

Ochrana osobních dat a přístup k informacím na UTB ve Zlíně

Bc. Michaela Beranová

Diplomová práce
2005



Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně

Fakulta managementu a ekonomiky

Ústav managementu

akademický rok: 2004/2005

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Michaela BERANOVÁ**

Studijní program: **N 6208 Ekonomika a management**

Studijní obor: **Management a marketing**

Téma práce: **Ochrana osobních dat a přístup k informacím na UTB ve Zlíně**

Zásady pro vypracování:

1. Provedte rozbor literárních pramenů vztahujících se k ochraně osobních dat a přístupu k informacím.
2. Provedte analýzu současného stavu ochrany osobních dat na UTB ve Zlíně.
3. Diagnostikujte riziková místa.
4. Navrhněte možnosti zvýšení úrovně ochrany osobních dat.
5. Iniciujte jejich realizaci na UTB.

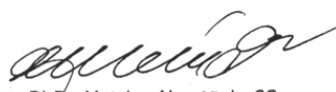
Rozsah práce: 70 stran
Rozsah příloh:
Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

- 1) MATOUŠOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. Kniha pro praxi. 1. vydání. Praha: ASPI Publishing, 2003. ISBN 80-86395-50-2.
 - 2) PŘIBYL, J., KODL, J. Ochrana dat v informatice. 1. vydání. Praha: ČVUT, 1997. ISBN 80-01-01664-1.
 - 3) JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. 1. vydání. Zlín: UTB ve Zlíně, 2002. ISBN 80-7318-095-2.
 - 4) MUSIL, R. Ochrana utajovaných skutečností. 1. vydání. Praha: EUROUNION, 2001. ISBN 80-85858-93-2.
 - 5) BENDA, R., ROSMAN, P., SODOMKA, P. Informatika a výpočetní technika. 1. vydání. Zlín: VUT v Brně, FaME, 1999. ISBN 80-214-1396-4.
- další dle doporučení vedoucího diplomové práce

Vedoucí diplomové práce: JUDr. Libor Šnédar, Ph.D.
Ústav managementu
Datum zadání diplomové práce: 7. března 2005
Termín odevzdání diplomové práce: 13. května 2005

Ve Zlíně dne 7. března 2005


doc. PhDr. Václav Nováček, CSc.
děkan




Ing. Pavla Staňková, Ph.D.
ředitel ústavu

ABSTRAKT

Abstrakt česky

Diplomová práce se zabývá problematikou ochrany osobních dat na Univerzitě Tomáše Bati ve Zlíně. Tuto problematiku řeším ze dvou hledisek, a to z hlediska práva a informatiky. V analytické části mapuji situaci na UTB v oblasti ochrany dat, co se týče povinností zaměstnanců a dodržování pravidel provozu počítačové sítě. Další částí je oblast použitých informačních systémů a jejich specifik. Zde se podrobně věnuji informačním technologiím (šifrovací kanály, antivirová ochrana apod.) aplikovaných na UTB. Následně hledám rizikové místo ochrany dat a v projektu navrhuji možný prostředek pro zlepšení úrovně ochrany dat na UTB.

Abstrakt v anglickém jazyce

This Master thesis deals the personal data protection at the Tomas Bata University in Zlín. It consists of the legal and the informatics part. The analytic part consists of the data protection examination at the UTB, as for the staff responsibility and the abidance by the rules of the network operation. After that I describe the applied information systems and its specifications. There I examine in detail the information technology (i.e. cipher channel, antivirus protection and so on) applied at the UTB. Subsequently I explore a potential weakness in the data protection. Finally I propose the recommendation for an improvement of the personal data protection at the Tomas Bata University and its implementation.

Za pomoc a odbornou konzultaci při zpracování mé diplomové práce bych chtěla poděkovat vedoucímu práce, JUDr. Liboru Šnédarovi, PhD., Ing. Romanu Jaškovi, PhD., dále garantovi mé práce Ing. Richardu Hornákovi a JUDr. Editě Gybasové.

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a použitou literaturu jsem citovala.

Vedení organizace, pro kterou se zpracovávala diplomová práce, jejíž název je uveden v práci a jejíž data byla v práci využita, nesouhlasí se zapůjčením práce třetí osobě.

Ve Zlíně dne 13. 5. 2005

.....

OBSAH

OBSAH.....	5
ÚVOD.....	8
I. TEORETICKÁ ČÁST	9
1 PRÁVNÍ ZAKOTVENÍ OCHRANY OSOBNÍCH DAT.....	10
1.1 SMYSL OCHRANY OSOBNÍCH DAT	10
1.1.1 Zákon o ochraně osobních dat.....	11
1.1.2 Trestní zákon	11
1.1.3 Vymezení základních pojmů	12
1.1.4 Správce a zpracovatel.....	13
2 INFORMACE	16
2.1 HODNOTA INFORMACE	16
2.2 BEZPEČNOST INFORMACE	16
2.3 ZÁKLADNÍ METODY OCHRANY DAT	18
2.3.1 Šifrování	19
2.3.2 Autentizace.....	21
3 INTERNET	23
3.1 ŘEŠENÍ BEZPEČNOSTI NA INTERNETU.....	23
3.2 VIRY.....	23
3.3 FIREWALL.....	24
II. PRAKTICKÁ ČÁST.....	25
4 STANOVENÍ HYPOTÉZY	26
5 OCHRANA DAT V INFORMAČNÍM SYSTÉMU UTB.....	27
5.1 POVINNOSTI VEDOUCÍCH ZAMĚSTNANCŮ	27
5.2 POVINNOSTI ZAMĚSTNANCŮ	28
5.3 POSKYTOVÁNÍ INFORMACÍ NA UTB	29
5.3.1 Žádost o poskytnutí informace.....	29
5.4 DODRŽOVÁNÍ AUTORSKÉHO ZÁKONA	30
6 PRAVIDLA PROVOZU POČÍTAČOVÉ SÍTĚ UTB.....	31
6.1 SPRÁVCE SÍTĚ UTB	31
6.2 UŽIVATELE SÍTĚ	32
6.3 OCHRANA AUTORSKÝCH PRÁV, DAT A INFORMACÍ	32
6.4 PŘÍSTUPOVÁ PRÁVA A IDENTIFIKACE UŽIVATELE	33
7 SYSTÉM STAG.....	35
7.1 PŘIHLÁŠENÍ DO SYSTÉMU	36
7.2 OCHRANA DAT V SYSTÉMU STAG	38
7.2.1 Databázový server – databáze Oracle 9i	38

