápať nielen priamu cenu (zväčša peňažnú), ale aj nepriamu cenu. Napríklad osobné údaje používateľov samé o sebe nemajú priamu merateľnú hodnotu, ale v prípade prezradenia týchto údajov to má negatívny vplyv na meno spoločnosti (nepriama cena). Vlastník aktív musí brániť tomu, aby nositeľ hrozby mohol využiť **zraniteľnosť** (tj. predpoklad pre naplnenie konkrétnej hrozby).

Vlastník aktív musí analyzovať možné hrozby vzhľadom na svoje prostredie. Výsledkom tohto skúmania je stanovenie **rizík**. Riziko je vlastne funkcia pravdepodobnosti nastatia hrozby a možného dopadu. Hodnotenie rizík nie je jednoduché. Už samostatné hodnotenie možného dopadu je zväčša problematické vyjadriť kvantitatívne, zvykne sa skôr používať skorej kvalitatívne hodnotenie rizík (na zvolenej stupnici).

Keďže nositeľ hrozby je schopný útoku využitím zraniteľností, je snaha vlastníka aktív tieto riziká eliminovať alebo aspoň znížiť na akceptovateľnú úroveň. Na to slúžia **protiopatrenia** (alebo opatrenia), ktoré majú redukovať riziká. Správa rizík sa skladá z dvoch primárnych aktivít: analýza rizík a zmierňovanie rizík. Okrem toho, že správa rizík sa snaží eliminovať riziká, musí to robiť efektívne vzhľadom na výdavky. Napríklad ako ochrana pred fyzickým útokom na server (snaha ukradnúť dáta) sa dá použiť najatie bezpečnostnej služby, ktorá by kontrolovala prístup do serverovne. Ale ak je riziko tohto útoku malé stačí napríklad obyčajné zamknutie s tým, že kľúče majú len oprávnené osoby. Keďže protiopatrenia zväčša neeliminujú všetky riziká v plnom rozsahu, zvyškové riziká by mali byť na akceptovateľnej úrovni a mali by sa pravidelne prehodnocovať.

Pri výbere opatrení treba dbať do úvahy rozličné faktory ako sú organizačné politiky, legislatívu a iné nariadenia, bezpečnosť, spoľahlivosť opatrení a iné kvalitatívne požiadavky, požiadavky na výkonnosť, presnosť a kompletnosť, počiatočné náklady, náklady na prevádzku, kultúrne obmedzenia a iné.

Protiopatrenia môžu byť rozličného charakteru: technické, organizačné, právne, logické, personálne a iné. Často sa jeden prostriedok dá zaradiť do viacerých kategórií. Medzi technické opatrenia patria rôzne technické prostriedky ako sú prístupové systémy, bezpečnostné dvere, klimatizácia (serverovní atď.), rozličné zariadenia ako firewall, zálohovacie zariadenia a podobne. Ďalším typom sú organizačné protiopatrenia. Tieto formou určitých organizačných politík, nariadení, postupov a príručiek určujú ako sa majú veci vykonávať. Napríklad keď už máme bezpečnostné dvere, tak by malo existovať nariadenie, že sa budú zamykať, keď majú slúžiť ako ochrana pred neoprávneným vstupom. Charakterom podobné sú právne opatrenia, ktoré napríklad stanovujú nutné protipožiarne opatrenia pre organizácie. Logické opatrenia slúžia najmä na obmedzenie logického prístupu (môže sa ísť aj o prístup k funkciám systému). Príkladom môžu byť definované prístupové práva k entitám systému alebo pravidlá firewallu. K personálnym opatreniam môžme zaradiť napríklad výber zamestnancov, ich tréning a vzdelávanie.

Viaceré z nich (najmä z oblasti technických a logických) využívajú kryptografické funkcie. Príkladom použitia môžu byť čipové alebo tzv. smart karty alebo použitie kryptografických funkcí na zabezpečenie dôvernosti alebo integrity. Preto sa v nasledujúcej kapitole pozrieme na základy kryptografie. Ukážeme ako kryptografia pomáha riešiť niektoré otázky informačnej bezpečnosti.

Kapitola 4

Kryptografia

Zaručenie súkromia a dôvernosti prenášaných a spracovávaných dát pri elektronickom obchodovaní je z hľadiska dôvery účastníkov a právnych požiadaviek kľúčovým predpokladom elektronického obchodu. Na riešenie týchto úloh sa používajú kryptografické prostriedky. Samotná kryptografia je veda zaoberajúca sa najmä udržaním tajnosti správ a zaručením autentickosti.

4.1 Kryptosystémy

Hlavným cieľom kryptografie je spoľahlivo preniesť medzi dvoma účastníkmi (zvyčajne označovanými ako Alica a Bob) tajnú správu cez nezabezpečený kanál. Pritom požadujeme, aby pasívny protivník nebol schopný zistiť skutočný obsah správy, alebo dokonca, aby ani aktívny oponent nebol schopný nepozorovane zmeniť či sfalšovať správu.

Nezašifrovaný text sa zvykne nazývať aj **otvorený text**. Pri šifrovaní sa zvolí **kľúč**, pomocou ktorého sa otvorený text transformuje na **šifrový text**. Šifrový text by mal byť potenciálnemu útočníkovi nezrozumiteľný, aby tento nebol schopný zistiť pôvodný otvorený text. Ďalej však požadujeme, aby legitímny príjemca bol schopný túto správu dešifrovať a tak určiť pôvodný otvorený text. Teda pre daný kľúč k a danú šifrovaciu funkciu e_k požadujeme, aby existovala v rozumnom čase vypočitateľná dešifrovacia funkcia d_k taká, aby pre všetky relevantné otvorené texty x platilo $d_k(e_k(x)) = x$. Takúto dvojicu funkcí zvykneme označovať ako **kryptosystém**.

Keď hovoríme o sile kryptosystémov, zvyknú sa používať dva pojmy: **výpočtovo bezpečný** kryptosystém a **bezpodmienečne bezpečný** kryp-

tosystém. Výpočtovo bezpečným kryptosystémom sa v praxi označuje taký systém, ak najlepšie známe algoritmy potrebujú na jeho prelomenie príliš veľa výpočtovej sily. Pod bezpodmienečne bezpečným kryptosystémom rozumieme taký systém, ak nemôže byť prelomený ani s neobmedzenou výpočtovou silou.

Z hľadiska vzťahu šifrovacej a dešifrovacej funkcie poznáme 3 základné druhy kryptosystémov: **symetrické**, **asymetrické** a tzv. **hybridné** kryptosystémy.

Symetrické kryptosystémy sú také kryptosystémy, kde sa na šifrovanie aj dešifrovanie používa ten istý kľúč. Dá sa povedať, že šifrovacie a dešifrovacie funkcie sú tvaru $e_k(x) = e(k, x)$ a $d_k(x) = d(k, x)$. Preto je zväčša ľahké zo šifrovacej funkcie ľahko určiť dešifrovaciu funkciu. Keďže na šifrovanie aj dešifrovanie sa používa ten istý kľúč, ten nesmie byť prezradený. Preto sa tieto systémy zvyknú nazývať aj systémy so tajným kľúčom.

Symetrické kryptosystémy sa podľa spôsobu šifrovania delia do dvoch hlavných skupín. **Blokové šifry** rozdelia text do blokov rovnakej dĺžky, ktoré sa postupne šifrujú. Existujú rôzne spôsoby akými tieto bloky na sebe závisia, pomocou čoho sa dá napríklad brániť proti zameneniu poradia týchto blokov. Iný prístup sa používa v **prúdových šifrách**. Pri prúdových šifrách sa v každom kroku vypočítava nový šifrovací kľúč (zväčša na základe inicializačného kľúča) a pomocou neho sa šifruje jeden znak otvoreného textu. Prúdové šifry sa výhodne používajú na šifrovanie údajov prichádzajúcich on-line.

26. novembra 2001 bol vybraný vo verejnej súťaži organizácie NIST (*National Institute of Standards and Technology*) symetrický systém AES (*Advanced Encryption Standard*) ako šifrovací algoritmus, ktorý možno používať na spoľahlivú ochranu elektronických dát [1] . Belgickí kryptológovia Joan Deamen a Vincent Rijmen vyvinuli tento algoritmus a jeho originálne meno je Rijndeal. V súťaži bol vybraný vďaka jeho dobrým hardvérovým výkonom a variabilite dĺžok kľúča.

Asymetrické kryptosystémy sú systémy, kde je výpočtovo neuskutočniteľné určiť dešifrovaciu funkciu d_k zo šifrovacej funkcie e_k. Na rozdiel od symetrických systémov sa šifrovacia funkcia môže zverejniť. Preto sa tieto systémy zvyknú nazývať aj systémy s verejným kľúčom. V prípade asymetrických kryptosystémov sa kľúč skladá z verejnej a súkromnej časti (napr.

[1] Pred systémom AES sa bežne používal ako štandardný blokový symetrický šifrovací systém DES, ktorý však bol rozlomený vďaka distribuovaným výpočtom na internete.

k_1 a k_2 po poradí) pričom je splnená podmienka, že je výpočtovo neuskutočniteľné určiť súkromnú časť z verejnej. Potom sa šifrovacie funkcie dajú zapísať vo forme $e_k(x) = e(k_1, x)$ a $d_k(x) = d(k_2, x)$.

Možnosť zverejniť šifrovaciu funkciu je výhoda oproti symetrickým systémom. Pri symetrických systémoch sa kľúč musel dohodnúť vopred alebo sa musí vymeniť zabezpečeným spôsobom. Pri asymetrických systémoch stačí zverejniť šifrovaciu funkciu a hocikto môže poslať správu, ktorú bude schopný dešifrovať len určený prijímateľ.

Bezpečnosť asymetrických kryptosystémov je založená vo všeobecnosti na výpočtovo zložitých problémoch. Asi najviac používaný kryptosystém je kryptosystém RSA. V roku 1977 ho vyvinuli Rivest, Shamir a Adleman. Kryptosystém RSA je založený na probléme faktorizácie veľkých čísel. Iný známy asymetrický kryptosystém je napríklad ElGamalov kryptosystém, ktorý je založený na probléme diskrétneho logaritmu pre konečné polia.

Hoci existujú bezpodmienečne bezpečné symetrické systémy (ako je napríklad Vernamova šifra), asymetrické systémy môžu byť iba výpočtovo bezpečné. S neobmedzenými výpočtovými prostriedkami sme schopní vyskúšať zašifrovať každý možný otvorený text, až kým nedostaneme daný šifrový text. Ďalšou výhodou symetrických systémov je ich výkon. Vo všeobecnosti sú rádovo rýchlejšie ako asymetrické systémy, keďže tie zväčša využívajú výpočtovo náročné matematické operácie. Hlavná výhoda asymetrických systémov už bola spomenutá - nie je potrebné dopredu dohodnúť kľúč. A navyše asymetrické systémy si vďaka svojim vlastnostiam našli uplatnenie aj v ďalších oblastiach kryptológie.

Hybridné kryptosystémy spájajú výhody oboch predchádzajúcich systémov. Využívajú rýchlosť šifrovania a dešifrovania symetrických systémov. Kľúč symetrickej šifry je (či už predtým, alebo potom) poslaný zašifrovaný pomocou asymetrického systému.

4.2 Podpisové schémy

V svete papierových dokumentov máme možnosť podpisovať rôzne dokumenty. Týmto spôsobom ukážeme to, že sme prinajmenšom oboznámení s obsahom dokumentu. Pri obchodovaní sa podpisujú zmluvy, ktoré sú potom záväzné pre podpísané strany. Takúto možnosť by sme potrebovali aj v elektronickom svete. Tu však narážame na niekoľko problémov, ktoré vo fyzickom svete nenastali. Vo fyzickom svete bola sila podpisov založená na

tom, že je ťažké sfalšovať podpis. V elektronickom svete vieme spraviť kópiu čohokoľvek a to tak, že nevieme rozlíšiť, čo je originál a čo je len kópia. Ďalším problémom je zabezpečiť spojenie medzi podpisom a dokumentom. V skutočnom svete máme podpis priamo na dokumente. Priamočiare pripojenie podpisu za elektronický dokument nepomôže, lebo ten môžme zobrať a nerozlíšiteľne pripojiť za iný dokument. To nás vedie k tomu, že elektronický podpis nemôže byť stále tá istá postupnosť bytov a musí byť závislý na podpisovanom dokumente. Riešenie vyššie uvedených problémov existuje a je založené na podpisových schémach.

Podpisová schéma pozostáva z podpisovacieho algoritmu a z overovacieho algoritmu, pomocou ktorého vieme overiť pravosť podpisu. Podpisujúci pomocou svojej inštancie podpisovacieho algoritmu sig_k podpíše dokument. Potom každý môže pomocou verejne známej príslušnej inštancie overovacieho algoritmu ver_k overiť, či podpis je platný pre daný dokument. Opäť sa vyžaduje, aby sa z overovacieho algoritmu nedalo v rozumnom čase zostrojiť podpisovací algoritmus.Vďaka tomu môžme veriť, že daný dokument bol naozaj podpísaný majiteľom inštancie podpisovacieho algoritmu prislúchajúceho k inštancií overovacieho algoritmu. Vzhľadom na povahu podpisových schém je opäť jasné, že podpisové schémy môžu byť len výpočtovo bezpečné a to z rovnakých dôvodov, ako boli spomínané pri asymetrických systémoch.

Podobné predpoklady na podpisové schémy nás vedú k myšlienke využiť asymetrické systémy pri podpisových schémach. V prípade, že šifrovacia aj dešifrovacia funkcia asymetrického systému sú bijekcie, môžme tieto použiť na vytvorenie podpisovacieho a overovacieho algoritmu nasledovným spôsobom:

$$sig_k(d) = d_k(d)$$

$$ver_k(d, s) = \text{platný} \iff e_k(s) = d$$

Takýmto spôsobom na kryptosystéme RSA je postavená RSA podpisová schéma, podobne existuje aj ElGamalova podpisová schéma.

Takýto prístup má však dve veľké nevýhody. Podpis je tak isto veľký ako podpisovaný dokument a asymetrické systémy sú relatívne pomalé. Riešením obidvoch týchto problémov je možnosť podpísať nie celý dokument, ale len jeho odtlačok, niečo malé, čo je úzko späté s dokumentom. Toto nám umožňujú **hašovacie funkcie**. Použitie hašovacích funkcí má ďalšiu výhodu, zabraňuje tzv. falšovaniu náhodnej správy [2] (*random message forgery*).

[2]Princíp je nasledovný: zoberieme ľubovoľný podpis a zostrojíme k nemu prislúchajúci

4.3 Hašovacie funkcie

Vo všeobecnosti slúžia hašovacie funkcie na vytváranie malých digitálnych odtlačkov z ľubovoľných dát.

Hašovacie funkcie majú viaceré možnosti využitia (napríklad aj použitie v dátových štruktúrach). Pre ich použitie pri podpisovaní digitálnych dokumentov však nemožno použiť hociaké hašovacie funkcie. Vhodné sú tzv. silné kryptografické hašovacie funkcie, ktoré by mali spĺňať nasledovné požiadavky: jednosmernosť, slabá a silná odolnosť voči kolíziam.

Hovoríme, že hašovacia funkcia h je slabo odolná voči kolíziam, ak pre danú správu x je výpočtovo neuskutočniteľné nájsť správu $x' \neq x$ takú, že $h(x') = h(x)$.

V prípade podpisovania táto požiadavka hovorí, že k danému podpísanému dokumentu je ťažké nájsť iný dokument, pre ktorý by takýto podpis bol tiež platný. V normálnom prípade je toto dostatočná podmienka, ale zvykne sa klásť ešte silnejšia podmienka.

Hovoríme, že hašovacia funkcia h je silno odolná voči kolíziam, ak je výpočtovo neuskutočniteľné nájsť správy x a x' také, že $x \neq x'$ a $h(x) = h(x')$.

Hovoríme, že hašovacia funkcia je jednosmerná, ak pre daný odtlačok z je výpočtovo neuskutočniteľné nájsť správu x takú, že $h(x) = z$.

Táto posledná vlastnosť hašovacích funkcí je užitočná napríklad proti falšovaniu náhodnej správy. Je jasné, že slabá odolnosť voči kolíziam vyplýva zo silnej odolnosti. Dá sa ukázať aj, že jednosmernosť je odvoditeľná zo silnej odolnosti, čiže pri hašovacej funkcí nám stačí skúmať jej silnú odolnosť voči kolíziam.

K známym hašovacím funkciám patrila ešte do nedávna používaná funkcia MD5, v ktorej však boli v roku 2004 nájdené vážnejšie chyby. Namiesto MD5 sa odporúčalo použiť funkciu SHA-1, v ktorej tiež už boli nájdené kolízie. Tieto však ešte neboli natoľko vážne a zatiaľ sa používa ďalej. V silnejších variantoch ako sú SHA-2, SHA-256,... sa zatiaľ nenašli kolízie, ale sú pochybnosti kvôli podobnosti návrhu so SHA-1.

Okrem použitia silných kryptografických hašovacích funkcií pri podpisoch, sa tieto zvyknú využívať aj pri kontrole integrity dát.