7.2.2	Aplikace STAG	40
7.2.3	WWW rozhraní STAGu.....	40
7.2.4	Protokol HTTPS	41
7.2.5	SSL protokol	41
7.2.6	SSH.....	44
7.2.7	PGP.....	45
7.3	SPRÁVCE STAGU	45
7.4	SYSTÉM STAG NA JINÝCH VŠ A VOŠ.....	46
8	SYSTÉM SAP	47
8.1	EKONOMICKÝ INFORMAČNÍ SYSTÉM SAP.....	47
8.2	OCHRANA DAT V SYSTÉMU SAP.....	47
8.3	UŽIVATELÉ.....	48
8.4	FUNKCE SAPU	49
8.5	SYSTÉM SAP NA JINÝCH VŠ.....	50
9	ANTIVIROVÁ OCHRANA	51
9.1	ANTIVIROVÝ SYSTÉM NOD32.....	51
9.2	ANTISPAMOVÁ OCHRANA	52
10	RIZIKOVÁ MÍSTA OCHRANY DAT NA UTB	53
10.1	SELHÁNÍ LIDSKÉHO FAKTORU.....	53
III.	PROJEKTOVÁ ČÁST.....	54
11	PROSTŘEDKY PRO VYŠŠÍ BEZPEČNOST	55
12	ZAVEDENÍ E-PODPISU NA UTB.....	56
12.1	ELEKTRONICKÝ PODPIS	57
12.1.1	Hashovací funkce	58
12.1.2	Jak vytvořit elektronický podpis	59
12.1.3	Podepisování	59
12.2	CERTIFIKAČNÍ AUTORITA A CERTIFIKÁTY	60
12.2.1	Tvorba a životnost certifikátu	61
12.2.2	Komerční a kvalifikované certifikáty.....	63
12.3	CERTIFIKAČNÍ AUTORITA I.CA.....	63
12.3.1	Časová razítka	64
12.3.2	Reference.....	65
12.3.3	Ceník služeb I.CA	65
12.3.4	Certifikační politika I.CA.....	66
12.3.5	Certifikáty Standard a Comfort	69
12.3.6	Osobní kvalifikovaný certifikát Comfort	70
13	RODNÁ ČÍSLA A BUDOUCNOST	74
	ZÁVĚR.....	75
	SEZNAM POUŽITÉ LITERATURY	77
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	80

SEZNAM OBRÁZKŮ	82
SEZNAM TABULEK.....	83

ÚVOD

Tématem mé diplomové práce je Ochrana osobních dat a přístup k informacím na UTB ve Zlíně. Je třeba říci, že se jedná, zejména v současné době, o velmi aktuální téma, což bylo hlavním důvodem mého výběru.

Problematika ochrany bezpečnosti informačního systému a dat se dostává stále více do popředí zájmu managementu každé organizace, ale i řadových zaměstnanců. Bezpečnost informačního systému zahrnuje ochranu všech prostředků informačního systému a dat v něm uložených, dále ochranu všech dat, která jsou v něm zpracovávána, ukládána a jeho prostřednictvím přenášena, a v neposlední řadě také ochranu všech jeho technických i netechnických prostředků, a proto je důležité věnovat tomuto tématu pozornost.

Organizace pracující s daty v tištěné, ale především v digitální podobě, jsou si vědomy, že je nutné tato data chránit a zabránit tak jejich vyzrazení neoprávněným osobám, neautorizované modifikaci či manipulaci s daty. Je vhodné, aby organizace zajistila bezpečnost dat systémově jako součást své bezpečnostní politiky zahrnující pravidla pro přístup subjektů k informacím a prostředkům informačního systému, pravidla pro výběr bezpečnostních funkcí, produktů a mechanismů a pro analýzu a ocenění rizik.

Mým hlavním cílem bylo zmapovat situaci v oblasti ochrany dat na UTB a zamyslet se nad tím, jakým způsobem by se dala úroveň této ochrany zvýšit.

Práci jsem pojala ze dvou hledisek, a to z hlediska právního a z hlediska informačního. V teoretické části jsem vycházela ze znalosti příslušných zákonů a z teoretického základu o bezpečnosti ochrany dat.

Moje práce zkoumá především ochranu osobních dat ve smyslu správného nakládání s informacemi, vhodných informačních systémů zabezpečujících tyto informace, a to vše za přítomnosti Zákona o ochraně osobních dat.

Věřím, že tato diplomová práce bude určitým přínosem pro Univerzitu Tomáše Bati ve Zlíně a poslouží k jejím interním účelům.

I. TEORETICKÁ ČÁST

1 PRÁVNÍ ZAKOTVENÍ OCHRANY OSOBNÍCH DAT

Existují tři roviny ochrany osobních dat:

- 1) Základní lidská práva
- 2) Právní rovina
- 3) Zabezpečení osobních údajů před únikem a zneužitím.

Jako subjekt údajů máme především práva, v ostatních rolích spíše povinnosti. V oněch ostatních rolích nám občas také přísluší být tím, kdo vyvažuje, např. zájmy a požadavky ochránců osobních údajů a informatiků. Ekonomicky odůvodněným ideálem informatiků je totiž opakovaně využívat jednou získané informace (údaje), ideálem skálních ochranářů osobních údajů nepřipustit využití žádného osobního údaje k jinému účelu, než pro který byl daný osobní údaj získán. [1]

Právo na informace je upraveno velkým počtem zákonů; většina z nich řeší a organizuje přístup k informacím v souvislosti s určitou právně regulovanou činností, jako je např. výběr a odvádění daní či poskytování sociálních dávek. Tuto úpravu označujeme jako „odvětvovou“, která bývá doplněna tzv. „průřezovou“ úpravou – u nás zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Ochranu soukromí a osobních dat upravuje mnoho zákonů. Jsou to tytéž zákony, které upravují rovněž přístup k informacím, v případě, že mezi takovými informacemi jsou i osobní data. V řadě zemí je ochrana osobních dat zakotvena v ústavě, ale za náležitou úpravu se považuje existence zákona o ochraně osobních dat. Aktuální zákon v ČR byl vyhlášen jako zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

1.1 Smysl ochrany osobních dat

Zájem o osobní data a jejich ochranu patří k aktuálním tématům tohoto tisíciletí ve veřejném životě všech obyvatel. Lidé vnímají mnohem citlivěji problémy spojené s osobními daty, bez ohledu na jejich věk či postavení. Pro bezpečnou orientaci v této problematice je nejdůležitější pochopit fenomén ochrany osobních dat.

Právní předpisy k ochraně osobních dat vznikly v 70. letech 20. století.

Lidé mohou jen nepatrně ovlivnit vytváření osobních dat, které se jich týkají, a proto jim musí zákony poskytnout určité záruky a jistou ochranu. Povinnost data chránit má za úkol ten, kdo je zjišťuje, zpracovává a popř. i sděluje. Chráněn je jednotlivec, resp. fyzická osoba.

Cílem ochrany osobních dat není absolutně bránit používání osobních dat jiných lidí, ale zabránit jejich zneužití a rovněž umožnit jejich zpřístupnění pro legální účely. V prostředí mezinárodních organizací se mluví o tzv. „volném toku“.

1.1.1 Zákon o ochraně osobních dat

Zákon o ochraně osobních dat a změně některých zákonů, tj. zákon č. 101/2000 Sb. nabyt účinnosti dnem 1. června 2000. Tento zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států.

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, pokud tento zákon nebo zvláštní zákon nestanoví jinak. Vztahuje se na veškeré zpracovávání osobních údajů, ať už k němu dochází automatizovaně nebo jinými prostředky.

Hlavním záměrem tohoto zákona je chránit citlivé údaje více než běžná osobní data. Každý informační systém, jež zpracovává osobní data, má svého správce. Ten může zpracovávat osobní data pouze se souhlasem subjektu údajů. Před zahájením je nutné zažádat o jeho registraci *Úřad pro ochranu osobních údajů*, jež má na starosti výkon záměru tohoto zákona včetně dozoru nad jeho dodržováním, a to od poloviny roku 2000.

Zpracování osobních údajů pro účely statistické a archivnictví stanoví zvláštní zákony, a to Zákon č. 89/1995 Sb., Zákon č. 158/1999 Sb. a Zákon č. 97/1974 Sb.

Z porušení zákona o ochraně osobních dat hrozí trestný postih. V § 178 trestního zákona č. 140/1961 Sb., ve znění pozdějších předpisů, je vymezena skutková podstata trestného činu neoprávněného nakládání s osobními údaji.

1.1.2 Trestní zákon

Kdo neoprávněně nakládá s osobními údaji (byť z nedbalosti), tzn. že neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném, bude podle § 178 potrestán odnětím svobody až na tři roky nebo zákazem činnosti či peněžitým trestem.

Stejně bude potrestán i ten, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.

Lidé, jež přicházejí do styku s utajovanými skutečnostmi legálně, se vyskytují ve vybraných organizacích a s těmito skutečnostmi nakládají v mnohem menším objemu než lidé, kteří osobní data zpracovávají.

1.1.3 Vymezení základních pojmů

Osobní údaj – jakýkoliv údaj, který se týká určeného nebo určitelného subjektu údajů – tj. jestliže je možné na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, jestliže je ke zjištění identity subjektu údajů zapotřebí nepřiměřené množství času, úsilí či materiálních prostředků.

Citlivý údaj – osobní údaj, jež vypovídá o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborech, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů.

Anonymní údaj – údaj, který nelze vztáhnout k subjektu údajů.

Subjekt údajů – fyzická osoba, ke které se vztahují osobní údaje.

Zpracování osobních údajů – jakákoliv operace či soustava operací, jež správce nebo zpracovatel systematicky provádějí s osobními údaji, a to buď automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se má na mysli hlavně shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Shromažďování osobních údajů – systematický postup nebo soubor postupů s cílem získání osobních dat za účelem dalšího uložení na nosič informací pro okamžité či pozdější zpracování.

Uchovávání osobních údajů – zachování údajů v podobě, která umožní jejich další zpracování.

Blokování osobních údajů – stav, při němž není osobní údaj po určitou dobu přístupný a není možné jej jinou cestou zpracovávat.

Likvidace osobních dat – fyzické zničení nosiče, tzn. jejich fyzické vymazání či jejich vyloučení z dalších zpracování natrvalo.

Správce – subjekt určující účel a prostředky zpracování dat, toto zpracování provádí a odpovídá za něj. Zpracováním může správce zmocnit či pověřit zpracovatele, pokud nestanoví zvláštní zákon jinak.

Zpracovatel – subjekt zpracovávající osobní údaje na základě zvláštního zákona či pověřením správce.

Zveřejněný osobní údaj – údaj, který je zpřístupněn zejména pomocí hromadných sdělovacích prostředků, jiným veřejným sdělením či jako součást veřejného seznamu.

1.1.4 Správce a zpracovatel

Na zpracování osobních dat se podílejí tyto subjekty:

- správce,
- zpracovatel,
- zaměstnanci správce nebo zpracovatele,
- jiné osoby.

Správce

Podle § 5 musí správce stanovit účel zpracování osobních dat, dále prostředky a způsob jejich zpracování, musí zpracovávat jen pravdivé a přesné osobní data, které získal v souladu se zákonem. Dále je povinen shromažďovat data, která odpovídají jen stanovenému účelu a v rozsahu nutném pro naplnění tohoto účelu. Data uchovává pouze po dobu potřebnou k účelu jejich zpracování. Správce musí všechny údaje zpracovávat pouze se souhlasem subjektů údajů. Bez souhlasu je může zpracovávat jen za zákonem stanovených podmínek.

Pokud provádí zpracování dat podle zvláštních zákonů, jako je např. Zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, musí dbát práva na ochranu soukromého a osobního života subjektu dat. Bez souhlasu subjektu dat je možné zpracovávat osobní data pro statistické či vědecké účely.

Provádí-li správce nebo zpracovatel zpracování osobních dat za účelem nabízení obchodu nebo služeb subjektu dat, může pro tento účel použít jméno, příjmení a adresu subjektu údajů, a to za předpokladu, že byly tyto údaje zjištěny z veřejného seznamu či v souvislosti se svojí činností jakožto správce či zpracovatele. Jiný správce, jemuž byly údaje předány, nesmí tato data předávat jiné osobě.

Jestliže zpracovatel zjistí, že správce porušuje povinnosti tímto zákonem stanovené, musí jej na to neprodleně upozornit a ukončit zpracování těchto údajů. V případě, že tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, a to společně se správcem údajů.

Povinnosti správce

- 1) povinnost stanovit účel,
- 2) povinnost stanovit prostředky a způsob zpracování,
- 3) povinnost získat souhlas subjektu údajů,
- 4) oznamovací povinnost,
- 5) příprava zpracování,
- 6) povinnost zpracovávat pravdivé a přesné osobní údaje,
- 7) povinnost shromažďovat údaje odpovídající účelu a v nezbytném rozsahu,
- 8) povinnost uchovávat osobní údaje pouze po nezbytnou dobu,
- 9) povinnost zpracovávat osobní údaje v souladu s původním účelem,
- 10) povinnost shromažďovat osobní údaje otevřeně,
- 11) povinnost nesdružovat osobní údaje,
- 12) povinnost přijmout bezpečnostní opatření,
- 13) další povinnosti při zpracování osobních údajů,
- 14) povinnosti spojené s poskytnutím osobních údajů do zahraničí,
- 15) povinnosti při ukončení zpracování.