---

dokument pomocou šifrovacej funkcie. Takto získame platný podpis pre dokument, hoci nepoznáme dešifrovaciu funkciu. Získaný dokument vysoko pravdepodobne nebude nič zmysluplné, ale vrhá to zlé svetlo na danú podpisovú schému.

4.4 Certifikáty a časové pečiatky

Digitálne podpisy nám umožňujú veriť, že daný podpis vytvoril naozaj len ten, kto vlastní príslušnú inštanciu podpisovacieho algoritmu. Ale čo nás má presvedčiť, že konkrétna inštancia overovacieho algoritmu je naozaj zviazaná s konkrétnou identitou (osobou alebo aj spoločnosťou), ak sme ju nedostali priamo od danej osoby bezpečným spôsobom? Riešením tohto problému je **certifikát verejného kľúča**. Certifikát verejného kľúča je digitálny dokument, ktorý vydala dôveryhodná tretia strana (tiež označovanou ako certifikačná autorita - CA), a ktorý viaže verejný kľúč s konkrétnou identitou. Tento certifikát obsahuje najmä hodnotu verejného kľúča, identitu majiteľa príslušného verejného kľúča, kto ho vydal a je podpísaný certifikačnou autoritou, ktorá ho vydala. Keďže musí byť jasný aj spôsob, ako overiť podpis prislúchajúci k tomuto verejnému kľúču, tj. zväčša použitá hašovacia funkcia s presnými parametrami a použitý asymetrický systém, sú v certifikáte uvedené aj tieto údaje. Navyše je v certifikáte uvedená aj časová platnosť tohto certifikátu a adresa revokačného centra. Revokácia certifikátu znamená zneplatnenie certifikátu ešte počas jeho časovej platnosti v prípade kompromitácie súkromného kľúča. V tom prípade je tento zaradený do zoznamu revokovaných alebo zrušených certifikátov (*CRL - certificate revocation list*). Medzi najpoužívanejšie formáty certifikátov patrí X.509.

V skutočnom svete je založená dôvera k podpisom na možnosti odhaliť podvod - sfalšovanie. V digitálnom svete však bezpečnosť podpisov spočíva na utajení súkromného kľúča používaného na podpisovanie. V prípade jeho odhalenia už nemôžeme zaručiť právoplatnosť digitálnych podpisov vytvorených po kompromitácií súkromného kľúča. A tu sa dostávame k ďalšiemu špecifiku digitálneho sveta. V digitálnom svete potrebujeme vedieť, kedy daný dokument (alebo jeho podpis) vznikol. Z tohto prirodzene vyplýva potreba datovania dokumentov, na čo slúžia **časové pečiatky**. Časové pečiatky slúžia ako dôkaz, že daný dokument existoval v konkrétnom časovom okamihu.

Časová pečiatka je digitálny dokument, ktorého vydavateľ dosvedčuje existenciu datovaného dokumentu v danom čase. Jednou jednoduchou metódou je pripojiť nejaké verejné informácie, ktoré sa nedajú predpovedať (napr. hodnoty kurzu vybraných mien) (to znamená, že vytvorenie pečiatky nemohlo nastať skôr) a zároveň sa táto pečiatka zverejní napríklad v novinách (nemohlo to byť neskôr).

V praxi sa na riešenie problému presného datovania používajú časové pečiatky vydávané dôveryhodnou autoritou, ktorá garantuje korektnosť časových pečiatok. Vytváranie časových pečiatok prebieha nasledovným spôsobom. Zoberie sa odtlačok dokumentu, ku ktorému chceme vytvoriť časovú pečiatku. Tento sa doplní o časový údaj z referenčného zdroja certifikačnej autority a takto upravený odtlačok sa podpíše pomocou súkromného kľúča na tento účel určeného.

Keďže môže existovať viacero certifikačných autorít, aby bolo možné overovať aj digitálne podpisy klientov iných certifikačných autorít, je potrebné prepojiť izolované domény jednotlivých certifikačných autorít. Na to slúžia dve principiálne riešenia: krížová certifikácia (CA A vydá certifikát verejného kľúča CA B a opačne) a hierarchický model, kedy nadradená certifikačná autorita vydá certifikáty verejných kľúčov jej podriadených CA. Na vrchu tejto hierarchie je koreňová certifikačná autorita. Na Slovensku koreňová certifikačná autorita pre akreditované certifikačné autority je zo zákona pod správou NBÚ. Zahraničné certifikáty sú právne uznávané len na základe medzinárodných zmlúv alebo ak ich vydavateľ je uznaný ako akreditovaná certifikačná autorita na Slovensku.

4.5 Dohody kľúčov

Keď dvaja alebo viacerí účastníci chcú komunikovať cez nezabezpečený kanál, použitie asymetrického šifrovania nie je efektívne pre dlhšie správy. Rozumnú možnosť nám ponúka využitie efektívnejších symetrických kryptosystémov. Musíme zabezpečiť, aby všetci účastníci komunikácie dostali tajné kľúče, ktoré sa použijú pri šifrovaní. Principiálne, kľúče môžu byť v prípade **distribúcie kľúčov** určené jednou stranou a rozdistribuované medzi ostatných. Druhá možnosť je **dohoda kľúčov**, kde hodnoty kľúčov sú vytvorené na základe údajov viacerých strán. Úlohou týchto protokolov je dohodnúť sa na vhodných kľúčoch, pomocou ktorých následne bude prebiehať komunikácia, tak, aby nepovolaní nemohli určiť tieto kľúče. Niektoré protokoly sa vedia brániť len proti pasívnym oponentom. Ďalšie sa snažia brániť aj proti rôznym typom aktívnych útočníkov. Najbežnejšie typy útokov sú útok opakovaním, zmena údajov, vydávanie sa za iného účastníka, či útok útočník uprostred (*man in the middle*).

Na ilustráciu uvedieme jednoduchý protokol na dohodu kľúčov - **Diffie-Hellmanov protokol**. Jeho bezpečnosť je založená na Diffie-Hellmanovom

probléme, ktorý by sa dal formulovať nasledovne: V poli $\mathcal{Z}_p$ pre primitívny prvok α z hodnôt α^x a α^y vypočítať hodnotu $\alpha^{x.y}$ pre ľubovoľné x a y. Samotný protokol prebieha nasledovne. Komunikujúce strany A a B si náhodne zvolia hodnoty x_A a x_B (po poradí). Potom si navzájom pošlú vypočítané hodnoty $\alpha^{x_A} \mathrm{mod}\ p$ a $\alpha^{x_B} \mathrm{mod}\ p$. Obidve strany sú potom schopné vypočítať hodnotu $\alpha^{x_A.x_B} \mathrm{mod}\ p$, ktorá bude slúžiť ako kľúč.

Tento protokol však nie je odolný voči útoku typu útočník uprostred. Oponent O môže odchytiť správy od A a dokončiť protokol vydávajúc sa za B. Pritom sám inicializuje ďalšiu inštanciu protokolu s B vydávajúc sa za A. Keď A potom pošle zašifrovanú správu pre B, keďže protokol v skutočnosti prebehol medzi A a O, O je schopný rozšifrovať a preposlať B správu zašifrovanú kľúčom z inštancie protokolu medzi O a B. Možné riešenie tohto problému poskytujú certifikáty, ale existujú aj mnohé ďalšie protokoly na dohodu kľúča.

Príkladom zložitejších, bežne používaných kryptografických protokolov je SSL a jeho nasledovník TLS. Tieto protokoly využívajú rôzne kryptografické primitíva. Na overenie identity (aspoň strany servera) využívajú certifikáty. Potom sa pomocou asymetrických systémov dohodnú na kľúči, pomocou ktorého sa šifrujú prenášané údaje. Použité primitíva nie sú pevne určené, protokol SSL podporuje viaceré algoritmy napríklad asymetrického šifrovania.

Ako vidno, kryptografia nám poskytuje nástroje na vyriešenie mnohých problémov, ktoré vznikli snahou preniesť obchodovanie do digitálneho sveta. Častokrát sa spoliehame na výpočtovú bezpečnosť alebo dokonca na algoritmy, o ktorých sa predpokladá, že sú výpočtovo bezpečné (napr. zatiaľ nie je dokázaná ekvivalencia problému prelomenia RSA a problému faktorizácie). Preto treba sledovať vývoj kryptológie, lebo sa môžu objaviť slabiny používaných algoritmov.

V tejto kapitole sme ukázali riešenia čiastkových problémov bezpečnosti, v nasledujúcej kapitole sa už pozrieme na možný spôsob riešenia celkovej bezpečnosti systémov.

Kapitola 5

Ochrana IT systémov

Ako vieme, nutným predpokladom úspešného použitia systémov pre elektronický obchod je ich bezpečnosť. Zaručenie súkromia osobných údajov, dôvernosti prenášaných údajov, ale aj nutnosť autentickosti sú kľúčové prvky k nadobudnutiu dôvery používateľov IT systémov. Elektronický obchod však vo všeobecnosti prebieha v nekontrolovanom prostredí (zväčša Internet), čo môže viesť k narušeniu týchto požiadaviek. Použiteľné nástroje na riešenie hore uvedených problémov nám ponúka kryptografia. Otázkou, ako využiť kryptografické nástroje pri riešení bezpečnostných problémou, sa zaoberá informačná bezpečnosť. Informačná bezpečnosť je vlastne multidisciplinárna oblasť zaoberajúca sa analýzou systémov, hľadaním zdrojov ich potenciálneho ohrozenia a návrhom opatrení na elimináciu hrozieb alebo aspoň redukciu rizika z nich vyplývajúcich, ktorá okrem kryptografie zahrňuje aj organizačné, personálne a iné aspekty bezpečnosti.

Problémov týkajúcich sa bezpečnosti je veľa, sú rozličného charakteru (nedostatočné technické zabezpečenie, prílišné právomoci používateľov, chyby v systéme) i pôvodu (útočník zvonku, sprenevera, chyby používateľov, prírodné udalosti). Často tieto problémy sú zložité alebo ťažko identifikovateľné.

Zložitosť a rozmanitosť problémov týkajúcich sa bezpečnosti nás vedie k poznaniu nasledovnej skutočnosti. Zaistiť bezpečnosť nejakého systému nemožno na základe subjektívnych pocitov a ad-hoc skúmania systému. Skúmanie systému musí mať objektívne hodnotiace kritéria. Sú potrebné objektívne kritéria pokrývajúce všetky aspekty bezpečnosti. Bezpečnostná analýza systému musí byť čo najviac objektívna a subjektívne prvky potlačené (Dvaja skúsení analytici by mali pri analýze systému dospieť nezávisle k tým

istým záverom). Dobrou praxou je potom vykonanie hodnotenia nezávislými osobami (nie nutne externými). Vyššiu úroveň spoľahlivosti skúmania je možné dosiahnuť nezávislým auditom spoločnosťou na to špecializovanou alebo až vykonaním certifikácie systému. Výsledkom analýzy bezpečnosti systému je potom ohodnotenie rizík a návrh opatrení na elimináciu, resp. aspoň zníženie rizík na prijateľnú úroveň.

Dodatočné zabezpečovanie existujúcich IT systémov je drahé a málo efektívne. Ak už pri návrhu týchto systémov nebolo prihliadané na bezpečnosť, snaha o zabezpečenie IT systému môže viesť k náročným zmenám tohto systému. Navyše sa zvyšuje pravdepodobnosť chýb a chybnej implementácie bezpečnostných funckií, ktoré môžu vyplývať aj z chýbajúcej alebo nepresnej dokumentácie. Preto je výhodnejšie dbať na otázku bezpečnosti počas celého životného cyklu systému už od fázy zbierania požiadaviek a návrhu.

Preto vývoj bezpečných systémov by mal štandardne začať analýzou bezpečnostných aspektov systému. Toto zahŕňa stanovenie bezpečnostného prostredia, v ktorom sa systém plánuje používať a analýzu rizík. Následný návrh a implementácia by mala zohľadňovať bezpečnostné požiadavky vyplývajúce z týchto analýz. Prirodzené je použitie certifikovaných komponentov (napríklad certifikované kryptografické moduly a pod.). Ohľad na bezpečnosť sa musí brať aj pri zvyšných fázach životného cyklu systému. Pravidelný audit a prehodnocovanie bezpečnostných politík vo svetle nových informácií je nutné počas prevádzky systému.

Základ pre takýto prístup poskytuje štandard **Common Criteria (CC**, [4]) a ďalšie štandardy z nich vychádzajúce. CC majú slúžiť ako základ pre vyhodnocovanie bezpečnostných vlastností IT produktov a systémov. Vybudovaním všeobecných kritérií je možné porovnávanie výsledkov nezávislých bezpečnostných skúmaní. Taktiež obsahuje všeobecnú množinu požiadaviek pre bezpečnostné funkcie IT produktov a systémov.

Štandard CC vznikol iniciatívou ujednotiť dovtedy existujúce štandardy ako výsledok spolupráce siedmich vládnych organizácií. V máji 1998 bola vydaná verzia CC 2.0, ktorá s malými zmenami bola adaptovaná ako štandard ISO/IEC 15408.

Aj keď CC slúžia na vyhodnocovanie bezpečnosti, je možné ich použiť aj už pri navrhovaní a vývoji IT produktov a systémov prihliadaním na možné budúce vyhodnocovacie postupy a identifikovaním bezpečnostných požiadaviek. CC je možné síce uplatňovať na hotové systémy, ale je to možné aj na navrhované - zovšeobecnené systémy vo forme bezpečnostných modelov. V CC sú tieto označované ako **profil ochrany** (PP - *protection profile*). PP je

implementačne nezávislá množina bezpečnostných požiadaviek pre kategóriu vyhodnocovaných systémov, ktoré spĺňajú špecifické potreby zákazníka. PP slúži ako rámec pre množinu podobných systémov. Pri vyhodnocovaní konkrétneho systému (v CC označovaného ako TOE - *target of evaluation*) sa zostrojuje bezpečnostný zámer (ST - *security target*), ktorý predstavuje množinu bezpečnostných požiadaviek a špecifikácií, ktoré majú slúžiť ako základ vyhodnocovania identifikovaného TOE.

Samotný štandard CC je rozdelený do troch častí:

1. **Úvod a všeobecný model**
   Definuje všeobecný koncept a princípy vyhodnocovania informačnej bezpečnosti. Taktiež uvádza konštrukcie pre vyjadrenie informačných bezpečnostných cieľov, definovanie bezpečnostných požiadaviek a pre popis hrubej špecifikácie.

2. **Funkčné bezpečnostné požiadavky** Stanovuje množinu funkčných komponentov ako základ pre vyjadrenie funkčných požiadaviek na TOE. Časť 2 tieto komponenty katalogizuje do množín rodín a tried.

3. **Požiadavky na bezpečnostné záruky** Stanovuje množinu komponent záruk ako štandardný spôsob vyjadrenia požiadaviek na záruky pre TOE. Časť 3 tieto komponenty katalogizuje do množín rodín a tried. Taktiež definuje kritéria pre vyhodnocovanie PP a ST a uvádza úrovne záruk, ktoré predstavujú preddefinovanú stupnicu pre hodnotenie úrovne záruk TOE. Tieto úrovne sa označujú ako EAL (*Evaluation Assurance Level*).

Vyhodnocovanie PP alebo ST sa uskutočňuje na základe vyhodnocovacích kritérií profilu ochrany alebo bezpečnostného zámeru z CC časti 3. Cieľom tohto vyhodnocovania je ukázať úplnosť, konzistentnosť a technickú realizovateľnosť a vhodnosť pre príslušné TOE. Ak ST má vyhovovať nejakému PP, treba ukázať, že ST spĺňa všetky požiadavky PP.

Pri popise IT systémov pre elektronický obchod budeme tieto skúmať z hľadiska bezpečnosti práve vo forme PP. Využitie PP sa dá použiť pre následnú konštrukciu konkrétnych ST pri skúmaní konkrétnych systémov - TOE. Navyše na základe vyhodnocovania PP sa tieto dajú katalogizovať pre ich následné opätovné použitie.

5.1 Štruktúra profilu ochrany

Teraz popíšeme štruktúru PP. Podľa CC má PP nasledovné časti:

- Úvod k PP
  - Identifikácia PP
  - Prehľad PP
- Popis TOE
- Bezpečnostné prostredie TOE
  - Predpoklady
  - Hrozby
  - Organizačné bezpečnostné politiky
- Bezpečnostné ciele
  - Bezpečnostné ciele pre TOE
  - Bezpečnostné ciele pre prostredie
- Bezpečnostné požiadavky
  - Bezpečnostné požiadavky pre TOE
    - Funkčné požiadavky pre TOE
    - Bezpečnostné záruky pre TOE
  - Bezpečnostné požiadavky pre prostredie
- Poznámky k použitiu
- Zdôvodnenie
  - Zdôvodnenie bezpečnostných cieľov
  - Zdôvodnenie bezpečnostných požiadaviek

Úvod k PP obsahuje prehľad a informácie o dokumente potrebné k zaradeniu do zoznamu PP, pričom identifikácia PP obsahuje jeho identifikáciu a popisné informácie pre identifikáciu, katalogizáciu, registráciu a referencie. Prehľad PP ho sumarizuje voľným textom. Prehľad by mal byť natoľko podrobný, aby mohol slúžiť ako samostatný abstrakt.