Zpracovatel

Zpracovatel osobních dat má následující povinnosti:

- dbát při zpracování osobních dat na to, aby subjekt údajů neutrpěl žádnou újmu na svých právech, a to zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů podle ustanovení § 10,
- přijmout taková opatření, aby nemohlo dojít k neoprávněnému či nahodilému přístupu k osobním datům, dále k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních dat podle ustanovení § 13,
- stanovit podmínky a rozsah, za nichž a v němž zaměstnanci správce či zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy, mohou zpracovávat osobní data dle ustanovení § 14,
- provést likvidaci osobních dat na základě pokynu správce dle ustanovení § 20.

Správce musí ukončit zpracování údajů po pominutí uvedených důvodů, údaje musí zlikvidovat.

Při zpracování údajů dbá zpracovatel i správce na to, aby subjekt údajů neutrpěl žádnou újmu na svých právech, a to zejména na právu na zachování lidské důstojnosti. Dbá také na ochranu před neoprávněným zasahováním soukromého a osobního života subjektu údajů.

2 INFORMACE

2.1 Hodnota informace

Pojem informace je v současné době jedním z nejčastěji používaných pojmů a má nespornou úlohu v řízení rozhodování. Informace jsou v dnešním světě velmi cenným zbožím, určité informace je možné charakterizovat jako strategické zdroje.

Přesné určení hodnoty informace je velmi obtížné. Důležité je položit si otázku: Jakou hodnotu pro mě daná informace má? Tato hodnota by měla být určitě vyšší než náklady na její získání. Zahraniční studie uvádějí dva přístupy pro odhad hodnoty informace:

- Organizace je ochotna za informace platit. Tato ochota může být měřena výší rozpočtu na zdroje informací (odborné knihy, časopisy, apod.) a časem, který zaměstnanci stráví nalezením, vytažením a přečtením dané informace.
- Organizace může odhadnout úsporu nákladů díky tomu, že určitý pracovník má danou informaci k dispozici.

2.2 Bezpečnost informace

Bezpečnost jakéhokoliv systému vyjadřuje stav, kdy je riziko ohrožení nulové či minimální. Požadavky na bezpečnost vyplývají zejména z požadavků na ochranu dat, stabilní a zabezpečený provoz a zabránění ztráty image.

Základní cíle zabezpečení informací lze definovat jako ochranu proti ztrátě dostupnosti, důvěrnosti, neoprávněnému přístupu a neoprávněné modifikaci. To, že daný informační systém je bezpečný, znamená, že jsou chráněny všechny prostředky tohoto systému a data v něm obsažená, dále všechna data v něm zpracovávaná, ukládaná a jím přenášena a také ochrana jeho technických a netechnických prostředků.

Pro zabezpečení počítačových a komunikačních systémů musí být implementovány všechny formy ve vyváženém poměru. Jedná se hlavně o tyto:

- ⇒ fyzické zabezpečení, které musí eliminovat fyzické ohrožení systémů,
- ⇒ zabezpečení proti elektromagnetickému vyzařování komponent chráněného systému,

- ⇒ administrativní a organizační zabezpečení zaručující provádění vhodné bezpečnostní politiky,
- ⇒ personální zabezpečení, které je v přímém vztahu s administrativním zabezpečením a znamená důkladný výběr pracovníků a jejich pravidelné doškolování,
- ⇒ softwarové zabezpečení – do systémů se pomocí operačních systémů a dalšího software implementují zásady bezpečnostní politiky určité třídy bezpečnosti především pomocí takových funkcí jako je identifikace a autentizace uživatele nebo řízení a protokolování přístupu,
- ⇒ zabezpečení na úrovni hardware a firmware,
- ⇒ zabezpečení na úrovni sítě (připojení do sítě komplikuje situaci již zabezpečených systémů a vyžaduje posouzení bezpečnosti v souvislosti s používanými protokoly a s úrovní poskytovaných síťových služeb).

[3]

Ohrožení systému může být jak vnější tak i vnitřní. Vnější ohrožení systému (tj. např. voda, požár, živelné pohromy, apod.) není tak pravděpodobné jako ohrožení vnitřní. Zdrojem vnitřního ohrožení je člověk neboli narušitel. Ten může být vnitřní či vnější. Může svým konáním bránit uživatelům ve využívání informačního systému, může se snažit o neautorizovaný přístup k údajům jejich získání apod. Pro zabránění narušiteli vniknout do systému je potřeba provést důkladnou analýzu motivace a metod, kterými může disponovat.

Podle toho, pomocí jaké metody působí narušitel na systém, rozlišujeme tyto metody:

1) on-line metody infiltrace do systému

- zneužití cizí identity a neautorizovaný přístup do systému,
- využití nedokonalosti a mezer v bezpečnostním systému,
- sledování komunikace v síti za účelem získání dat nebo autentizačních kódů,
- rušení komunikace v síti.

2) metody automatizované infiltrace

- nerušitel nemění stav systému přímou komunikací, ale vytváří novou datovou strukturu nebo ji modifikuje. Tyto struktury způsobují změny v chování počítačového systému (viry, trojské koně, červy).

[3]

2.3 Základní metody ochrany dat

1. *Zálohování a archivace dat* – zálohováním se myslí vytvoření kopie důležitých dat a jejich uložení na bezpečné místo, archivace je uložení dat dlouhodobě.
2. *Identifikace a autentizace uživatele* – identifikace je prohlášení uživatele o totožnosti, autentizace je proces nebo výsledek ověření této totožnosti., kterou je možné provádět těmito metodami:
3. *Kryptografická ochrana* – jedná se o šifrování, jehož úkolem je spolehlivé řešení utajení informace, zajištění důvěrnosti dat, autentizace autora informace a zajištění integrity dat.
4. *Antivirová ochrana*
5. *Ochrana dat na úrovni sítě* – postupy sloužící k řízení komunikace s okolními sítěmi pro zvýšení bezpečnosti. Příkladem může být firewall oddělující dvě komunikující sítě.
6. *Zálohování napájecího napětí* – poruchy napájení počítačových systémů elektrickou energií jsou rizikovým faktorem při ochraně dat a řeší se hlavně přepětíovými ochranami a zdroji nepřetržitého napájení.
7. *Účinná likvidace nepotřebných dat na paměťových médiích.*

Zajištění bezpečnosti dat je vhodné řešit systémově jako součást celkové bezpečnostní politiky organizace, která musí zahrnovat všechna pravidla pro přístup subjektů k informacím a prostředkům informačního systému dané třídy bezpečnosti, pro vhodný výběr bezpečnostních funkcí, produktů a mechanismů a pro analýzu a ocenění rizik. [3]

Podle průzkumu informační bezpečnosti se jako nejúčinnější ochrana jeví kombinace šifrování a dostatečné autentizace.

2.3.1 Šifrování

Nejúčinnější ochranou je kombinace více ochranných složek – hesla, šifrování a hardwarového klíče. Úspěšný útok je pak skoro nemožný. Útočník má k souborům sice přístup, ale data v nich obsažená jsou pro něj nečitelná, tzn. že zničit je sice může, ale zneužít jejich obsah nemůže.