Popis TOE popisuje typ produktu a všeobecné IT vlastnosti TOE potrebné na pochopenie jeho bezpečnostných požiadaviek. Poskytuje kontext pre vyhodnocovanie pri odhaľovaní nekonzistentností. Keďže PP sa normálne nezmieňuje o špecifickej implementácií, popisované vlastnosti TOE možno uvádzať ako predpoklady.

Bezpečnostné prostredie TOE obsahuje tvrdenia o bezpečnostných okolnostiach prostredia, v ktorom je zamýšľané použiť TOE. Tieto tvrdenia zahŕňajú:

- Popis predpokladov na prostredie, v ktorom sa TOE zamýšľa použiť. Tieto predpoklady obsahujú informácie o plánovanom použití TOE, potenciálne hodnoty aktív, možné ohraničenia použitia, ako aj popis fyzických, personálnych aspektov prostredia a možností pripojenia.

- Popis všetkých hrozieb voči aktívam proti ktorým je nutná špecifická ochrana v rámci TOE alebo jeho prostredií. Samozrejme nemajú tu byť vymenované všetky možné hrozby , len tie, ktoré sú relevantné pre bezpečné fungovanie TOE.
  V prípade, že bezpečnostné ciele sú odvodené len z predpokladov a organizačných bezpečnostných politík, časť o hrozbách možno vynechať.

- Popis organizačných bezpečnostných politík, ktoré sú potrebné pre používanie TOE. Ak je to nutné pre jasné pochopenie bezpečnostných cieľov, PP môže obsahovať aj vysvetlenie týchto politík.
  V prípade, že bezpečnostné ciele sú odvodené len z predpokladov a hrozieb, časť o organizačných bezpečnostných politikách možno vynechať.

Bezpečnostné ciele pre TOE a jeho prostredie určujú všetky aspekty identifikované pre bezpečnostné prostredie. Bezpečnostné ciele majú čeliť všetkým identifikovaným hrozbám a pokrývať všetky identifikované predpoklady a organizačné bezpečnostné politiky. V prípade, že hrozba alebo organizačná bezpečnostná politika je čiastočne pokrytá pomocou TOE a čiastočne jeho prostredím, potom súvisiace bezpečnostné ciele sa opakujú v obidvoch častiach.

Časť PP o **bezpečnostných požiadavkách** popisuje podrobné IT bezpečnostné požiadavky, ktoré majú byť naplnené pomocou TOE alebo jeho prostredím. Táto časť obsahuje nasledujúce tvrdenia:

- Tvrdenia o bezpečnostných požiadavkách pre TOE definujú funkčné požiadavky a bezpečnostné záruky, ktoré sú potrebné na naplnenie bezpečnostných cieľov TOE.
  - Tvrdenia o funkčných požiadavkách pre TOE definujú funkčné požiadavky pre TOE ako funkčné komponenty z CC časti 2 kde je to použiteľné.
  - Tvrdenia o bezpečnostných zárukách pre TOE uvádzajú bezpečnostné záruky pre TOE zvolenej EAL voliteľne rozšírenej o komponenty záruk z CC časti 3. PP môže byť rozšírený aj o ďalšie explicitne stanovené bezpečnostné záruky.
- Voliteľné tvrdenia o bezpečnostných požiadavkách pre prostredie identifikujú IT bezpečnostné požiadavky pre IT prostredie TOE.
  Aj keď bezpečnostné požiadavky pre nie-IT prostredie sú často v praxi veľmi užitočné, nie sú nutnou súčasťou PP, keďže sa nevzťahujú na implementáciu TOE.

Časť **poznámky k použitiu** je voliteľná a môže obsahovať dodatočné informácie, ktoré sú relevantné alebo užitočné pre konštrukciu, vyhodnocovanie alebo použitie TOE.

Časť **zdôvodnenie** uvádza dôkaz použitý pri vyhodnocovaní PP. Tento dôkaz podporuje tvrdenia o úplnosti PP a o dostatočnosti protiopatrení. Táto časť obsahuje:

- Zdôvodnenie bezpečnostných cieľov má ukázať, že uvedené bezpečnostné ciele sú odvoditeľné z všetkých aspektov bezpečnostného prostredia TOE a sú vhodné na ich pokrytie.
- Zdôvodnenie bezpečnostných požiadaviek má ukázať, že bezpečnostné požiadavky spĺňajú a sú odvoditeľné z bezpečnostné ciele.

V tejto časti sme zdôvodnili potrebu komplexného pohľadu na bezpečnosť systémov. Snaha o objektívne vyhodnotenie bezpečnosti systému nás doviedla k štandardu CC a k použitiu profilov ochrany (PP) ako možného

bezpečnostného modelu. Vyhovuje nám všeobecnosť PP a ich možné znovupoužitie pre podobné systémy elektronického obchodu. V nasledujúcich častiach sa pozrieme už na konkrétny PP pre systémy elektronického obchodu.

Časť IV

Funkcionálne a bezpečnostné požiadavky

Kapitola 6

Model systému

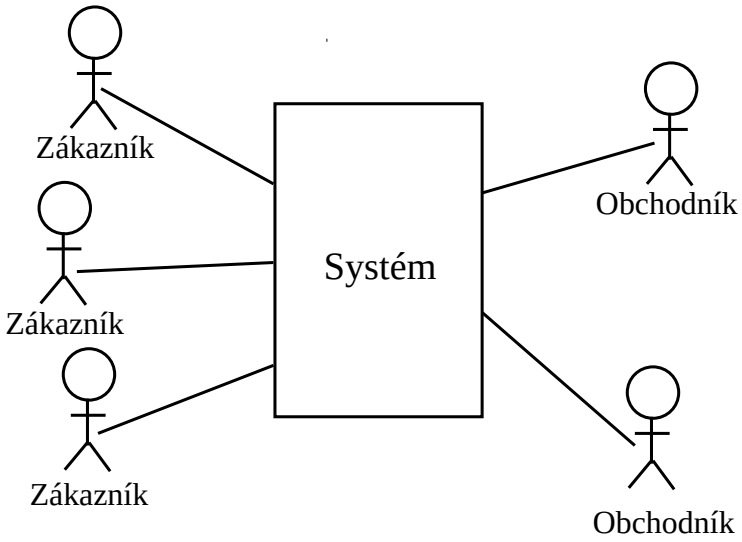
V tejto kapitole stanovíme špecifickú triedu systémov pre elektronický obchod, pre ktorú následne vypracujeme PP.

Trieda systémov pre elektronický obchod je naozaj veľmi široká. Keďže elektronický obchod typu B2B sám o sebe je dosť rozmanitý, zahŕňa mnoho procesov, o ktorých častokrát sa ani nehovorí verejne a môžu byť súčasťou obchodného tajomstva. Navyše B2B systémy fungujú už dlhšie a zvyknú byť založené na starých systémoch, preto tam nie je až taký predpoklad budovania nových systémov.

Spolu s rozvojom internetu sa začala rozvíjať oblasť B2C obchodov. O tejto oblasti aj máme lepšie znalosti. Preto zvolíme model z oblasti B2C obchodov.

Elektronický obchod typu B2C je vo väčšine obmedzovaný vhľadom na predpoklady na strane zákazníka. Ten väčšinou chce obchodovať priamo, bez nutnosti inštalovať nákladné zariadenie a používať zložitý softvér. To vedie k použitiu tenkých klientov. Tento jav badať aj v praxi, kde väčšina systémov elektronického obchodu je tvorená webovým alebo iným serverom a ako tenký klient slúži internetový prehliadač.

K účastníkom nášho systému budú teda patriť koncoví zákazníci. Na zákazníkov však musíme položiť aj nejaké požiadavky. Náš systém by nemal dovoľovať zneužívanie zákazníkmi napríklad tým, že si objednajú tovar a potom odmietnu zaplatiť. Použitie zaručeného elektronického podpisu, ktorý by síce objednávke dal právnu váhu, však nie je veľmi realistické kvôli malému počtu potenciálnych zákazníkov, ktorí majú možnosti zaručeného elektronického podpisu. Rozumnou možnosťou je uzavretie dohody medzi obchodníkom a potenciálnym zákazníkom napríklad popri registrácií zákaz-



Obrázok 6.1: Vzťah k systému

níka. Použitie registrácie skutočne nachádzame aj v praxi. Ďalšou možnosťou je použitie platobných systémov, pomocou ktorých sa dá vykonať platba na účet obchodníka ešte pred poskytnutím služby či dodaním tovaru.

Prirodzene nás musí zaujímať aj ochrana zákazníka. Tu sme však chránení zákonmi SR a ustanoveniami Európskej únie. Podľa zákona č.22/2004 musí obchodník trvalo, presne a jednoznačne informovať o svojej organizácií, ako aj podmienkach objednávky. Navyše musí vytvoriť také podmienky, ktoré umožnia zistiť a opraviť chyby zákazníkových úkonov pred odoslaním objednávky. Podľa smernice EU 97/7/EC má zákazník právo do 7 pracovných dní odstúpiť od zmluvy bez akýchkoľvek poplatkov. A v prípade nedodržania zmluvy zo strany obchodníka, má zákazník právo na odškodnenie. Ak nie je dohodnuté inak, zmluva na diaľku musí byť splnená do 30 dní od objednávky.

Druhým účastníkom nášho systému budú obchodníci. Môže ísť o jedného obchodníka, ktorý môže sám prevádzkovať systém, alebo skupina obchodníkov, ktorá spolu chce poskytovať svoje služby zákazníkom. Možnosťou je aj prevádzkovanie systému špecializovanou spoločnosťou, ktorá umožňuje predávať iným obchodníkom ich služby alebo produkty. Kvôli všeobecnosti budeme uvažovať túto možnosť.

Pozrieme sa na služby, ktoré tento systém môže ponúknuť. Tieto rozdelíme podľa miery digitalizácie prebiehajúcich procesov na tri druhy: informačné, komunikačné a transakčné.

6.1 Informačné služby

Systém bude uchovávať potrebné informácie a tieto poskytovať zákazníkom. Tieto informácie môžu byť interaktívne (napríklad získané vyhľadávaním podľa určitých kritérií) alebo dokonca aj personifikované (špecifické pre konkrétneho používateľa). Tieto informácie sa však akýmsi spôsobom musia dostať do systému. Z pohľadu obchodníka, systém obsahuje dva druhy informácií: stálejšie informácie, kde prezentuje svoju spoločnosť ako takú (kontakty, adresy, zameranie spoločnosti a iné) a informácie, ktoré vyžadujú častejšiu aktualizáciu . K takýmto informáciám patrí napríklad aktuálna ponuka a iné informácie o tovaroch alebo službách. Keďže obchodník sa nebude chcieť zaoberať tvorbou webových (predpokladaná forma prezentácie) stránok, upravovanie týchto informácií prenecháme na operátorov systému na základe podkladov od obchodníka. Pri obchodných informáciách nám ide najmä o zachovanie integritu a zaručenie autentickosti. Pre prípad chybného obsahu, či už z dôvodu chyby alebo útoku, by mala byť možnosť tento obsah rázne zablokovať napríklad formou hotline.

Za obsah bude zodpovedať obchodník. Zodpovednosť obchodníka musí byť upravená pomocou uzatvorenej zmluvy medzi obchodníkom a poskytovateľom systému. Poskytované informácie musia byť v súlade s legislatívou. Poskytovateľ systému má síce možnosť zistiť a obmedziť zjavné porušenia zákonov (napríklad propagovanie fašizmu), ale už ťažko by sa zisťovalo, či niektoré poskytované informácie sú v súlade s pravdou (viď napr. zákon č.22/2004). Navyše sa redukujú hrozby, ktoré by vyplývali z možnosti priameho menenia informácií obchodníkom. Ďalej je vhodné zaznamenávať komunikáciu od obchodníka (s dôrazom na integritu, autentickosť a čas) kvôli možným obvineniam zo strany obchodníka (napríklad žaloba za ušlý zisk kvôli "oneskoreniu" aktualizácie informácií, prípadne pre poskytovanie zlých informácií).

Ďalšou možnou informačnou službou je napríklad poskytovanie rôznych štatistík prístupov k poskytovaným informáciám. Pre rôzne marketingové účely môže byť zaujímavé vedieť, v akých časoch si ľudia pozerali informácie, ktoré informácie boli pre nich zaujímavejšie a podobné štatistiky. Prípadne

môže ísť aj o sofistikovanejšie štatistiky ako napríklad ponúka Amazon - odporúčanie ďalších kníh ku knihe na základe toho, že si ich zvyknú kupovať zákazníci, ktorý si kúpili aj danú konkrétnu knihu.

6.2 Komunikačné služby

Pri komunikačných službách už prebieha istá forma komunikácie medzi účastníkmi, nejde len o jednostranné podávanie informácií.

Pri uvažovaní komunikačných služieb už vystáva otázka autorizácie. Tento problém sa objavil už pri dodávaní podkladov obchodníkmi. Jednu možnosť ponúka PKI a využitie certifikátov. Riešenie založené na PKI pomáha zároveň riešiť otázku autentickosti ale aj otázku integrity dát. Toto riešenie však nemusí byť akceptovaná všetkými, najmä medzi zákazníkmi. Alternatívu ponúka používanie hesiel alebo PIN čísel. Pre zaručenie autentickosti potrebujeme spojiť takúto identifikačnú informáciu (PIN, heslo, ...) s konkrétnou identitou, čo môže byť napríklad pri podpise zmluvy s obchodníkom. V prípade registrácie zákazníkov cez internet zväčša nemôžeme priamo overiť totožnosť, máme len istú formu slabšej autentifikácie, pri ktorej vieme povedať, že ide o jednu identitu, ale informáciu o totožnosti máme len neoverenú. To sa rieši právnou cestou, v podmienkach registrácie býva klauzula o pravosti vyplnených údajov.

V najjednoduchšej podobe komunikácia môže prebiehať mimo systém len pomocou zverejnenia kontaktov. Systém však môže poskytovať aj vlastné komunikačné služby. Príkladom môžu byť aj rôzne formy dotazníkov, možnosť kontaktu podpory obchodníka či samotného systému, prípadne aj iná komunikácia najmä medzi zákazníkom a obchodníkom. Riešenie problému integrity a dôvernosti prenášaných správ bude systém riešiť použitím štandardných prostriedkov (použitie PKI, SSL, ...). Príkladom môžu byť elektronické podoby kníh prianí a sťažností, dotazníky, rôzne užívateľské fóra (napr. diskusia k tovaru) a iné.

Keďže systém vystupuje ako prostredník - dôveryhodná tretia strana, môže v prípade sporu potvrdiť prenos správy (samozrejme správ poslaných pomocou systému). Systém nepotrebuje odkladať samotné správy (tieto správy môžu byť aj zašifrované), stačí odložiť odtlačok správy spolu s ďalšími potrebnými údajmi ako odosielateľ, prijímateľ a čas prenosu vo forme časovej pečiatky. Ide vlastne o akúsi formu elektronického notára v obmedzenej podobe. Táto služba by sa už mohla možno zaradiť aj k transakčným službám,

keďže nie je striktne definovaná hranica medzi komunikačnými a transakčnými službami.

6.3 Transakčné služby

Základnou úlohou transakčných služieb je uskutočnenie obchodu medzi zákazníkom a obchodníkom. V prípade klasického predaja produktov (tovarov alebo služieb), kde sú dopredu jasne dané podmienky predaja, si zákazník má možnosť vybrať tovar pomocou istej formy nákupných košíkov. V závislosti na druhu produktu a na type zákazníka (najmä ide o to, akou formou je uzatvorená dohoda so zákazníkom - či ide o slabšiu formu autentifikácie, či ide o stáleho zákazníka ap.) je možnosť vyžadovať platbu vopred pomocou platobného systému.

Vo všeobecnejšom prípade je možné stanoviť konkrétne podmienky kontraktov na základe dohody. Stanovovanie tejto dohody môže prebiehať pomocou komunikačných služieb systému, prípadne aj mimo systém. Po uzavretí dohody je možnosť túto registrovať v systéme pre prípadné neskoršie overenie (tým istým systémom ako pri správach).

Kvôli právnej ochrane prevádzkovateľa systému je nutné mať dobre stanovené právne podmienky najmä voči obchodníkom pri uzatváraní zmluvy. Keďže systém je prostredník medzi zákazníkom a obchodníkom, musí byť dostatočne jasne stanovené, ktoré povinnosti sa prenášajú na obchodníka a v akej podobe. Zákazník by mal byť tiež oboznámený s podmienkami využívania služieb pri registrácií.

Doteraz sme sa zaoberali očakávanou funkčnosťou systémy, teraz aspoň naznačíme, aké hrozby sú relevantné pre tento systém. Základným aktívom, čo chceme chrániť, sú samozrejme informácie. Jednak ide o obchodné informácie obchodníkov, ale ide aj o osobné informácie, ktoré sú uložené v systéme (uskutočňované alebo uskutočnené objednávky, adresy doručenia a iné).