Šifrování neboli kryptografie je nejdůležitějším nástrojem, aby byla zajištěna bezpečnost na počítačové síti. A nejdůležitějším prostředkem šifrovaných systémů je klíč, díky němuž odesílatel data šifruje a příjemce je dešifruje.

- *šifrování se symetrickým klíčem* – znamená, že odesílatel i příjemce používají stejný klíč. Odesílatel tato data zašifruje dohodnutým algoritmem a klíčem a poté ho odešle příjemci. Příjemce přijatou zprávu dešifruje díky použití zpětného algoritmu a stejného klíče;
- *algoritmy s veřejným klíčem* – odesílatel i příjemce používají odlišné klíče, a to klíč veřejný a klíč soukromý. Veřejný klíč je k dispozici volně, což znamená, že kdokoliv chce poslat utajenou zprávu, může ji zašifrovat pomocí veřejného klíče. Tuto zprávu však může dešifrovat jen ten, kdo zná soukromý klíč.

On-line šifrování

Toto šifrování dat probíhá při čtení nebo při jejich ukládání na disk. Při otevření souboru, např. dokumentu ve Wordu, je ověřeno, zda má uživatel k tomuto souboru přístup či ne, zda vlastní šifrovací klíč apod. Pokud ano, soubor je dešifrován a otevřen; pokud ne, je uživateli přístup znemožněn. V případě ukládání dat je to obráceně.

Off-line šifrování

Tato technologie nešifruje data v reálném čase, nýbrž jednorázově, a to při přihlášení (kdy jsou jeho soubory dešifrovány) či odhlášení uživatele (kdy jsou naopak zašifrovány). Této metody se užívá především pro ochranu menšího objemu dat.

On-demand šifrování

Tento způsob zajištění ochrany je nejjednodušší. Na požádání uživatele je soubor zašifrován. Obvykle je tato metoda dostupná v nabídce kontextového menu operačního systému a otevírá se kliknutím pravého tlačítka myši na daný soubor. Existují také šifrovací programy umožňující šifrování do samorozbalovacích EXE souborů (např. PGP).

V tomto případě zadáme frázi, která slouží jako klíč k šifrování daných souborů. Tyto se pak zašifrují do jednoho EXE souboru, kdy je po spuštění tohoto souboru požadována právě vstupní fráze. Takto lze zasílat data i těm, kteří nemají instalovaný příslušný šifrovací program. Nevýhodou je, že EXE soubor může být velmi snadno napaden virem.

Šifrování lze rozdělit na:

- a) on-line a off-line šifrování,
- b) softwarové, hardwarové šifrování (i jejich kombinace),
- c) šifrování na úrovni jednotlivých souborů, virtuálních filesystémů a celých filesystémů,
- d) šifrování na úrovni I/O operací,
- e) šifrování podle druhu a síly šifry,
- f) patří sem také šifrování podle toho, kde jsou uloženy šifrovací klíče (v hlavě uživatele, HW předmětu); hierarchie klíčů ano/ne.

Síla šifry → většina šifer používá tzv. klíč jako parametr, přičemž síla šifry závisí na délce klíče. Ta bývá většinou rozdělena na „malou“, „střední“ a „silnou“. Obecně platí, že čím delší je klíč, tím větší je bezpečnost, to ale zvyšuje nároky na HW i cenu.

Před samotným šifrováním je třeba učinit několik kroků:

- určit cenu chráněných informací a z ní určit cenu, kterou za produkt zaplatíme (tzn. že vybereme druh, systém, sílu šifry apod.).
- masivnost nasazení,
- budeme potřebovat multiplatformní řešení ano/ne,
- určit šifru, která bude standardem,
- potřebujeme ukládat klíče v předmětu,
- hierarchie klíčů,
- návaznost na další projekty,
- použijeme rozšiřující možnosti nabízených systémů (přihlašování předmětem,...),

- vypracovat návody, postupy a doporučení pro uživatele,
- šifrování pošty, komunikace dat na síti,....

Obecně platí, že čím bezpečnější systém vybudujeme, tím více snížíme uživatelský komfort.

2.3.2 Autentizace

Při autentizaci prokazuje uživatel pomocí stanovených prostředků svou identitu. Existují 3 základní způsoby této identifikace:

- 1) autentizace pomocí znalosti, kterou disponuje daná osoba,
- 2) autentizace pomocí fyzického znaku dané osoby,
- 3) autentizace pomocí daného bezpečnostního předmětu.

Ad 1) Znalostí se rozumí zadání správného hesla. Do systému se přihlašujeme pomocí jména (login) a pomocí hesla (password). Jedná se o nejpoužívanější způsob přihlašování. Co se hesla samotného týče, musíme dávat pozor na několik věcí:

- Nikdy nesmíme sdílet jedno heslo s více lidmi.
- Neměli bychom volit velmi jednoduché a tedy snadno uhádnutelné heslo, jako je např. naše rodné číslo, datum narození, jméno partnera apod.
- Měli bychom volit takové heslo, které odolá slovníkovému útoku. Na internetu totiž existují programy, která dokáží během krátké doby vyzkoušet všechna slovíčka ze svého rozsáhlého slovníku.
- Heslo, které volíme, by mělo být delší, minimálně osm znaků. Nejlépe je vybrat náhodnou směsici znaků, která je vysoce odolná proti slovníkovému útoku.
- Je dobré heslo po určité době změnit a činit tak pravidelně.
- Toto heslo bychom si měli uložit na bezpečné místo, v případě, že si jej nepamatujeme.
- Jedno heslo bychom neměli používat ve více aplikacích.

- Pokud zjistíme, že naše heslo je již odhaleno, musíme jej okamžitě zrušit. Neexistuje bezpečné heslo, ale je možné se k němu přiblížit.

Ad 2) Tyto metody spočívají ve snímání jedinečných fyzických znaků dané osoby, jedná se o snímání otisků prstů či oční duhovky. Po stránce technologické jsou tyto metody určité náročnější. Postupem času se však mohou tyto snímané znaky nepatrně odchylovat, čímž činí následnou identifikaci obtížnější a tedy i méně spolehlivou.

Ad 3) Tento způsob autentizace je velmi zajímavý. Při identifikaci osoby, která přistupuje k citlivým údajům, je použit některý z hardwarových autentizačních prostředků jako jsou např. čipové karty, magnetické karty nebo tzv. tokeny. To je identifikace pomocí něčeho, co daná osoba vlastní. Použití těchto prostředků je velmi snadné a výhodná je také jejich přenosnost. Jejich použití je obvykle vázáno na zadání PINu, čímž se riziko spojené s krádeží či ztrátou snižuje.

K dalším metodám ochrany dat patří kontrola softwaru a hardwaru, dále administrativní, legislativní a etická kontrola a v neposlední řadě také kontrola fyzická.