K tomuto aktívu sa viažu aj základné hrozby - hrozby týkajúce sa porušenia integrity, autentickosti, súkromia a dôvernosti ako pri uchovávaní týchto informácií ale aj pri ich prenose. Keďže autorizovaní používatelia môžu získať prístup k niektorým z neverejných dát, je nutné sa brániť voči falošnej autentifikácií. Taktiež očakávame od systému, že sa bude schopný priradiť zodpovednosť konkrétnej identite za akcie, ktoré by mohli viesť k zneužitiu systému.

V tejto časti sme popísali model systému, pre ktorý v nasledujúcej časti zostrojíme profil ochrany.

Kapitola 7

Profil ochrany

Táto časť obsahuje samotný profil ochrany (PP) pre systém elektronického systému typu B2C.

V tomto a aj inom texte sú používané pojmy a skratky, ktorých vysvetlenie sa dá nájsť v dodatku A.

7.1 Úvod k PP

7.1.1 Identifikácia PP

Názov:	PP pre systém elektronického systému typu B2C
Úroveň záruk:	EAL 3
Súlad s CC:	v súlade s časťou 2 aj 3
Registrácia:	-
Kľúčové slová:	elektronický obchod

7.1.2 Prehľad PP

Tento PP popisuje základné bezpečnostné požiadavky pre B2C systém, ktorý umožňuje uskutočňovanie objednávok formou elektronického obchodu. Tento systém umožňuje zverejňovať ponuky a iné informácie spoločnosti pre viacerých obchodníkov. Tieto informácie budú zadávané a aktualizovane pomocou autorizovaných operátorov systému na základe podkladov.

7.2 Popis TOE

Neformálny popis TOE sa u nachádza v kapitole 6. Nebudeme ho celý prepisovať, len trochu formálnejšie popíšeme účastníkov a fungovanie systému.

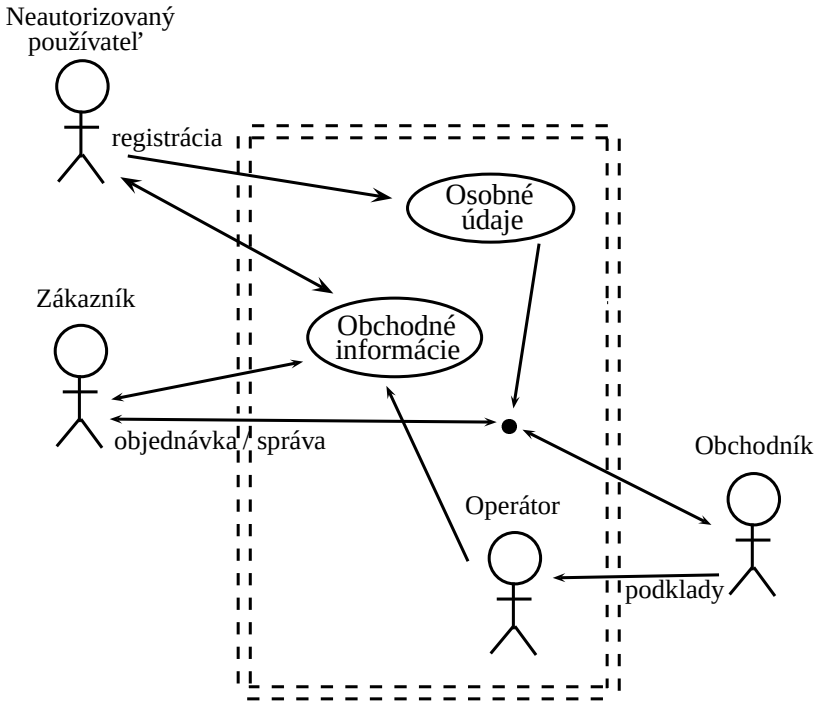
Základný model systému je vzťah viacerých zákazníkov a viacerých obchodníkov pomocou servera ako prostredníka, ako už bolo načrtnuté na obrázku 6.1. Aktérov systému môžme rozčleniť primárne na neautentifikovaných a autentifikovaných. Týchto autentifikovaných môžme ďalej deliť nasledovne:

- bežní používatelia
  - zákazníci
  - obchodníci
- privilegovaní používatelia
  - administrátori
  - operátori
  - auditori

Neautorizovaní používatelia majú možnosť len si prezerať obchodné informácie. Úplne nový používateľ má možnosť sa registrovať, kde sa o ňom uložia aspoň základné osobné údaje (identita, spôsob autorizácie, ...). Po prihlásení sa do systému ako zákazník si môžu vybrať tovar a na základe tovaru sa vytvorí objednávka, ktorá sa pošle obchodníkovi. Potrebné osobné údaje sa doplnia buď na základe uložených osobných informácií alebo musia byť zadané ako detaily transakcie priamo od zákazníka (napríklad chce doručiť tovar nie na domácu adresu). Voliteľne (v závislosti od voľby obchodníka a zákazníka) môže na dokončenie transakcie prebehnúť ešte aj platba pomocou platobného systému. Odtlačok (obsahuje časovú pečiatku a iné potrebné metadata) objednávky sa uloží pomocou elektronického archívu. Potvrdenie platby (ak bola vykonaná) už musí zabezpečiť daný platobný systém.

Zákazníci a obchodníci si môžu posielať aj správy pomocou systému. Pomocou nich si môžu dohodnúť zmluvu, ak nejde o prípad typizovaných produktov. Aj v tomto prípade systém vie odkladať odtlačky týchto správ. Posielanie správ je možné len známym účastníkom, systém v prípade rozposielania spamu má možnosť túto službu zamietnuť.

Obchodník má možnosť ovplyvniť obchodné informácie tým, že systému dodá podklady pre tieto informácie. Na základe týchto informácií operátor



Obrázok 7.1: Základné funkcie systému

systému modifikuje obchodné informácie. Operátor okrem menenia obchodných informácií má možnosť tieto dočasne zablokovať zákazníkom na základe podnetu obchodníka.

Úlohou administrátora je priraďiť používateľov do jednotlivých rolí, prípadne pozastaviť platnosť alebo len deaktivať niektoré funkcie. Navyše spravuje funkcie systému ako sú štart alebo zastavenie systému a konfigurácia bezpečnostných nastavení systému.

Systém bude auditovať relevantné udalosti. Pomocou analýzy týchto auditovacích záznamov je možnosť odhaliť možné pokusy o nekalú činnosť ako aj možné zraniteľnosti systému. V prípade bezpečnostných (ale aj iných) incidentov taktiež môžu viesť k zisteniu zodpovednosti a skúmaním vzniku tohto incidentu odhaliť príčinu. Prezeraním auditovacích záznamov sa zaoberajú auditori. Okrem toho v prípade potreby zálohujú staré auditovacie záznamy (toto bude dovolené až po uplynutí určitej dobe, aby nebolo možné hneď odstrániť aktuálne auditovacie záznamy).

7.3 Bezpečnostné prostredie TOE

Hlavným aktívom TOE sú informácie obsiahnuté v systéme. Okrem týchto obchodných informácií a osobných údajov je potrebné chrániť korektnosť bezpečnostných nastavení systému.

7.3.1 Predpoklady

A1.Súlad s legislatívou TOE bude používané v súlade s legislatívou a právne chránené pred zneužitím zmluvnými partnermi.
TOE nebude zverejňovať zjavne protizákonným obsah a podmienky spolupráce s obchodníkmi a zákazníkmi sú jasne upravené tak, aby ani jedna strana sa nezbavila svojej zodpovednosti v neprospech prevádzkovateľa TOE.

A2.Platobný systém Spoľahlivé použitie platobného systému.
TOE bude môcť využívať platobný systém za predpokladov zachovania dôvernosti, autentickosti a integrity prenášaných údajov.

A3.Externé služby Spoľahlivé využívanie služieb CA, elektronického archívu a časových pečiatok.
TOE bude môcť pomocou nich využívať a overovať certifikáty, vytvárať časové pečiatky a bezpečne uskladniť potrebné informácie použiteľné pri preukazovaní určitých skutočností.

A4.Fyzická ochrana TOE je dostatočne fyzicky chránené.
Fyzický prístup k TOE je dostatočne zabezpečený voči útočníkom ako aj prípadným iným nebezpečenstvám, ako je napríklad požiar.

A5.Žiadne utajované skutočnosti TOE nie je určené na spracovávanie utajovaných skutočností.
TOE nebude spracovávať údaje podliehajúce ochrane utajovaných skutočností podľa zákona č.215/2004 Z.z. v znení neskorších predpisov.

A6.Použitie osobných údajov TOE využíva len najnutnejšie osobné údaje.
TOE nebude používať osobité kategórie osobných údajov podliehajúce ochrane podľa zákona č. 363/2005 Z.z. ako sú etnický pôvod a pod. Používané údaje bude používať len na určenú ciele a nebude ich poskytovať iným stranám.

A7.Stredná hrozba odhalenia zraniteľností Hrozba útokov na odhalenie zraniteľností je nanajvýš na strednej úrovni.
Pri vyššej hrozbe útokov na odhalenie zraniteľností by bolo nutné použitie vyššej úrovne bezpečnostných záruk, zložitejších vývojárskych postupov, testov a pod.

A8.Nie nepriateľské skupiny TOE nebude schopné sa efektívne brániť nepriateľskej skupine autorizovaných používateľov.
Vďaka separácii používateľských rôl je možné odhaliť nepriateľskú činnosť jednotlivca (aj keď nie obmedziť), ale v prípade skupín by to už nemuselo byť možné. Napriek tomu riziko nepriateľských autorizovaných používateľov by malo byť primerane malé.

A9.Bežný hardvér a softvér TOE môže byť postavené z bežných hardvérových a softvérových komponentov.
Použitie špecializovaných komponentov by mohlo značne navýšiť nákladnosť systému.

A10.Nie sofistikovaný útok TOE nie je schopné odolávať sofistikovaným útokom.

A11.Stanovené pravidlá Na fungovanie TOE sú stanovené presné a úplne pravidlá.
Tieto pravidlá určujú ako a za akých podmienok sa vykonávajú funkcie systému, ale definujú aj spôsob údržby personálom.

A12.Kompetentní privilegovaní používatelia Privilegovaní používatelia vykonávajú svoje povinnosti zodpovedne.
Pri nedôslednom uplatňovaní organizačných a iných pravidiel opatrenia z nich vyplývajúce nemusia byť účinné.

7.3.2 Hrozby

Hrozby bránené TOE

T1.Neautorizované použitie Neautorizovaný používateľ bude schopný využívať služby, ktoré vyžadujú autorizáciu.

T2.Falošná autentifikácia Používateľovi sa podarí uskutočniť falošnú autentifikáciu.

Príkladom môže byť hádanie hesla, či použitie odchytených autentifikačných údajov.

T3.Nepravé obchodné informácie Informácie o obchodníkoch a ich ponukách nebudú pravé.
Toto môže byť spôsobené napríklad podhodeným falošných podkladov alebo modifikáciou už uložených informácií.

T4.Odhalenie alebo zmena prenášaných informácií Citlivé informácie prenášané medzi systémom a účastníkmi môžu byť odpočúvaná alebo zmenené.

T5.Odhalenie osobných údajov Osobné údaje sa dostanú do nepovolaných rúk.
Osobné údaje majú byť používané len na účely uskutočňovania obchodných transakcií.

Hrozby bránené TOE a prostredím

T6.Zbavenie sa zodpovednosti Pre kontrolované udalosti v systéme nebude možné zistiť iniciátora.
Identitu iniciátora kontrolovaných udalostí nebude možné zistiť, alebo neskôr budú záznamy o tejto aktivite zmenené alebo odstránené.

Hrozby bránené prostredím

T7.Nie bezpečné použitie TOE môže byť nastavené, používané alebo administrované nie bezpečným spôsobom.

7.3.3 Organizačné bezpečnostné politiky

P1.Kryptografické štandardy Používane kryptografické primitíva sú v súlade s uznávanými kryptografickými štandardami a legislatívou.

P2.Tréning Autorizovaní používatelia sú školení na používanie TOE bezpečným spôsobom.
Používatelia systému budú školení, ako používať TOE, ale aj ako pri tom zachovať bezpečnosť. To zahŕňa napríklad poučenie o sociálnom inžinierstve a spôsoboch ako sa proti nemu brániť.

7.4 Bezpečnostné ciele

7.4.1 Bezpečnostné ciele pre TOE

Tabuľka 7.1: Bezpečnostné ciele pre TOE

Bezpečnostné ciele	Zodpovedajúce hrozby alebo politiky
O1.Identifikácia TOE dostatočne spoľahlivo jednoznačne autentifikuje používateľa pred použitím funkcií, ktoré vyžadujú autorizáciu.	T1.Neautorizované použitie T2.Falošná autentifikácia T3.Nepravé obchodné informácie T6.Zbavenie sa zodpovednosti
O2.Bezpečná komunikácia V prípade prenosu dôverných informácií TOE komunikuje s používateľmi pomocou kanála zabezpečujúceho dôvernosť a integritu prenášaných dát.	T4.Odhalenie alebo zmena prenášaných informácií
O3.Audit TOE vykonáva auditovanie udalostí systému a umožní prezeranie a vyhľadávanie v auditovacích záznamoch. Kontrolovanie auditovacích záznamov je vykonávané pravidelne.	T6.Zbavenie sa zodpovednosti
O4.Kontrola prístupu TOE povoľuje použitie funkcií TOE na základe určených pravidiel a identity iniciátora.	T1.Neautorizované použitie T5.Odhalenie osobných údajov T6.Zbavenie sa zodpovednosti
O5.Ochrana dát TOE kontroluje integritu uložených dát a v prípade dôverných informácií tieto šifruje.	T3.Nepravé obchodné informácie T5.Odhalenie osobných údajov
O6.Kryptografické štandardy Používane kryptografické primitíva sú v súlade s uznávanými kryptografickými štandardami a legislatívou.	P1.Kryptografické štandardy

7.4.2 Bezpečnostné ciele pre prostredie

Všetky predpoklady pre bezpečnostné prostredie TOE sú zároveň aj bezpečnostné ciele pre prostredie. Nebudeme ich tu znovu vymenovávať.

Tabuľka 7.2: Bezpečnostné ciele pre prostredie

Bezpečnostné ciele	Zodpovedajúce hrozby alebo politiky
O3.Audit TOE vykonáva auditovanie udalostí systému a umožní prezeranie a vyhľadávanie v auditovacích záznamoch. Kontrolovanie auditovacích záznamov je vykonávané pravidelne.	T6.Zbavenie sa zodpovednosti
O7.Školenia a dokumentácia Pre používateľov je dostupná potrebná dokumentácia, ktorá je postačujúca a presná. Na jej základe budú používatelia školení.	T7.Nie bezpečné použitie P2.Tréning
O8.Bezpečný operačný systém Použitý operačný systém je dostatočne bezpečný. Bezpečnosť operačného systému napríklad znamená, že iné procesy nemôžu zasahovať do behu TOE, že dokáže zaručiť neobchádzanie bezpečnostných prvkov systému atď.	T1.Neautorizované použitie T3.Nepravé obchodné informácie T5.Odhalenie osobných údajov T6.Zbavenie sa zodpovednosti
O9.Oprava nájdených chýb Dodávateľ TOE opraví chyby nájdené pri jeho používaní.	T*.

7.5 Bezpečnostné požiadavky pre TOE

7.5.1 Funkčné požiadavky pre TOE

V tejto časti stanovíme potrebné funkčné požiadavky. Tieto funkčné požiadavky môžu mať závislosti na iným bezpečnostných požiadavkach. Navyše uvedieme, ktoré bezpečnostné ciele pomáhajú naplniť, resp. ako závislosti ktorých bezpečnostných požiadaviek sa dostali do nášho zoznamu (nie nutne všetky).

Tabuľka 7.3: Funkčné požiadavky pre TOE

Funkčné požiadavky	Ciele / Závislosti	Závisí na
Trieda FAU: Bezpečnostný audit (Security audit) Táto trieda zahŕňa rozpoznávanie, zaznamenávanie, uchovávanie a analýzu bezpečnostne relevantných informácií. Na základe výsledných auditovacích záznamov môže byť určené, ktoré relevantné aktivity nastali a kto je za ne zodpovedný.		
FAU_GEN Generovanie auditovacích záznamov (Security audit data generation)	O3.Audit	FPT_STM FIA_UID
Definuje auditované udalosti a obsah auditovacích záznamov.		
FAU_SAR Prezeranie auditovacích záznamov (Security audit review)	O3.Audit	FAU_GEN
Definuje požiadavky na nástroje pre prezeranie auditovacích záznamov.		

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FAU_SEL Výber auditovaných udalostí (Security audit event selection)	O3.Audit	FAU_GEN FMT_MTD
Definuje požiadavky na výber auditovaných udalostí.		
FAU_STG Úložisko auditovacích záznamov (Security audit event storage)	O3.Audit	FAU_GEN
Definuje požiadavky na schopnosť TSF vytvoriť a udržiavať bezpečné auditovacie záznamy.		
Trieda FCO: Komunikácia (Communication) Táto trieda sa zaoberá zaručením identity účastníkov výmeny dát. Nedovoľuje príjemcovi popretie prijatia správy a odosielateľovi popretie odoslatia správy. [1]		
FCO_NRO Nepopretie pôvodu (Non-repudiation of origin)	O1.Identifikácia	FIA_UID
Zaručuje, že pôvodca informácie nemôže úspešne poprieť poslatie informácie.		
Trieda FCS: Kryptografická podpora (Cryptographic support) TSF môže používať kryptografické funkcie na splnenie vyšších bezpečnostných cieľov. V tom prípade sa používa táto trieda.		

[1] Rodinu FCO_NRR Nepopretie prijatia sme nezaradili do PP kvôli jeho obtiažnej dosiahnuteľnosti. Najmä na strane zákazníka by dosahovanie tejto požiadavky mohlo viesť k neštandardným riešeniam, ktoré by nemuseli byť široko akceptované.

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FCS_CKM Správa kryptografických kľúčov (Cryptographic key management)	O6.Kryptografické štandardy	FDP_ITC FMT_MSA
Používa sa na podporu životného cyklu správy kľúčov.		
FCS_COP Kryptografické operácie (Cryptographic operation)	O6.Kryptografické štandardy O5.Ochrana dát	FDP_ITC FMT_MSA
Definuje správne používanie kryptografickým funkcií.		
Trieda FDP: Ochrana používateľských dát (User data protection) Táto trieda špecifikuje požiadavky vzťahujúce sa k ochrane používateľských dát. Zahŕňa v sebe definovanie politík, rôzne formy ochrany , export, import a komunikáciu medzi TSF.		
FDP_ACC Politiky kontroly prístupu (Access control policy)	O4.Kontrola prístupu	FDP_ACF
Identifikuje politiky kontroly prístupu a definuje pôsobnosť týchto politík.		
FDP_ACF Funkcie kontroly prístupu (Access control functions)	O4.Kontrola prístupu	FDP_ACC FMT_MSA
Popisuje pravidlá pre funkcie, ktoré implementujú politiky definované v FDP_ACC.		

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FDP_IFC Politiky kontroly toku dát (Information flow control policy)	O4.Kontrola prístupu	FDP_IFF
Identifikuje politiky kontroly toku dát a definuje pôsobnosť týchto politík.		
FDP_IFF Funkcie kontroly toku dát (Information flow control functions)	O4.Kontrola prístupu	FDP_IFC FMT_MSA
Popisuje pravidlá pre funkcie, ktoré implementujú politiky definované v FDP_IFC.		
FDP_ITC Import z mimo kontroly TSF (Import from outside TSF control)	FCS_*	[FDP_ACC / FDP_IFC] FMT_MSA
Definuje mechanizmy pre zavedenie používateľských dát do TOE.		
FDP_RIP Ochrana zvyškových informácií (Residual information protection)	O5.Ochrana dát	
Určuje potrebu zaručiť, že zmazané informácie už ďalej nebudú prístupné a novo vytvorené objekty nebudú obsahovať informácie, ktoré nemajú byť prístupné.		

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FDP_SDI Integrita uložených dát (Stored data integrity)	O5.Ochrana dát	
Definuje požiadavky, ktoré adresujú ochranu používateľských dát, pokiaľ sú uchovávané v TSC.		
Trieda FIA: Identifikácia a autentifikácia (Identification and authentication) Táto trieda popisuje požiadavky na preukazovanie a overovanie identity používateľov.		
FIA_AFL Zlyhanie autentifikácie (Authentication failures)	O1.Identifikácia	FIA_UAU
Definuje hodnoty pre neúspešné pokusy o autentifikáciu a akcie TSF v prípade zlyhania týchto pokusov. Tieto parametre zahrňujú (ale nie sú limitované len na) napríklad počet neúspešných pokusov a časové hranice.		
FIA_ATD Definícia používateľských atribútov (User attribute definition)	O4.Kontrola prístupu	FIA_UAU
Definuje spôsob spojenia používateľa s jeho bezpečnostnými atribútmi, ktoré sa používajú na uplatňovanie TSP.		
FIA_UAU Autentifikácia (User authentication)	O1.Identifikácia	FIA_UID
Definuje typy mechanizmov autentifikácie a potrebné atribúty, na základe ktorých je autentifikácia založená.		

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FIA_UID Identifikácia (User identification)	O1.Identifikácia FAU_GEN FIA_UAU	
Definuje podmienky, za ktorých musí byť používateľ identifikovaný.		
Trieda FMT: Bezpečnostná správa (Security management) Táto trieda špecifikuje správu rôznych aspektov TSF: bezpečnostné atribúty, dáta a funkcie TSF.		
FMT_MSA Správa bezpečnostných atribútov (Management of security attributes)	FCS_* FDP_ACF FDP_IFF	[FDP_ACC / FDP_IFC] FMT_SMR ADV_SPM
Umožňuje autorizovaným používateľom spravovať bezpečnostné atribúty.		
FMT_MTD Správa dát TSF (Management of TSF data)	FAU_SEL	FMT_SMR ADV_SPM
Umožňuje autorizovaným používateľom spravovať dáta TSF (napríklad hodiny, systémové konfigurácie a pod.)		
FMT_SMR Bezpečnostné role (Security management roles)	O4.Kontrola prístupu	FIA_UID
Kontroluje priradenie rôznych rolí používateľom.		
Trieda FPT: Ochrana TSF (Protection of the TSF) Táto trieda obsahuje rodiny funkčných komponentov vzťahujúcich sa k integrite a správe mechanizmov poskytujúcich TSF (nezávisle od špecifík TSP) a k integrite dát TSF.		

Tabuľka 7.3: pokračovanie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
FPT_STM Časové pečiatky (Time stamps)	FAU_GEN	
Adresuje požiadavky na spoľahlivé časové pečiatky v rámci TOE.		
Trieda FTP: Zabezpečené cesty/kanály (Trusted path/channels) Rodiny tejto triedy poskytujú funkčné požiadavky pre zabezpečenú komunikáciu medzi TSF a používateľom alebo iným dôveryhodným IT produktom.		
FTP_ITC Zabezpečené kanály medzi TSF (Inter-TSF trusted channel)	O2.Bezpečná komunikácia	
Definuje požiadavky na vytvorenie zabezpečeného kanála medzi TSF a iným dôveryhodným IT produktom.		
FTP_TRP Zabezpečené cesty (Trusted path)	O2.Bezpečná komunikácia	
Definuje požiadavky na vytvorenie a udržanie zabezpečenej cesty medzi TSF a používateľom.		

7.5.2 Bezpečnostné záruky pre TOE

Tabuľka 7.4: Bezpečnostné záruky pre TOE

Bezpečnostné záruky	Závisí na
Trieda ACM: Správa konfigurácii (Configuration management) Správa konfigurácii (*CM*) je metóda dosahujúca to, že funkčné požiadavky a špecifikácie sú zachytené v implementácii TOE. CM systémy sa používajú na zaručenie integrity častí TOE tým, že sledujú zmeny a zaručujú, že zmeny sú autorizované.	
ACM_CAP.3 Kontrola autorizácie (Authorisation controls)	ACM_SCP.1 ALC_DVS.1
Jednoznačná identifikácia konfigurácií (zdrojové kódy, dokumentácie, ...) zabráni nejednoznačnosti, ktorá inštancia TOE sa používa alebo skúma. Mechanizmy kontrolujúce zmeny TOE a používanie CM systémov pomáha udržať integritu TOE.	
ACM_SCP.1 Pokrytie TOE pomocou CM (TOE CM coverage)	ACM_CAP.3
CM systém má mať pod kontrolou aspoň nasledujúce konfiguračné prvky: implementáciu, dizajn, testy a dokumentáciu.	
Trieda ADO: Doručenie a prevádzka (Delivery and operation) Táto trieda definuje požiadavky pre korektné doručenie, inštaláciu, generovanie a spúšťanie TOE.	
ADO_DEL.1 Postupy doručenia (Delivery procedures)	
Popisuje potrebné postupy pre bezpečnú distribúciu verzii TOE.	

Tabuľka 7.4: pokračovanie

Bezpečnostné záruky	Závisí na
ADO_IGS.1 Postupy inštalácie, generovania a spúšťania (Installation, generation and start-up procedures)	AGD_ADM.1
Popisuje potrebné kroky pre bezpečnú inštaláciu, generáciu a spúšťanie TOE.	
Trieda ADV: Vývoj (Development) Táto trieda definuje požiadavky pre popis TSF na rôznych stupňoch abstrakcie a pre demonštráciu súladu (korešpondencie) medzi týmito stupňami abstrakcie a vzťahu medzi TSP a funkčnou špecifikáciou	
ADV_FSP.1 Neformálna funkčná špecifikácia (Informal functional specification)	ADV_RCR.1
Kompletne a konzistentne popisuje TSF na úrovni neformálnej funkčnej špecifikácie.	
ADV_HLD.2 Hrubý návrh uplatňujúci bezpečnosť (Security enforcing high-level design)	ADV_FSP.1 ADV_RCR.1
Kompletne a konzistentne popisuje TSF na úrovni hrubého návrhu. Tento popisuje štruktúru TSF na úrovni podsystémov, popisuje účel a použitie všetkých rozhraní podsystémov. Navyše popisuje rozdelenie TOE na podsystémy vynucujúce TSP a ostatné podsystémy.	
ADV_RCR.1 Neformálna demonštrácia súladu (Informal correspondence demonstration)	
Demonštruje, že všetky relevantné bezpečnostné funkcionality viac abstraktnej reprezentácie TSF sú korektne a úplne zastúpené aj v menej abstraktnej reprezentácii TSF.	

Tabuľka 7.4: pokračovanie

Bezpečnostné záruky	Závisí na
Trieda AGD: Príručky (Guidance documents) Táto trieda popisuje požiadavky na používateľské a administrátorské príručky, ktoré majú popisovať všetky relevantné aspekty potrebné pre bezpečnú správu a používanie TOE.	
AGD_ADM.1 Administrátorská príručka (Administrator guidance)	ADV_FSP.1
Administrátorská príručka je písaný materiál určený pre osoby zodpovedné konfigurovaním, údržbou a správou TOE.	
AGD_USR.1 Používateľská príručka (User guidance)	ADV_FSP.1
Používateľská príručka je materiál určený pre ne-administrátorov, t.j. iných používateľov používajúcich vonkajšie rozhrania TOE. Popisuje bezpečnostné funkcie poskytované TSF a postupy (vrátane varovaní) pre ich bezpečné použitie.	
Trieda ALC: Životný cyklus (Life cycle support) Životný cyklus predstavuje disciplínu a kontrolu v procese doľaďovania TOE počas jeho vývoja a údržby.	
ALC_DVS.1 Identifikácia bezpečnostných opatrení (Identification of security measures)	
Popisuje všetky fyzické, procedurálne, personálne a iné bezpečnostné opatrenia potrebné na ochranu dôvernosti a integrity návrhu a implementácie TOE počas jeho vývoja.	
Trieda ATE: Testy (Tests) Testy pomáhajú preukázať, že funkčné požiadavky na TOE sú splnené.	

Tabuľka 7.4: pokračovanie

Bezpečnostné záruky	Závisí na
ATE_COV.2 Analýza pokrytia (Analysis of coverage)	ADV_FSP.1 ATE_FUN.1
Cieľom je preukázať, že TSF bolo pretestované voči jeho funkčnej špecifikácii systematickým spôsobom.	
ATE_DPT.1 Testovanie hrubého návrhu (Testing: high-level design)	ADV_HLD.1 ATE_FUN.1
Poskytnutá analýza hĺbky testov má ukázať, že identifikované testy sú dostačujúce pre demonštráciu toho, že TSF fungujú v súlade s ich hrubým návrhom.	
ATE_FUN.1 Funkčné testy (Functional testing)	
Cieľom je ukázať vývojárom, že všetky bezpečnostné funkcie sú vykonávané ako majú. Vývojár má vykonať tieto testy a vypracovať o tom testovaciu dokumentáciu.	
ATE_IND.2 Nezávislé testy - vzorka (Independent testing - sample)	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1
Cieľom je ukázať, že testy boli vykonaná ako bolo špecifikované. Hodnotiteľ vyberie a zopakuje vzorku vývojárskych testov.	
Trieda AVA: Zhodnotenie zraniteľností (Vulnerability assessment) Táto trieda adresuje existenciu zneužiteľných tajných ciest, možnosť neprávnej konfigurácie, možnosť zneužitia zraniteľností zavedených pri vývoji alebo prevádzke TOE.	

Tabuľka 7.4: pokračovanie

Bezpečnostné záruky	Závisí na
AVA_MSU.1 Preskúmanie príručiek (Examination of guidance)	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1
Cieľom je zaručiť príručky neobsahujú klamné alebo konfliktné informácie a že obsahujú bezpečné postupy pre všetky módy úkonov TOE. Nebezpečné stavy by mali byť jednoducho detekovateľné.	
AVA_SOF.1 Preskúmanie príručiek (Examination of guidance)	ADV_FSP.1 ADV_HLD.1
I v prípade, že bezpečnostné funkcie TOE nemôžu byť deaktivované, obíditeľné alebo poškodené, stále môžu byť porazené kvôli zraniteľnostiam v koncepte používaných bezpečnostných mechanizmov. Spôsobilosť bezpečnostného správania týchto funkcií je vyjadrená vo forme tvrdenia o sile bezpečnostných funkcií TOE.	
AVA_VLA.1 Vývojárska analýza zraniteľností (Developer vulnerability analysis)	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1
Analýza zraniteľností je vykonávaná vývojárom, aby zistila prítomnosť zjavných bezpečnostných zraniteľností, a aby potvrdila, že tieto nemôžu byť zneužité v zamýšľanom prostredí TOE.	

7.6 Bezpečnostné požiadavky pre prostredie

V tejto časti stanovíme IT funkčné požiadavky pre prostredie. Pokrytie bezpečnostných cieľov pre prostredie je však zväčša riešené nie-IT požiadavkami. [2]

[2] V kapitole 8 sú popísané pravidlá bezpečnej prevádzky a správy systému, ktoré pokrývajú všeobecné nie informačné požiadavky. Tieto však už nie sú oficiálnou súčasťou PP.

Tabuľka 7.5: Funkčné požiadavky pre prostredie

Funkčné požiadavky	Ciele / Závislosti	Závisí na
Trieda FPT: Ochrana TSF (Protection of the TSF) Táto trieda obsahuje rodiny funkčných komponentov vzťahujúcich sa k integrite a správe mechanizmov poskytujúcich TSF (nezávisle od špecifík TSP) a k integrite dát TSF.		
FPT_SEP Separácia domén (Domain separation)	O8.Bezpečný operačný systém	
Zaručuje, že existuje aspoň jedna bezpečnostná doména pre vykonávanie TSF taká, že TSF je chránená pred vonkajším rušením a svojvoľným menením.		

7.7 Zdôvodnenie

7.7.1 Zdôvodnenie bezpečnostných cieľov

Teraz ukážeme, že všetky aspekty bezpečnostného prostredia TOE sú dostatočne pokryté pomocou bezpečnostných cieľov.

Všetky predpoklady bezpečnostného prostredia sú aj bezpečnostné ciele pre prostredie, takže v ich prípade je pokrytie splnené triviálne.

Tabuľka 7.6: Pokrytie hrozieb a organizačných politík bezpečnostnými cieľmi

Hrozba / Organizačná politika
T1.Neautorizované použitie **Pokrývajúce bezpečnostné ciele:** O4.Kontrola prístupu O1.Identifikácia **Zdôvodnenie:** Túto hrozbu pokrýva primárne O4.Kontrola prístupu,ktorý využíva informácie získané z O1.Identifikácia.

Tabuľka 7.6: pokračovanie

Hrozba / Organizačná politika
T2.Falošná autentifikácia **Pokrývajúce bezpečnostné ciele:** O1.Identifikácia **Zdôvodnenie:** Túto hrozbu pokrýva O1.Identifikácia.
T3.Nepravé obchodné informácie **Pokrývajúce bezpečnostné ciele:** O1.Identifikácia O5.Ochrana dát **Zdôvodnenie:** Táto hrozba má dva možné aspekty: možnosť podstrčenia obchodných informácií je riešená pomocou O1.Identifikácia a prípadná neskoršia zmena už zaznamenaných obchodných informácií je pokryté O5.Ochrana dát.
T4.Odhalenie alebo zmena prenášaných informácií **Pokrývajúce bezpečnostné ciele:** O2.Bezpečná komunikácia **Zdôvodnenie:** Túto hrozbu pokrýva O2.Bezpečná komunikácia.