3 INTERNET

Jedním z hlavních důvodů, proč jsou počítače propojovány do složitých počítačových sítí, je bezpečnost osobních či podnikových dat a aplikací. Děje se tomu tak proto, že systém nemusí být vždy spolehlivý, čímž dochází k úmyslnému napadení či ke ztrátě dat.

Bezpečnost dat je určena těmito hledisky:

- skladba uživatelů,
- topologie sítě a použitý systém,
- zabezpečení hlavních systémů.

3.1 Řešení bezpečnosti na internetu

- ⇒ *chráněný přístup*, kdy je neautorizovaným osobám zakázán vstup do systému;
- ⇒ *šifrovaný přenos informací*, jde o tzv. zašifrovaný kanál, který se vytváří mezi klientem a serverem. Pro verifikaci klíčů se užívají certifikační autority a šifrovaný přenos probíhá pomocí standardů, které jsou zavedeny na internetu;
- ⇒ *neodmítnutelná odpovědnost klienta*, k té dochází pomocí generování asymetrického podpisu dokumentu, který je přenášen spolu s dokumentem. Položky podpisu nemohou být během přenosu změněny a ten, kdo podpis vytvořil, je za něj plně odpovědný, jelikož může podpis vygenerovat jen svým vlastním zařízením;
- ⇒ *nezaměnitelná identifikace klienta*, technologie umožňují generovat jen nezaměnitelné řetězce, které není možné imitovat – jsou totiž generovány vnějším zařízením velikosti kalkulačky. Na začátku spojení si obě strany tyto řetězce vymění. Opět je spolu s dokumenty přenášen i elektronický podpis.

3.2 Viry

Počítačový virus je kus programového kódu, který se dokáže díky hostitelské aplikaci replikovat více než jednou. Šíří se bez vědomí uživatele sedícího právě u počítače. Jeho jedinou vlastností je, že zabírá část paměti. To, že virus škodí, je jeho projev navíc. Viry často obsahují obranný mechanismus proti detekci a některé druhy jsou schopny mutace.

Jaké následky virus má?

Virová nákaza má především podobu zvukových a obrazových efektů, ale nejvážnějším následkem je možnost rozsáhlého zničení dat a programů.

Obdobné programy:

- 1) *Emailoví, internetoví červi* – síťová obdoba jako u počítačových virů, šíří se samovolně pomocí komunikačních linek.
- 2) *Trojské koně* – vedle očekávané činnosti provádějí ještě činnost skrytou, např. mohou odesílat z počítače soubory bez vědomí uživatele či zašifrovat část disku.
- 3) *Zadní dvířka* – bez vědomí uživatele otevírá počítač útočníkovi, bývají součástí počítačových virů či trojských koní.
- 4) *Žertovné programky* – zvláštní kategorie škodlivých kódů, nelze je vypnout a počítač je nutné restartovat.
- 5) *Obtěžující programy a zprávy* – někdo nám vnucuje tyto objekty, aby získal nějaké informace. Příkladem jsou:
 - a) Spyware – obtěžující reklama.
 - b) Hoaxy – poplašné zprávy, novinářské kachny.
 - c) Spamy – nevyžádané e-maily.

3.3 Firewall

Brány firewall jsou prvotní ochranou sítě proti externím útokům z internetu, protože vylučují nepovolenou komunikaci. Je možné si je představit jako operátora telefonní ústředny spojujícího jen hovory schválených uživatelů. Brány firewall blokují veškerý provoz mezi sítí a internetem, který není povolen. Také mohou skrývat adresy počítačů v místní síti, které tak nejsou k dispozici externím uživatelům.

Brána firewall blokuje provoz na konkrétních portech, což znamená, že externí uživatelé se nedostanou k našim datům, ale my můžeme přistupovat ke službám v počítačích ostatních uživatelů. Některé brány kontrolují tok paketů oběma směry, aby ověřily jejich správnost, a zároveň mohou podezřelé pakety odfiltrovat. Skrývají identitu počítačů v síti a tím ztěžují možnost nebezpečným útočníkům zaměřit se na konkrétní počítače.

II. PRAKTICKÁ ČÁST

4 STANOVENÍ HYPOTÉZY

Ve své práci jsem si stanovila následující hypotézu a v dalších částech práce budu ověřovat její pravdivost na základě provedené analýzy.

Hypotéza:

Pokud bude na UTB zaveden elektronický podpis, zvýší se ochrana soukromých údajů na pracovištích a zamezí se jejich nechtěnému úniku mimo oblast oprávněných příjemců.

5 OCHRANA DAT V INFORMAČNÍM SYSTÉMU UTB

Na UTB je přísně dodržován Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Data jsou poskytována jen soudu a policii, a to po podání písemné žádosti v případě přestupku, výživného apod. Přístup k těmto datům mají jen studijní referentky. Osobními daty se myslí:

- jméno a příjmení,
- bydliště,
- číslo občanského průkazu,
- rodné číslo,
- kontaktní adresa,
- telefonní číslo,
- emailová adresa,
- studijní výsledky.

5.1 Povinnosti vedoucích zaměstnanců

Každý vedoucí zaměstnanec na jemu podřízeném pracovišti, na němž jsou zpracovávána osobní data, je povinen:

- stanovit účel, k němuž mají být osobní údaje zpracovány, a provozovat informační systém v souladu s tímto účelem;
- zajistit ochranu informací i celého systému před neoprávněným přístupem, zpracováním, případně zneužitím informací;
- v rámci zajištění ochrany informací stanovit prostředky a způsob zpracování informací;
- zabezpečit zpracování pouze pravdivých a přesných osobních dat (ověřovat zpracováváná data), jen v rozsahu, jenž je pro naplnění stanoveného účelu nezbytný;

- zajistit uchovávání osobních dat pouze po dobu nezbytnou k účelu jejich zpracování či stanovenou zvláštním zákonem;
- zabezpečit zpracování osobních dat jen se souhlasem subjektu údajů. Bez něj mohou být zpracovány jen, pokud to stanoví zvláštní zákon či je jejich zpracování nutné pro plnění povinností stanovených zvláštním zákonem;
- při zpracování osobních dat musí dbát, aby subjekt neutrpěl újmu na svých právech;
- zabezpečit zpracování citlivých dat jen v souladu se zákonem;
- likvidaci a uchovávání osobních dat provádět v souladu se zákonem;
- všechny databáze UTB a jeho součásti zasílat subjektům mimo UTB jen prostřednictvím rektorátu;
- jsou-li zpracovávány údaje pravidelně či příležitostně poskytovány subjektům mimo UTB, zabezpečit toto jen se souhlasem subjektu údajů.

Dále musí každý zaměstnanec na pracovišti, které řídí:

- průběžně vyhodnocovat, zda jsou na jemu podřízeném pracovišti zpracovávány osobní data či citlivá data.