Tabuľka 7.6: pokračovanie

Hrozba / Organizačná politika
T5.Odhalenie osobných údajov **Pokrývajúce bezpečnostné ciele:** O4.Kontrola prístupu O5.Ochrana dát **Zdôvodnenie:** Túto hrozbu pokrýva O4.Kontrola prístupu tým, že kontroluje použitie týchto informácií len na určené účely. Pred možnosťou priameho čítania chráni O5.Ochrana dát.
T6.Zbavenie sa zodpovednosti **Pokrývajúce bezpečnostné ciele:** O3.Audit O4.Kontrola prístupu O1.Identifikácia **Zdôvodnenie:** Túto hrozbu primárne pokrýva O3.Audit a fakt, že vykonanie činností sa kontroluje pomocou O4.Kontrola prístupu (,čo v prípade relevantných akcií vyžaduje O1.Identifikácia).
T7.Nie bezpečné použitie **Pokrývajúce bezpečnostné ciele:** O7.Školenia a dokumentácia A12.Kompetentní privilegovaní používatelia **Zdôvodnenie:** Túto hrozbu pokýva O7.Školenia a dokumentácia spolu s predpokladom A12.Kompetentní privilegovaní používatelia.

Tabuľka 7.6: pokračovanie

Hrozba / Organizačná politika
P1.Kryptografické štandardy **Pokrývajúce bezpečnostné ciele:** O6.Kryptografické štandardy **Zdôvodnenie:** Táto politika je priamo pokrytá O6.Kryptografické štandardy.
P2.Tréning **Pokrývajúce bezpečnostné ciele:** O7.Školenia a dokumentácia **Zdôvodnenie:** Táto politika je pokrytá O7.Školenia a dokumentácia.

Teraz ešte zdôvodníme stanovenie niektorých všeobecných bezpečnostných cieľov, ktoré sme nespomínali explicitne pri všetkých hrozbách.

A10.Nie sofistikovaný útok Keďže má ísť o bežne používaný systém, kvôli použitiu bežných prostriedkov (napr. A9.Bežný hardvér a softvér) sa nepredpokladá, že bude schopný čeliť sofistikovaným útokom. Tento predpoklad / cieľ má preto dopad na skoro všetky hrozby.

O8.Bezpečný operačný systém Korektné fungovanie systému musí byť podporené operačným systémom, na ktorom tento beží. Tento cieľ prostredia má teda dopad na ciele týkajúce sa činností v rámci TOE.

O9.Oprava nájdených chýb Pre správne fungovanie systému je nutné objavené chyby opraviť. Tento cieľ ovplyvňuje všetky ciele a hrozby.

Odvoditeľnosť bezpečnostných cieľov vyplýva z ich použitia pri pokrývaní aspektov bezpečnostného prostredia. Ešte uvedieme sumarizujúcu tabuľku vzťahov medzi cieľmi a hrozbami a politikami (predpoklady prostredia vynecháme).

Tabuľka 7.7: Pokrytie hrozieb a politík

	O1.	O2.	O3.	O4.	O5.	O6.	O7.	O8.	O9.
T1.	X			X				X	X
T2.	X								X
T3.	X				X			X	X
T4.		X							X
T5.				X	X			X	X
T6.	X		X	X				X	X
T7.							X		X
P1.						X			
P2.							X		

7.7.2 Zdôvodnenie bezpečnostných požiadaviek

Zdôvodnenie funkčných požiadaviek

Teraz ukážeme, že všetky bezpečnostné ciele sú pokryté pomocou bezpečnostných požiadaviek.

O1.Identifikácia Tento cieľ priamo napĺňajú FIA_UID Identifikácia a FIA_UAU Autentifikácia. Na zabezpečenie korektnej identifikácie pri posielaní podkladov obchodníkom alebo posielaní správ sa používa FCO_NRO Nepopretie pôvodu. Ako zabezpečenie proti možnosti hádania autentifikačných údajov sa navyše používa FIA_AFL Zlyhanie autentifikácie.

O2.Bezpečná komunikácia Tento cieľ je naplnený pomocou FTP_ITC Zabezpečené kanály medzi TSF a FTP_TRP Zabezpečené cesty.

O3.Audit Tento cieľ je naplnený pomocou triedy FAU (FAU_GEN Generovanie auditovacích záznamov, FAU_SAR Prezeranie auditovacích záznamov, FAU_SEL Výber auditovaných udalostí a FAU_STG Úložisko auditovacích záznamov).

O4.Kontrola prístupu Tento cieľ je primárne naplnený pomocou FDP_ACC Politiky kontroly prístupu, FDP_ACF Funkcie kontroly prístupu, FDP_IFC Politiky kontroly toku dát a FDP_IFF Funkcie kontroly toku dát. Politiky definované týmito rodinami sú založené na rolách

(FMT_SMR Bezpečnostné role) a/alebo iných atribútoch (FIA_ATD Definícia používateľských atribútov).

O5.Ochrana dát Tento cieľ napĺňa FDP_SDI Integrita uložených dát a FCS_COP Kryptografické operácie, pomocou čoho môžeme dôverné informácie šifrovať.

O6.Kryptografické štandardy Tento cieľ je naplnený pomocou triedy FCS (FCS_CKM Správa kryptografických kľúčov a FCS_COP Kryptografické operácie).

O7.Školenia a dokumentácia Dostupnosť potrebnej dokumentácie je naplnená pomocou AGD_ADM.1 Administrátorská príručka a AGD_USR.1 Používateľská príručka. Školenie používateľov musí byť zabezpečené prostredím - zväčša formou organizačných pravidiel.

O8.Bezpečný operačný systém Tento cieľ prostredia je napĺňaný pomocou FPT_SEP Separácia domén, ale vyžaduje to aj pravidelnú údržbu systému.

O9.Oprava nájdených chýb Pre tento cieľ prostredia nie je príslušná bezpečnostná požiadavka v CC a musí byť riešená prostredím zväčša právnym záväzkom s dodávateľom systému.

Odvoditeľnosť použitých bezpečnostných požiadaviek vyplýva z ich použitia pri pokrývaní bezpečnostných cieľov príp. z dodržiavania závislostí bezpečnostných požiadaviek. Uvedieme tabuľky vzťahov medzi bezpečnostnými požiadavkami a bezpečnostnými cieľmi (X znamená priame pokrývanie,z znamená pokrývanie cez závislosti).

Tabuľka 7.8: Pokrytie funkčnými požiadavkami

	O1.	O2.	O3.	O4.	O5.	O6.	O7.	O8.	O9.
FAU_GEN			X						
FAU_SAR			X						
FAU_SEL			X						
FAU_STG			X						
FCO_NRO	X								
FCO_NRR									
FCS_CKM						X			

Tabuľka 7.8: pokračovanie

	O1.	O2.	O3.	O4.	O5.	O6.	O7.	O8.	O9.
FCS_COP					X	X			
FDP_ACC				X					
FDP_ACF				X					
FDP_IFC				X					
FDP_IFF				X					
FDP_ITC						z			
FDP_RIP					X				
FDP_SDI					X				
FIA_AFL	X								
FIA_ATD				X					
FIA_UAU	X								
FIA_UID	X		z						
FMT_MSA				z		z			
FMT_MTD			z						
FMT_SMR				X					
FPT_SEP								X	
FPT_STM			z						
FTP_ITC		X							
FTP_TRP		X							

Zdôvodnenie bezpečnostných záruk

Zvolená úroveň EAL3 umožňuje dosiahnuť maximálne záruky z procesu návrhu bez značnejších zmien existujúcich zdravých princípov vývoja. Zvolená úroveň poskytuje strednú úroveň nezávisle zaručenej bezpečnosti, čo zodpovedá predpokladom na prostredie.

Oproti úrovni EAL2 poskytuje kompletnejšie testovanie a garantuje, že TOE nebolo svojvoľne zmenené vo fáze vývoja. Úroveň EAL4 vyžaduje ešte podrobnejší návrh a testovanie systému a viacero nezávislých testov. Úroveň EAL4 je už na hranici ekonomickej uskutočniteľnosti pre zdokonalenie existujúceho produktu.

Zdôvodnenie nenaplnenia všetkých závislostí

Funkčný komponent FMT_MSA Správa bezpečnostných atribútov závisí na ADV_SPM.1 Neformálny model bezpečnostných politík. Ak vývojár dodá v rámci príručiek jasnú definíciu bezpečných hodnôt pre jednotlivé atribúty, tak nie je nevyhnutné do PP zahrnúť ADV_SPM.1.

Kapitola 8

Implementácia a prevádzka

V predchádzajúcej časti sme zostrojili PP pre systém elektronického obchodu. PP slúži najmä na popis IT požiadaviek na systém, kritérií na jeho vyhodnotenie. Vyhodnotením systému však starostlivosť o jeho bezpečnosť nekončí. Okrem IT požiadaviek však treba uvažovať aj tie ostatné. Navyše bezpečnosť nie je jednorazová záležitosť, treba ju pravidelne prehodnocovať, či už po vyskytnutí bezpečnostných incidentov alebo aj postupná zmena prostredia môže viesť k neaktuálnosti protiopatrení, ktoré mali čeliť hrozbám.

K riešeniu týchto problémov využijeme existujúci štandard ISO/IEC 17799 Information security management (*Správa informačnej bezpečnosti*, [17]), ktorý špecifikuje požiadavky pre stanovenie, implementáciu a udržiavanie systému pre správu informačnej bezpečnosti. Tento štandard je v súlade s normou ISO 9001. ISO/IEC 17799 vznikol prebratím britského štandardu BS 7799 ([16]).

V rámci tohto štandardu je definovaný model procesu známy ako "Plan-Do-Check-Act"(PDCA ,*Plánovanie-vykonanie-kontrola-reakcia*). Tento má nasledujúce fázy:

Plánovanie V tejto fáze sa stanovujú bezpečnostné politiky, ciele, procesy a postupy relevantné pre kontrolu rizík a zlepšovanie informačnej bezpečnosti. Tieto by mali byť v súlade so všeobecnými politikami a cieľmi spoločnosti.

Vykonanie V tejto fáze sa implementujú a vykonávajú tieto politiky, procesy a postupy.

Kontrola V tejto fáze sa meria a hodnotí výkon procesov voči politikám,

cieľom a praktickým skúsenostiam. Výsledok je predkladaný zodpovedným a kompetentným osobám.

Reakcia V tejto fáze sa vykonajú nápravné a preventívne akcie pre budúce zlepšenie.

Obrázok 8.1: Model PDCA. Zdroj: [16]

Štandard ISO/IEC 17799 rozdeľuje úlohy potrebné pre zaistenie bezpečnosti systému do 10 skupín. Najprv popíšeme všeobecné opatrenie vyplývajúce z tohto štandardu a následne uvedieme aké konkrétne dôsledky z tých opatrení vyplývajú pre náš systém . Budeme predpokladať, že systém bude prevádzkovaný IT spoločnosťou, ktorá bude prevádzkovať aj iné systémy.

8.1 Bezpečnostné politiky

Pre bezpečné fungovanie systému je dôležité stanoviť istý rámec jeho fungovania. Cieľom bezpečnostných politík je poskytnúť riadenie a podporu pre informačnú bezpečnosť. Tieto sú definované vo forme dokumentov, ktoré stanovujú bezpečnostné ciele systému a ako ich naplniť. Tieto dokumenty musia byť schválené manažmentom a publikované všetkým potrebným používateľom. V súlade s procesom typu PDCA je nutná pravidelná kontrola bezpečnostných politík a v prípade potreby ich aktualizácia.

V rámci používateľskej a najmä administrátorskej príručky sú popísané relevantné aspekty bezpečného používania systému, tieto by mali byť zohľadnené v bezpečnostných politikách. Keďže využívame možnosti auditovania, je nutné aj tento aspekt zahrnúť do bezpečnostných politík.

Keďže predpokladáme, že systém bude fungovať v rámci väčšej spoločnosti, táto už bude mať vypracované všeobecné bezpečnostné politiky (ktoré by nemali byť v rozpore s BS). Týmito sa musí riadiť aj náš systém, však pre jeho špecifické potreby treba dodefinovať konkrétnejšie bezpečnostné politiky ako sú politiky klasifikácií aktív, politiky o kontrole prístupu a iné spomínané v tejto kapitole.

8.2 Organizačná bezpečnosť

Cieľom je spravovať informačnú bezpečnosť v rámci organizácie. Touto úlohou musí byť poverená odborne kompetentná osoba (alebo tím osôb), ktorá musí mať dostatočné kompetencie a zdroje na presadzovanie bezpečnostných politík. Zodpovednosti za ochranu jednotlivých aktív a za vykonávanie bezpečnostných procesov musia byť jednoznačne definované. V prípade potreby rady ohľadom informačnej bezpečnosti je potrebné zvážiť vyhľadanie spolupráce špecialistov.

Keďže je tu možnosť, že pri prevádzke alebo riešení bezpečnostných incidentov budú pristupovať k systému aj externí účastníci (experti,...), je nutné vyhodnotiť riziko spojené s týmto prístupom a prijať príslušné protiopatrenia. Prístup iným organizácií by mal byť založený na formálnych zmluvách.

Pravdepodobne pre náš systém nebude existovať osobitná skupina ľudí, ktorá by spravovala bezpečnosť tohto systému. Viac pravdepodobné je, že v rámci organizácie existuje takáto skupina, ktorá však má na starosti viacero prevádzkovaných systémov alebo pre celú organizáciu. Táto skupina by spravovala aj náš systém. V rámci nej by existovala osoba, ktorá by bola za neho zodpovedná.

Prístup externých špecialistov je pravdepodobný, keďže prevádzkujúca spoločnosť nebude mať asi špecialistov na všetky rôzne oblasti správy bezpečnosti. Keďže náš systém obsahuje aj citlivé údaje, je potrebné vyberať kompetentných externých účastníkov a právne zabezpečiť podmienky prístupu k systému jednak voči týmto externým účastníkom ako aj voči obchodníkom a zákazníkom (ako majiteľom potenciálne citlivých údajov).

8.3 Klasifikácia a riadenie aktív

Dôležitou úlohou je samozrejme primeraná ochrana aktív. Kvôli tomu je nutná inventarizácia všetkých dôležitých aktív, určenie vlastníkov zodpovedných za bezpečnosť týchto aktív a určenie ich identifikácie. Je nutné mať stanovenú klasifikáciu aktív, ktorá určuje potrebnú ochranu pre jednotlivé kategórie aktív.

Aktíva môžme rozdeliť na hmotné a nehmotné. K hmotným aktívam patrí hardvér a iné fyzické vybavenie. Ich vlastník je spoločnosť. K nehmotným aktívam patrí operačný systém, prípadne iné potrebné aplikačné vybavenie. Tu je opäť vlastník spoločnosť. V prípade vlastného systému pre elektronický obchod treba rozlišovať prípady, keď ho vyvinula samotná spoločnosť a keď ho prevádzkujúca spoločnosť len zakúpila. V prvom prípade je systém a jeho zmeny pod kontrolou spoločnosti, v druhom treba právne zabezpečiť vzťahy medzi prevádzkujúcou spoločnosťou a spoločnosťou, ktorá daný systém poskytla. Treba dohodnúť podmienky autorských práv, možnosti modifikácie, podpory a opravy nájdených chýb.

Ďalšou dôležitou skupinou aktív sú údaje obsiahnuté v systéme. V prípadne zverejnených informácií obchodníkov treba dodržať integritu a autentickosť a v prípade tajných informácií (osobné údaje, autentifikačné údaje, detaily transakcií a pod.) aj dôvernosť.

8.4 Personálna bezpečnosť

Bezpečnosť systému vo veľkej miere závisí od spoľahlivosti privilegovaných používateľov. Na minimalizáciu rizík hrozieb spôsobených ľuďmi. Preto je potrebné vyberať na pozície privilegovaných používateľov ľudí, u ktorých je predpoklad, že nebudú konať v rozpore s bezpečnostnými politikami systému, čo je v súlade s predpokladom kompetentných privilegovaných používateľov. Bezpečnostné role a zodpovednosti musia byť dokumentované v pracovnej náplni zamestnancov. Ak je to potrebné, tak dohoda o dodržaní dôvernosti má byť súčasťou pracovnej zmluvy. Porušenie bezpečnostných politík zamestnancom by malo byť riešené formálnym disciplinárnym konaním. Okrem týchto počiatočných podmienok je nutné vykonávať kontrolu dodržiavania týchto podmienok.

Okrem výberu zamestnancov je nutný aj ich tréning, aby si boli vedomí bezpečnostných hrozieb a aby boli schopní uplatňovať bezpečnostné politiky

pri ich práci. Taktiež by mali byť vedení k tomu, aby čo najrýchlejšie ohlásili bezpečnostné incidenty a slabosti.

Opatrenia pri výbere zamestnancov sú najviac dôležité pre roly administrátora a auditora. Samozrejme sú dôležité aj pre rolu operátora, ktorý je tiež privilegovaný používateľ.

Okrem tréningu zamestnancov (privilegovaných používateľov) je nutné poskytnúť istú formu tréningu aj ostatným používateľom. V prípade zákazníkov je prijateľná forma pomocou zverejnených používateľských príručiek pre zákazníkov, v prípade obchodníkov je v prípade dohody možný aj tréning.

8.5 Fyzická bezpečnosť a bezpečnosť prostredia

Na zabezpečenie správneho fungovania systému je potrebné zabezpečiť aj fyzickú bezpečnosť. Oblasti, v ktorých nastáva spracovávanie informácií musia byť fyzicky oddelené a prístup musí byť chránený primeranými prostriedkami, aby sa zamedzilo neautorizovanému prístupu.