5.2 Povinnosti zaměstnanců

Zaměstnanci UTB a ostatní osoby, jež přicházejí do styku s informacemi zpracovávanými v informačním systému UTB, jsou povinni:

- zachovávat mlčenlivost o osobních údajích i o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů;
- zachovávat mlčenlivost i po ukončení zaměstnání či příslušných prací;
- nesmějí zpřístupnit tyto informace třetí osobě nebo je využít pro sebe bez souhlasu správce a subjektu, jehož se informace týkají, pokud se nejedná o informace, které jsou poskytovány podle zvláštního zákona.

5.3 Poskytování informací na UTB

Poskytování informací o UTB ve Zlíně se řídí zákonem č. 106/1999 Sb., o svobodném přístupu k informacím. Ve věcech uplatňování ustanovení tohoto zákona, zejména poskytování informací žadateli na základě žádosti či zveřejněním:

- rozhodují na fakultách příslušní děkani v rozsahu stanoveném zákonem č. 111/1998 Sb., o vysokých školách v platném znění, popřípadě v rozsahu stanoveném plnou mocí rektora,
- v záležitostech celoškolského charakteru a v záležitostech dalších součástí školy rozhoduje rektor.

Na dalších součástech školy toto ustanovení zákona zabezpečují, koordinují a kontrolují příslušní ředitelé, na rektorátě včetně hospodářské a vnitřní správy je to kvestor, a v celoškolských záležitostech pak kancléř.

Fakulty a další části školy předají kancléři zprávu o své činnosti v oblasti poskytování informací za každý předcházející rok.

5.3.1 Žádost o poskytnutí informace

Tato žádost se podává ústně, telefonicky nebo elektronickou poštou a směřuje rovnou na zaměstnance UTB, a to podle jejich funkčního zařazení. Ti jsou povinni, pokud to jde, poskytnout požadované informace obratem, popřípadě odkázat žadatele na zveřejněnou informaci.

Pokud není žadateli na tuto žádost podána informace či ji nepovažuje za dostačující, musí žádost podat písemně, a to na adresu UTB, či elektronickou poštou na adresu rektora, kvestora, kancléře nebo děkana.

Písemné žádosti neobsahující identifikační údaje žadatele (tj. jméno, příjmení a adresu žadatele pro korespondenci), resp. žádosti zaslané elektronicky bez elektronické adresy žadatele, se ve smyslu zákona nepovažují za podané a odkládají se.

Pokud je žádost nesrozumitelná, je žadatel ve lhůtě do 7 dní od podání žádosti vyzván, aby tuto žádost upřesnil. Jestliže ji neupřesní do 30 dní, UTB tuto žádost zamítá.

Žádost s informacemi, které se nevztahují k působnosti UTB, je odložena a toto je sděleno žadateli do 3 dní.

Pokud je informace už zveřejněna, oznámí se žadateli do 7 dní údaje umožňující mu informaci vyhledat a získat.

Vyžádané informace podá UTB žadateli do 15 dnů od přijetí podání či od upřesnění žádosti. V závažných důvodech je možné tuto lhůtu prodloužit nejdéle o 10 dní. Žadatel musí být o prodloužení lhůty a o důvodech vždy a včas informován.

5.4 Dodržování autorského zákona

Zaměstnanci a studenti UTB mají umožněn přístup na internet a při manipulaci se softwarem musí respektovat licenční ujednání. Je jim zakázáno v prostorách UTB nelegálně stahovat, ukládat, instalovat, kopírovat a šířit software chráněný autorským zákonem. tento software je označen značkou „copy read“.

Porušení tohoto zákazu studentem je bráno jako disciplinární přestupek, porušení zákazu zaměstnancem pak jako porušení pracovní kázně.

Za software na serverech UTB odpovídají jejich správci, příp. správci jednotlivých částí serverů. Za software na počítači odpovídá hmotně zaměstnanec za toto odpovědný.

6 PRAVIDLA PROVOZU POČÍTAČOVÉ SÍTĚ UTB

Tato pravidla jsou závazná pro všechny uživatele počítačové sítě UTB a vztahují se na všechny počítače a podobná zařízení připojená k počítačové síti.

Počítačovou sítí se rozumí všechny technické a programové prostředky sloužící k propojení počítačů. *Uživatelem* této sítě je každý, kdo užívá síť nebo zařízení k nim připojená, tedy zaměstnanci a studenti UTB ve Zlíně.

To, že má někdo uživatelský účet, znamená, že může na daném zařízení pracovat. Tento účet je chráněn *heslem*.

6.1 Správce sítě UTB

Správce počítačové sítě je osoba pověřená správou všech prostředků sítě – instalace, konfigurace, ochrana, zapínání a vypínání systému a aktivních prvků, připojování periferních zařízení, zálohování dat, vytváření nových uživatelských účtů a připojování nových uživatelů.

Globálním správcem sítě UTB je Centrum výpočetní techniky, které odpovídá za provoz páteřní sítě a za připojení jednotlivých lokalit UTB. Správce je oprávněn monitorovat činnost uživatelů v mezích, která neohrožují veřejná, osobní či vlastnická práva jednotlivých uživatelů.

Informace, se kterými přichází neustále do styku, musí udržovat v naprosté tajnosti a nemůže seznamovat další osoby s obsahem adresářů jednotlivých uživatelů. V případě porušení pravidel provozu sítě UTB je povinen s tímto seznámit odpovědného vedoucího pracovníka (děkana fakulty, kvestora, apod.).

Správce může odpojit část sítě, k níž byly připojeny nekonzultované technické prostředky nebo na níž byla provedena se správcem nekonzultovaná změna konfigurace síťového programového vybavení a to by vedlo k poruchám ohrožujícím provoz sítě.

CVT zabezpečuje přidělování uživatelských účtů, e-mailových adres, síťového diskového prostoru, adres jednoznačně identifikujících zařízení sítě (tzv. IP adres) a adres jednotlivým subsítím.

Za přidělení uživatelského účtu a dalších zdrojů na konkrétním počítači odpovídá správce tohoto počítače.

Správu jednotlivých součástí UTB provádějí pracovníci dané součásti.

6.2 Uživatelé sítě

Uživatelé mohou využívat počítačové prostředky UTB ve shodě se svými pracovními a studijními úkoly. Je nutné, aby přitom respektovali vlastnická práva k datům uloženým v elektronické podobě.

Všechny složky počítačové sítě jsou vlastnictvím UTB. Uživatelům je zakázáno:

- ⇒ neautorizované kopírování částí programového vybavení či dat, ke kterým vykonává UTB práva k užívání,
- ⇒ neautorizovaná modifikace programů, dat či technického vybavení v majetku či užívání UTB,
- ⇒ poškození nebo zničení počítačových prostředků,
- ⇒ odposlouchávání provozu a vytváření kopií zpráv procházejících jednotlivými uzly sítě,
- ⇒ použití počítačových prostředků UTB k výše uvedeným činnostem a činnostem namířeným proti další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím sítě.