Okrem potrebnej ochrany proti neautorizovanému prístupu je nutné oblasti spracovávajúce informácie zabezpečiť voči rizikám vyplývajúcim z hrozieb prostredia. To napríklad znamená, že používaná budova je riadne udržiavaná a chránená pred prírodnými vplyvmi. Zariadenia by mali byť chránené pred výpadkami elektrickej energie a používaná kabeláž zabezpečená pred prerušením a poškodením.

Navyše je potrebné vymazať dôverné informácie zo zariadení pred ich odstránením (napríklad v prípade starých záznamových médií, ale aj v prípade odovzdania zariadení do opravy) alebo pred ich znovupoužitím (najmä v prípade použitia zariadenia na nižšie klasifikované aktíva, kde bezpečnostné opatrenia môžu byť nižšie).

K fyzickej bezpečnosti patria aj politiky zamedzujúce kompromitácií alebo ukradnutiu informácií tým, že používatelia nenechávajú bez dozoru svoje veci - tzv. politika "čistého stolu a čistej obrazovky". To sa napríklad môže týkať operátorov, aby sa ešte nezverejnené informácie nedostali do nepovolaných rúk (napríklad nová ponuka by sa nemala dostať do rúk konkurencia, ktorá by sa mohla stihnúť potom na ňu pripraviť).

8.6 Správa komunikácie a operácií

8.6.1 Operačné postupy a stanovenie zodpovednosti

Pre správne a bezpečné fungovanie systému je nutné v bezpečnostných politikách definovať operačné postupy a tieto udržiavať. Všetky zmeny spracovávania informácií musia byť kontrolované. Pre prípad bezpečnostných incidentov musia byť vypracované postupy zvládania incidentov a stanovenie zodpovedností. Navyše je nutné separovať povinnosti používateľov, aby sa redukovala šanca zneužitia informácií alebo služieb (preto sú definované až tri skupiny privilegovaných používateľov). Kvôli zamedzeniu prístupu vývojárov k skutočným údajom (ktoré môžu byť dôverné) a aj kvôli minimalizácií zanesenia chýb do produkčného prostredia, toto je oddelené od vývojového prostredia.

Pre každú rolu privilegovaného používateľa musia byť definované postupy, ktorými má bezpečne vykonávať svoje povinnosti, a zodpovednosti, ktoré vyplývajú z jeho povinností. Napríklad administrátor spravuje priradenie rolí. Preto musia byť definované pravidlá, za akých podmienok môže byť pridelená konkrétna rola (pravidlo separácie rolí, schválenie manažmentom, prípadne iné), pravidlá na odobratie a pod. Taktiež musí niesť zodpovednosť (ktorá musí byť definovaná) za prípadné porušenia týchto pravidiel či za ich úmyselné obídenie. Podobne to platí pre ostatné činnosti vykonávané administrátorom (správa systému atď.), auditorom (kontrola auditovacích záznamov, ich zálohovanie atď.) a operátorom (správa obchodných informácií atď.).

8.6.2 Plánovanie a akceptácia systému

Vývoj systému musí byť plánovaný a organizovaný. Je nutné sledovať schopnosti systému a odhadovať budúce požiadavky, aby systém poskytoval dostačujúcu výpočtovú silu. Pri zavádzaní nových verzií je potrebné stanoviť kritéria pre akceptáciu a vhodnú množinu testov na overenie, či systém je vhodný na nasadenie do ostrej prevádzky.

Pred každým nasadením novej verzie systému by sa mala minimálne vykonať množina testov preverujúca základnú funkcionalitu systému (správa a prezeranie obchodných informácií, správa rolí, ...).

8.6.3 Ochrana pred zlomyseľným softvérom

Pre zabezpečenie správneho fungovania systému a na ochranu integrity softvéru a údajov treba zabezpečiť systém proti zlomyseľnému softvéru (vírusy, trójske kone, červy a pod.). Toto sa dosahuje implementáciou mechanizmov na detekovanie a prevenciu pred týmto zlomyseľným softvérom (antivírusy, bezpečnostné záplaty, ...). Okrem týchto technických opatrení však treba aj poučenie používateľov, aby si boli vedomí rizík vyplývajúcich z tejto hrozby.

Ochrana pred zlomyseľných softvérom je jedným z dôležitých úkonov pre naplnenie predpokladu o bezpečnom operačnom systéme.

8.6.4 Udržiavanie systému

Cieľom je udržať integritu a dostupnosť služieb spracovávajúcich informácie a komunikačných služieb. V pravidelných intervaloch by sa mali vykonávať zálohy dôležitých obchodných údajov a softvéru pre možnosť prípadného obnovenia systému. Dôležité udalosti systému sú zaznamenávané a v prípade zaznamenanie chybových stavov je toto oznámené, aby sa prijali nápravné opatrenia.

Určovanie, v akých intervaloch treba systém zálohovať, musí zohľadniť okrem iného aj údaj o maximálnej nedostupnosti systému. V prípade, že by maximálna dĺžka nedostupnosti systému mala byť kratšia ako čas potrebný na úplnú obnovu systému (zo zálohy), je toto možné riešiť záložným systémom, pri ktorom je potom potrebné definovať spôsob replikácie údajov.

8.6.5 Správa siete

Keďže prenášané informácie prúdia pomocou počítačových sietí, je potrebné zabezpečiť ich pri tomto prenose. Vnútornú - neverejnú časť siete treba zabezpečiť fyzicky (formou fyzického obmedzenia prístupu neautorizovaných osôb) ale aj logicky (zväčša formou firewalu, ktorý blokuje nepovolenú komunikáciu s vonkajškom). Pri prenose údajov po verejných sieťach treba zabezpečiť údaje primeranou formou (použitie šifrovania alebo podpisov) ak je to primerané.

Fyzické zabezpečenie neverejnej časti musí byť zaručené pre naplnenie predpokladu o fyzickej bezpečnosti systému pre elektronický obchod. Prenos citlivých údajov je riešený pomocou funkčnej požiadavky na zabezpečené cesty medzi systémom a používateľom. Taktiež spojenie medzi systémom

a externými službami (platobný systém, archív, ...) musí byť zabezpečené, pravdepodobne s využitím PKI a certifikátov.

8.6.6 Zaobchádzanie s médiami a bezpečnosť

Keďže pri prevádzke systému sa narába s médiami (pásky, disky a iné), je nutné zabrániť poškodeniu aktív a možným prerušeniam obchodných aktivít spôsobených nesprávnym zaobchádzaním s médiami. V prípade vymeniteľných médií treba definovať postupy práce s médiami tak, aby sa minimalizovala možnosť zneužitia údajov na týchto médiách. Postupy zaobchádzania a uskladňovania médií musia chrániť údaje pred neautorizovaným prezradením a zneužitím. Toto platí aj pri vyraďovaní médií, média treba vyradiť bezpečne, ak už nebudú ďalej používané.

8.6.7 Výmena informácií a softvéru

Pri výmene informácií medzi organizáciami je potrebné zabrániť strate, zmene a zneužitiu vymieňaných informácií. Na dosiahnutie tohto cieľa musia byť uzatvorené dohody pre výmenu údajov medzi organizáciami. Navyše musia byť definované bezpečnostné politiky a postupy, ako bezpečne prenášať údaje vo všetkých používaných spôsoboch (email, zvuk, elektronický systémy atď.), aby nedošlo k ich zneužitiu, prezradeniu alebo poškodeniu.

V rámci komunikácie medzi obchodníkom a systémom musí byť presne definované použitie poskytovaných údajov. Napríklad obchodné informácie od obchodníka majú byť zverejnené v určitú dobu, ale obchodník môže požadovať, že pred zverejnením musia zostať dôverné. Na druhú stranu ale obchodník musí niesť zodpovednosť za tieto informácie a taktiež za informácie, ktoré mu poskytol systém o zákazníkovi pri uzatváraní obchodu medzi obchodníkom a zákazníkom. Tieto pravidlá musia byť právne podchytené pomocou zmlúv. Podobne (aj keď už nie v takej miere) treba upraviť aj výmenu informácií medzi zákazníkom a systémom. Zákazník musí tiež niesť istú zodpovednosť za ním poskytnuté informácie, na druhú stranu systém musí zaručiť korektné zaobchádzanie s týmito údajmi v rámci vopred určených pravidiel.

8.7 Kontrola prístupu

8.7.1 Obchodné požiadavky pre kontrolu prístupu

Pre kontrolu prístupu k informáciám je najprv nutné definovať a zdokumentovať obchodné požiadavky pre túto kontrolu, ktoré hovoria o tom, kto, kde, kedy a za akých podmienok má prístup ku konkrétnym informáciám. Prístup následne musí byť obmedzený len na definovaný v prístupovej politike.

Ako už bolo spomínané skôr, je potrebné definovať zaobchádzanie s informáciami prichádzajúcimi zvonku (obchodné informácie, osobné údaje, ale aj detaily transakcií a pod.). Napríklad len operátor má možnosť modifikovať obchodné informácie. Navyše však treba definovať podmienky prístupu aj k interným informáciám ako sú konfigurácia systému, auditovacie záznamy atď.

8.7.2 Správa prístupu používateľov

Aby sa zabránilo neautorizovanému prístupu k informačným systémom, je potrebné definovať presné postupy pridelenia práv konkrétnym používateľom. Najprv je potrebné formálnym spôsobom stanoviť pravidlá pre udelenie a odobratie prístupu k informačným systémom a službám. Prideľovanie hesiel musí byť kontrolované formálnym procesom.

Následné pridelenie a použitie práv musí byť obmedzené a kontrolované. V pravidelných intervaloch je potrebné revidovať prístupové práva používateľov, aby bola dodržané separácia rolí a bolo možné odhaliť zneužitia právomocí. Okrem nutnosti dodržať pravidlo separácie rolí by administrátor nemal mať možnosť len tak svojvoľne prideľovať práva, ale prideľovanie práv privilegovaných používateľov by malo byť schvaľované definovaným procesom v rámci spoločnosti.

8.7.3 Zodpovednosti používateľov

Pre korektné dodržiavanie prístupových politík je nutné, aby sa používatelia správali zodpovedne. Toto zahŕňa voľbu a používanie hesiel v súlade s dobrými bezpečnostnými praktikami. Ďalej by používateľ nemal nechávať zariadenia bez dostatočnej ochrany pred možným zneužitím (ako napríklad odísť od počítača, keď je tam prihlásený a pod.)

Tieto ciele sa zväčša dosahujú tréningom používateľom, ktorý by mal nielen povedať ako treba veci robiť, ale aj poukázať, prečo je to dôležité. Dodržiavanie týchto praktík by malo byť aj kontrolované a potenciálne sankcionované. Niektoré praktiky sa dajú dosahovať aj nepersonálnymi prostriedkami, napríklad systém môže vyžadovať pravidelné menenie hesiel a zároveň klásť podmienky na zložitosť hesla (použitie špeciálnych znakov atď.).

8.7.4 Kontrola prístupu na úrovni sietí

Na úrovni sietí treba taktiež definovať politiky kontroly prístupu, aby boli chránené sieťové služby. Je potrebné autorizovať používateľov pred využitím služieb. V prípade použitia vzdialených diagnostických portov, je tieto nutné chrániť a kontrolovať.

Kontrola prístupu na úrovni sietí môže napríklad zahŕňať napríklad možnosť pripojenia privilegovaných používateľov len z lokálnych adries a podobne.

8.7.5 Kontrola prístupu na úrovni operačného systému

Pri prihlasovaní používateľa musí tento proces prebehnúť bezpečným spôsobom. Používané heslá musia byť spravované efektívnym spôsobom zaručujúcim kvalitu hesiel (nutnosť pravidelnej zmeny, porovnávanie so slovníkom, vyžadovanie špeciálnych znakov a pod.) Všetci používatelia musia byť jednoznačne identifikovateľní, aby mohli niesť zodpovednosť za svoje činy. Pre zvýšenie bezpečnosti je potrebné neaktívne spojenia po vypršaní primeraného času zrušiť, aby sa zabránilo potenciálnemu neautorizovanému prístupu.

8.7.6 Monitorovanie prístupu a použitia

Na detekciu neautorizovaných aktivít je potrebné generovať auditovacie záznamy bezpečnostne relevantných udalostí a uchovávané aspoň po definovanú dobu (aby nebolo možné hneď odstrániť stopy po vykonaní auditovaných udalostí - na druhú stranu, auditovacie záznamy nemôžu byť udržiavané v systéme navždy, po istom čase by mali byť odzálohované a vymazané). Na ich základe je možné neskôr vyšetrovanie bezpečnostných incidentov a kontrola prístupov. Na prezeranie týchto záznamov musia byť definované postupy a musí sa vykonávať v pravidelných intervaloch. Kvôli presnosti týchto záznamov je nutná synchronizácia počítačových hodín.

Auditovanie udalostí by sa malo týkať najmä dôležitých udalostí, ktoré môžu ovplyvňovať citlivé údaje. Prirodzené je sledovať modifikáciu údajov v systéme, ale v prípade citlivých údajov môže ísť aj o ich čítanie, kde nezvyklá aktivita môže znamenať pokus o únik informácií. Dôležité je tiež sledovať prihlásenia jednotlivých používateľov a najmä neúspešné pokusy o autentifikáciu ako aj neúspešné pokusy o ostatné aktivity (ako napríklad už spomínanú modifikáciu údajov).

8.8 Vývoj systému a údržba

8.8.1 Bezpečnostné požiadavky systému

Obchodné požiadavky na nový systém alebo na vylepšenie existujúceho by mali špecifikovať požiadavky pre bezpečnostné mechanizmy, ktoré ich budú napĺňať. Toto nám zaručí, že bezpečnosť bude zabudovaná do systému a že sa na ňu myslelo už pri definovaní požiadaviek.

Táto požiadavka je v súlade s požiadavkami z CC, podľa ktorých by už hrubý návrh mal uvažovať bezpečnostné aspekty systému.

8.8.2 Bezpečnosť aplikačných systémov

Pre bezpečnejšie spracovávanie údajov v aplikačných systémoch je vhodné používať kontrolné mechanizmy. Pri zadávaní vstupných hodnôt sa vykonáva ich validácia, aby sa zaručilo, že sú korektné a primerané. Slúži to hlavne ako ochrana proti preklepom a chybám používateľa. Pre vnútornú kontrolu je vhodné používať validáciu aj počas spracovávania dát alebo pri ich kontrole výstupných dát.

Pri zadávaní dôležitých informácií (registračné údaje, objednávka) je pred ich odoslaním nutné mať možnosť skontrolovať ešte tieto údaje a prípadne opraviť. Niektoré z informácií (napríklad adresa doručenia tovaru) môžu byť predvypĺňané z uložených údajov, čo redukuje riziko chyby. Samozrejmosťou by mala byť aj základná validácia typov jednotlivých položiek pred odoslaním na spracovanie (je naozaj počet číslo a pod.).

8.8.3 Kryptografické prostriedky

Na zabezpečenie dôvernosti, autentickosti a integrity údajov sa budú využívať kryptografické prostriedky. Využívané bude šifrovanie, elektronické podpisy s využitím služieb certifikačnej autority a služby, ktoré budú vedieť preukázať nastatie či nenastatie určitých udalostí. Použité kryptografické funkcie by mali byť v súlade s uznávanými štandardami.

8.8.4 Bezpečnosť v procese vývoja a podpory

Aby bola zabezpečená bezpečnosť aplikačného softvéru a údajov, je potrebné riadiť zmeny systému. Je nutné definovať pravidlá, ktoré popisujú, akým spôsobom sa zmeny systému majú vykonať. Tieto pravidlá slúžia na minimalizáciu poškodenia informačného systému. Pred nasadením zmien, tieto zmeny by mali byť skontrolované a pretestované, aby tieto zmeny neznefunkčnili časti systému.

Tieto požiadavky sú napĺňané použitím vhodného systému na správu konfigurácií (CM systém), ako vyplýva aj z bezpečnostných záruk PP pre náš systém.

8.9 Zabezpečenie kontinuity

Našou snahou je zabezpečiť neprerušené fungovanie systému a chrániť ho pred zlyhaniami. Dosiahnutie tohto cieľa je riešené pomocou vypracovania strategické plánu založeného na analýze rizík, ktorý poskytuje všeobecný prístup k zabezpečeniu kontinuity obchodných procesov. Tento plán by mal udržať alebo obnoviť obchodné procesy včasným spôsobom. Tento plán musí byť pravidelne revidovaný a aktualizovaný, aby mohol plniť svoju funkciu.

Tento plán proti nepredvídaným udalostiam zväčša obsahuje stratégie zálohovania a následného obnovenia systému. Samozrejme okrem definovania procesov obnovy z rôznych nepredvídaných udalostí obsahuje aj postupy ako predchádzať týmto udalostiam.

8.10 Súlad

Keďže systém má byť reálne používaný, musí byť v súlade so zákonmi (viaceré boli spomínané v časti PP). Je nutné identifikovať relevantné zákony, súlad

s nimi, zaručiť neporušenie vlastníckych práv. Taktiež je nutné, aby systém bol v súlade aj s organizačnými politikami a inými predpismi platnými pre organizáciu, ktorá prevádzkuje daný systém. Súlad musí byť pravidelne kontrolovaný a udržiavaný.

Systém pre elektronický obchod musí byť v súlade najmä so zákonom o elektronickom obchode (22/2004 Z.z.) a so zákonom o ochrane osobných údajov (363/2005 Z.z.) ako aj ostatnými zákonmi. Okrem toho náš systém musí byť v súlade aj direktívami Európskej únie a to najmä s direktívou o predaji na diaľku (97/7/EC) a s direktívou o elektronickom obchode (2000/31/EC). Zodpovednosti medzi vystupujúcimi stranami (obchodník, zákazník, správca systému) musia byť taktiež právne podložené.

Pravidlá vyplývajúce zo štandardu ISO/IEC 17799 sa čiastočne prekrývajú s niektorými požiadavkami z CC, ale okrem toho pomáhajú zapĺňať medzeru v nie informačných požiadavkách na systém a jeho správu. Pomáhajú napĺňať bezpečnostné ciele na prostredie (ktoré zahŕňajú aj predpoklady prostredia TOE).

Časť V

Záver

V tejto práci sme podali čitateľovi základný prehľad o systémoch pre elektronický obchod. Analyzovali sme základné modely elektronického obchodu, ich účastníkov a vzťahy medzi nimi. Uviedli sme možné príklady použitia takýchto systémov v praxi.

Ďalej sme sa venovali hlavnej časti tejto práce - bezpečnostným aspektom elektronického obchodu. Čitateľa sme uviedli do základov kryptografie a informačnej bezpečnosti. Taktiež sme predstavili štandard, podľa ktorého sme nakoniec vybudovali bezpečnostný model pre množinu systémov elektronického obchodu. Úroveň bezpečnosti sme postavili relatívne vysoko, avšak bez nutnosti zásadne meniť existujúce dobré zvyklosti pri návrhu a vývoji systémov. Uvedený model sme doplnili aj o zásady správnej prevádzky a správy pre komplexnejšej pohľad na bezpečnosť.

Možnými rozšíreniami tejto práce by mohli byť najmä pokusy škálovať systém buď na úrovni dosahovanej bezpečnosti, poskytovanej funkčnosti alebo spracovať bezpečnostný model pre systémy iných typov elektronického obchodu. Ďalšou možnosťou by bolo rozpracovanie profilu ochrany do formy bezpečnostného zámeru (ST).

Dodatok A

Slovník pojmov a skratiek

V tejto časti sa nachádza slovník použitých termínov a skratiek spolu so stručným popisom a s prekladom, ak existuje vhodný preklad.

Advanced Encryption Standard, AES Symetrická bloková šifra, ktorá sa momentálne považuje za dostatočne bezpečnú.

AES *viď. Advanced Encryption Standard*

Assets (Aktíva) Informácie alebo zdroje, ktorá majú byť chránené systémom.

Asymmetric cryptosystem (Asymetrický kryptosystém) Taký systém, ktorý používa dva kľúče : verejný na šifrovanie a súkromný na dešifrovanie. Z verejného kľúča je výpočtovo neuskutočniteľné nájsť súkromný kľúč.

Authentication (Autentifikácia) Proces overovania identity účastníka.

Authorization (Autorizácia) Proces zisťovania, či daný účastník má právo vykonať konkrétnu akciu.

B2B *viď. Business-to-business*

B2C *viď. Business-to-customer*

Block cipher (Bloková šifra) Šifra šifrujúca text po blokoch pevnej dĺžky.

Business-to-business, B2B Elektronický obchod prebiehajúci medzi obchodníkmi (organizáciami).

Business-to-customer, B2C Elektronický obchod prebiehajúci medzi obchodníkom a zákazníkom.

CA *viď. Certification Authority*

CC *viď. Common Criteria*

Certificate Revocation List, CLR Zoznam revokovaných - zneplatnených certifikátov.

Certification Authority (Certifikačná autorita) Dôveryhodná autorita, ktorá vydáva digitálne certifikáty.

Cipher text (Šifrový text) Výsledok procesu šifrovania.

CLR *viď. Certificate Revocation List*

CM *viď. Configuration Management*

Common Criteria Štandard ISO 15408 slúžiaci primárne na vyhodnocovanie bezpečnostných vlastností IT produktov a systémov.

Computational secure cryptosystem (Výpočtovo bezpečný kryptosystém) Taký systém, ak najlepšie známe algoritmy potrebujú na jeho prelomenie príliš veľa výpočtovej sily.

Confidentiality (Dôvernosť) Zaručenie, že informácie sú dostupné len autorizovaným účastníkom.

Configuration Management (Správa konfigurácií), CM Súbor pravidiel, zodpovedností, úloh/cieľov a nástrojov na správu konfigurácií (teda zdrojových kódov, dokumentácie, modelov, atď.).

Countermeasures (Protiopatrenia) Spôsoby bránenia sa riziku a jeho redukcie na prijateľnú úroveň.

Cryptography (Kryptografia) Veda zaoberajúca sa najmä udržaním tajnosti správ a zaručením autentickosti.

Cryptosystem (Kryptosystém) Systém pozostávajúci zo šifrovacieho a dešifrovacieho algoritmus.

E-commerce (Elektronický obchod) Výmena alebo spracovávanie obchodných informácií pomocou počítačov spojených v sieti.

EAL *viď. Evaluation Assurance Level*

EDI *viď. Electronic Data Interchange*

Electronic Data Interchange, EDI Protokol slúžiaci na výmenu štruktúrovaných správ.

Evaluation Assurance Level, EAL Balík bezpečnostných záruk z CC, ktorý reprezentuje určitý stupeň záruk.

Extensible Markup Language, XML Všeobecný značkovací jazyk slúžiaci na popis dát.

File Transfer Protocol, FTP Protokol slúžiaci na prenos súborov po sieti.

FTP *viď. File Transfer Protocol*

G2C *viď. Government-to-citizen*

Government-to-citizen, G2C Interakcia medzi vládou a súkromnou osobou pomocou počítačovej siete.

Hash function (Hašovacia funkcia) Funkcia vytvárajúca malé digitálne odtlačky z ľubovoľných dát.

Hybrid cryptosystem (Hybridný kryptosystém) Kombinácia prístupov symetrických a asymetrických kryptosystémov: Na šifrovanie sa používa symetrická šifra, kľúč tejto symetrickej šifry je prenesený pomocou asymetrickej šifry.

Information Technology (Informačné technológie), IT Téma zaoberajúca sa technológiou a inými aspektmi spracovávania informácií.

Integrity (Integrita) Vlastnosť vyjadrujúca kompletnosť a neporušenosť.

International Organization for Standardization, ISO Medzinárodná organizácia produkujúca celosvetové štandardy.

ISO *viď. International Organization for Standardization*

IT *viď. Information Technology* Tiež používané ako skratka pre *informačný.*

Key (Kľuč) Informácia určujúca priebeh kryptografických protokolov. Zväčša sa hovorí o kľúči pri šifrovaní a dešifrovaní.

Key agreement (Dohody kľúčov) Protokol, kde hodnoty kľúčov sú vytvorené na základe údajov viacerých strán.

Key distribution (Distribúcia kľúčov) Protokol, pri ktorom jeden účastník určí kľúč a distribuuje ho medzi ostatných účastníkov.

Man in the middle (Útočník uprostred) Útok, pri ktorom oponent zachytáva komunikáciu medzi dvoma stranami a pozmenenú posiela ďalej predstierajúc identitu pôvodcu originálnej správy.

National Institute of Standards and Technology, NIST Americká agentúra pre tvorbu štandardov a podporu technológií.

NIST *viď. National Institute of Standards and Technology*

PDCA Skratka pre procesný model "Plan-Do-Check-Act"(Plánovanie-vykonanie-kontrola-reakcia).

Personal Identification Number, PIN Informácia slúžiaca ako forma autentifikácie používateľa.

PIN *viď. Personal Identification Number*

PKI *viď. Public Key Infrastructure*

Plain text (Otvorený text) Pôvodná informácia, ktorá má byť chránená procesom šifrovania.

PP *viď. Protection Profile*

Privacy (Súkromie) Zaručenie, že osobné údaje jednotlivca alebo skupiny sa nedostanú k neautorizovaným účastníkom.

Protection Profile (Profil ochrany), PP Implementačne nezávislá množina bezpečnostných požiadaviek pre skupinu TOE, ktorá spĺňa potreby spotrebiteľa.

Public key certificate (Certifikát verejného kľúča) Digitálny dokument, ktorého vydavateľ potvrdzuje, že v ňom uvedený verejný kľúč je spojený s konkrétnou identitou.

Public key cryptography (Kryptografia verejných kľúčov) Forma kryptografie dovoľujúca účastníkom bezpečne komunikovať bez dopredu dohodnutého tajného kľúča.

Public Key Infrastructure, PKI Súhrn protokolov, služieb a štandardov na podporu aplikácií používajúcich kryptografiu verejných kľúčov.

Request For Comments, RFC Séria internetových informačných dokumentov a štandardov.

RFC *viď. Request For Comments*

Risk (Riziko) Funkcia pravdepodobnosti nastatia hrozby a možného dopadu.

RSA Asymetrická šifra, jej názov pochádza z iniciálov jej vynálezcov : Rivest, Shamir a Adleman

Secure Electronic Transaction, SET Protokol pre bezpečné spracovávanie transakcií kreditných kariet.

Secure Sockets Layer, SSL Protokol pre bezpečnú komunikáciu po sieti.

Security Function Policy, SFP Bezpečnostné politiky vynútené pomocou SF.

Security Function, SF Časti TOE, ktoré vynucujú úzko súvisiacu podmnožinu z TSP.

Security Target (Bezpečnostný zámer), ST Množina bezpečnostných požiadaviek a špecifikácií použitá pre vyhodnotenie identifikovaného TOE.

SET *viď. Secure Electronic Transaction*

SFP *viď. Security Function Policy*

SF *viď. Security Function*

Signature scheme (Podpisová schéma) Schéma pozostajúca z podpisovacieho algoritmu a z overovacieho algoritmu, pomocou ktorého vieme overiť pravosť podpisu.

Simple Object Access Protocol, SOAP Protokol na výmenu XML správ cez počítačovú sieť.

SOAP *viď. Simple Object Access Protocol*

SOF *viď. Strength of Function*

SSL *viď. Secure Sockets Layer*

Stream cipher (Prúdová šifra) Šifra šifrujúca text ako prúd znakov.

Strength of Function, SOF Predpoklad pre bezpečnostné funkcie TOE vyjadrujúci minimálne úsilie potrebné na obídenie očakávaného správania bezpečnostných funkcií.

ST *viď. Security Target*

Symmetric cryptosystem (Symetrický kryptosystém) Taký systém, kde sa na šifrovanie aj dešifrovanie používa ten istý kľúč.

Target of Evaluation, TOE IT produkt alebo systém a jeho príslušná administrátorská a používateľská dokumentácia, ktorý je predmetov vyhodnocovania.

TELNET Sieťový protokol pre všeobecnú dvojsmernú komunikáciu.

Threat (Hrozba) Potenciálna odchýlka od pravidiel, podľa ktorých by mal fungovať systém.

Timestamps (Časové pečiatky) Digitálny dokument, ktorého vydavateľ dosvedčuje existenciu datovaného dokumentu v danom čase.

TLS *viď. Transport Layer Security*

TOE Security Functions, TSF Množina všetkého hardvéru, softvéru a firmvéru TOE, ktorá vynucujú korektné uplatnenie TSP.

TOE Security Policy, TSP Množina pravidiel, ktoré určujú ako sa narába s aktívami, ako ich treba chrániť a distribuovať v rámci TOE.

TOE *viď. Target of Evaluation*

Transport Layer Security, TLS Protokol pre bezpečnú komunikáciu po sieti. Nasledovník SSL.

TSC *viď. TSF Scope of Control*

TSF Scope of Control, TSC Množina interakcií, ktoré môžu nastať s TOE alebo v rámci TOE a sú predmetom pravidiel z TSP.

TSF *viď. TOE Security Functions*

TSP *viď. TOE Security Policy*

UDDI *viď. Universal Description, Discovery and Integration*

Unconditional secure cryptosystem (Bezpodmienečne bezpečný kryptosystém) Taký systém, ak nemôže byť prelomený ani s neobmedzenou výpočtovou silou.

Universal Description, Discovery and Integration, UDDI Protokol založený na XML, ktorý poskytuje adresár, ktorý umožňuje obchodníkom a organizáciám zverejniť svoje služby, vyhľadávať iné služby a definuje, ako tieto služby môžu spolupracovať.

Vulnerability (Zraniteľnosť) Predpoklad pre naplnenie konkrétnej hrozby.

Web services (Webovské služby) Množina protokolov a štandardov na výmenu údajov medzi aplikáciami.

XML *viď. Extensible Markup Language*

Literatúra

[1] *Advanced Encryption Standard*
FIPS PUB 197, NIST, 2001
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12, 1995

[3] Forišek, Michal
Archív elektronických dokumentov, diplomová práca, FMFI UK, 2004

[4] *Common Criteria for Information Technology Security Evaluation*, verzia 2.1, 1999, štandard ISO/IEC 15408

[5] *Configuration management*, materiál k prednáškam z predmetu Softvérové inžinierstvo, FMFI UK

[6] Stoneburner, Gary
COTS Security Protection Profile - Operating Systems, (Worked Example Applying Guidance of NISTIR-6462, CSPP), verzia 1.0, 2003

[7] Stinson, Douglas
Cryptography: Theory and Practice, CRC Press, 1995

[8] *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*
http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/
l_178/l_17820000717en00010016.pdf

[9] *Directive 97/7/EC on the protection of consumers in respect of distance contracts*

http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf

[10] Spiliopoulos, Spilios
e-Commerce, Athens University of Economics and Business, GR
http://www2.ellinogermaniki.gr/ep/agroweb/htmls/lessons/commerce1/E_Commerce_material.zip

[11] IDC/LINK, Forrester, Mercer Internet Database
prevzaté z Gert E. Bielefeld
e-Commerce/e-Business focussed on Business to Business, The Information Economy in Eastern Europe, Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik Berlin, April 2000

[12] Delina, Radoslav
Elektronické trhy, AT&P Journal 10/2002

[13] *Formát XML*
http://www.w3.org/XML/

[14] Swanson, Marianne, Guttman, Barbara
Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST Special Publication 800-14, 1996

[15] Swanson, Marianne
Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, 1998

[16] *Information security management - Part2: Specification for information security management systems*, BS 7799-2, Draft for Public Comment, 2002

[17] *Information technology - Code of practice for information security management*
štandard ISO/IEC 17799:2000(E)

[18] *Jednotný automatizovaný systém právnych informácií*
http://jaspi.justice.gov.sk/

[19] Delina, Radoslav
Marketing and the Internet, materiál k prednáškam z predmetu Elektronický obchod, KBaI, Ekonomická fakulta, TU Košice

[20] *Model integrovaných e-služieb verejnej správy*, príloha Bezpečnostné aspekty systému integrovaných e služieb verejnej správy, číslo úlohy podľa číselníka IS VVP: 2003 SP 20 029 01 02, 2005

[21] *Prezentácie NBÚ o elektronickom podpise*
http://www.nbusr.sk/NBU_SEP/leg_rozne/all_pps.zip

[22] *Protokol TLS, verzia 1.0*
http://www.ietf.org/rfc/rfc2246.txt

[23] *Public-Key Cryptography Standards*
edícia štandardov a de facto štandardov PKI, RSA Laboratories
http://www.rsasecurity.com/rsalabs/node.asp?id=2124

[24] *RSA Cryptography Standard*
PKCS #1, RSA Laboratories
http://www.rsasecurity.com/rsalabs/node.asp?id=2125

[25] *Špecifikácia protokolu SSL 2.0*
http://wp.netscape.com/eng/security/SSL_2.html

[26] *Štandard UN / EDIFACT*
http://www.unece.org/trade/untdid/welcome.htm

[27] Choi, Soon-Yong, Stahl, Dale O. and Whinston, Andrew B
The economics of electronic commerce, Macmillian Technical Publishing 1997.

[28] Jansen, Wayne, Walsh, Jack, Dolan, Kathy V., Wright, Patricia A.
U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Enviroments., verzia 1.1, 1999

[29] *Wikipedia*, the free encyclopedia
http://www.wikipedia.org/

[30] *World Wide Web Consortium*
http://www.w3.org/

[31] *Public-Key Infrastructure (X.509)*
http://www.ietf.org/html.charters/pkix-charter.html

[32] Delina, Radoslav
Základy e-obchodu, materiál k prednáškam z predmetu Elektronický obchod, KBaI, Ekonomická fakulta, TU Košice
http://www.tuke.sk/ekf-kbai/delina/zakladyEO.doc

[33] Stanek, Martin
Základy kryptológie, material k prednáškam z predmetu Kryptológia, FMFI UK