6.3 Ochrana autorských práv, dat a informací

UTB chrání občanská, osobní i vlastnická práva všech uživatelů sítě a v rámci svých technických možností se snaží chránit i soukromí dat a informací uložených na počítačích UTB či přenášených prostřednictvím sítě, ale úplné soukromí a bezpečnost uložených či přenášených dat nemůže UTB zajistit.

Pro maximální ochranu dat je uživatelům zakázáno:

- provádět akce vedoucí k narušení soukromí jiného uživatele,
- kopírovat či jen prohlížet si data nebo programy z uživatelských adresářů bez souhlasu jejich majitelů,
- využívat a šířit vědomě nelegální programové vybavení a data,

- používat a šířit vědomě zavirované soubory, čímž je narušena bezpečnost v síti,
- využívat elektronické prostředky k obtěžování jiných uživatelů,
- využívat počítačové prostředky UTB ke konání přestupků a trestných činů,
- používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům.

6.4 Přístupová práva a identifikace uživatele

Každý akademický pracovník, akademický pracovník pracující na základě uzavřené dohody o pracovní činnosti, ostatní zaměstnanec i student UTB má právo na zřízení uživatelského účtu, těchto účtů může mít i více. S každým účtem jsou spojena přístupová práva, která opravňují uživatele ke zdrojům sítě.

Uživatel musí svůj účet chránit netriviálním heslem a udržovat jej v tajnosti. Nesmí poskytnout své uživatelské jméno a heslo k účtu jiné osobě. Uživatel může používat jen přístupová práva jemu přidělená správcem.

Přístup k osobním datům všech zaměstnanců a studentů UTB mají:

- 1) správcové systémů STAG a SAP,
- 2) studijní referentky,
- 3) zaměstnanci knihovny UTB,
- 4) zaměstnanci personálního oddělení UTB.

Ochrana osobních dat podléhá těmto zákonům:

- zákon č. 101/2000 Sb. o ochraně osobních dat,
- zákon č. 53/2004 Sb. o evidenci obyvatel,
- tisková zpráva ÚOOÚ ze dne 11. 3. 2004.

Od 1. 1. 2006 by měl platit zákaz evidence rodných čísel v informačních systémech, pokud to nebude umožňovat zvláštní zákon.

Na UTB jsou v současné době aplikovány 2 systémy:

- 1) STAG – studijní systém,
- 2) SAP – ekonomický informační systém.

V následující části práce se budu zabývat těmito dvěma systémy, a to přesně jejich popisem, užitným funkcím, dále stupni bezpečnosti jednotlivých úrovní systémů a v neposlední řadě také technologiím, které zabezpečují ochranu dat uvnitř těchto systémů a jsou tedy hlavním ukazatelem úrovně ochrany dat na UTB.

7 SYSTÉM STAG

Systém IS/STAG je informační systém pro evidenci studijní agendy vysoké školy či univerzity.

Studijní systém STAG byl vyvinut a realizován v prostředí Oracle. Přístup do databáze probíhá pomocí vzdáleně (lokálně) nainstalovaných klientů.

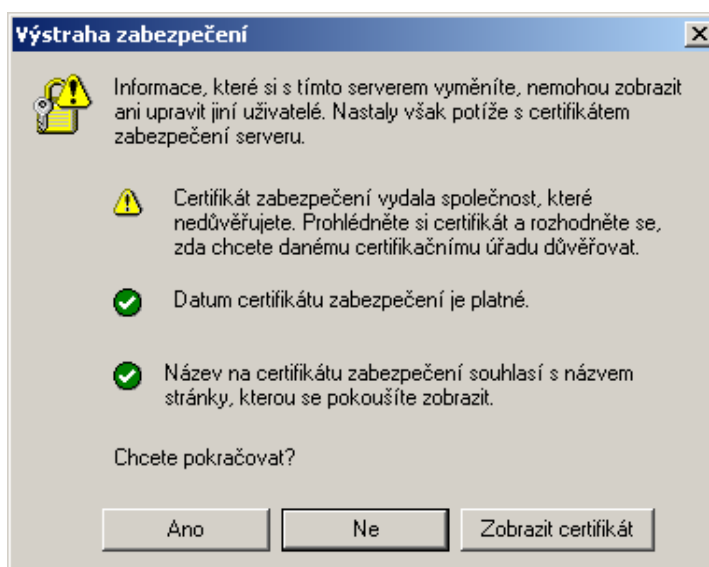
Systém v současnosti pokrývá následující uživatelské funkce:

- *kompletní evidence studenta* – osobní údaje a průběh studia,
- *zadání a editaci sylabu předmětu* – a to včetně vazby na předměty podmiňující, vylučující a kapacity předmětů,
- *zadání a editaci studijních programů* – včetně vazby na aprobace, kombinace aprobací a podmiňující obory,
- *zadání a editaci studijních plánů* – včetně vazby na bloky předmětu, povinné předměty v prvním semestru a globálně povinné předměty,
- *zadání a editaci rozvrhu* – včetně kontrol kolizí, vyhledávání údajů podle různých kritérií apod.,
- *předzápas studentů* – každý student si interaktivně na hotovém rozvrhu sestavuje svůj individuální studijní plán na příští akademický rok, možnost vytištění rozvrhu,
- *zápis známek* - realizován nikoliv centrálně, ale tam kde údaje vznikají, tedy na katedrách,
- *vypisování termínů zkoušek a zapisování na ně*,
- *tisk informačních brožurek o studiu v prostředí TeX* - není podmínkou,
- *příprava podkladů pro zápis* - kontroly splnění podmínek studia, umožněn jak kreditní, tak nekreditní způsob studia,
- *množství různých tiskových sestav* - od konkrétních o studentovi či předmětu a rozvrhové akci až po např. zahajovací výkaz v11, matriku studentů nebo výpis pro VZP,
- *výměnu dat mezi systémem STAG a systémem pro evidenci ubytování studentů na koleji*,

- *modul Přijímací řízení* - evidence uchazečů, nastavení parametrů pro přijetí, automatické vyhodnocení přijetí, korespondence, apod.,
- *modul Absolvent* - evidence absolventů, zadání diplomové práce, vystavení dokladů ke státní závěrečné zkoušce, tisk dokumentů systémem TeX - diplomy, vysvědčení, certifikáty,
- *připravuje se modul Statistika* - porovnání výsledků studia absolventa s jeho výsledky na střední škole a při přijímacím řízení, porovnání výsledků absolventů s typem střední školy, četnost studentů podle okresu trvalého bydliště a další,
- *připravuje se modul Evaluate* – sběr a statistické zpracování dat ze studentských dotazníků.

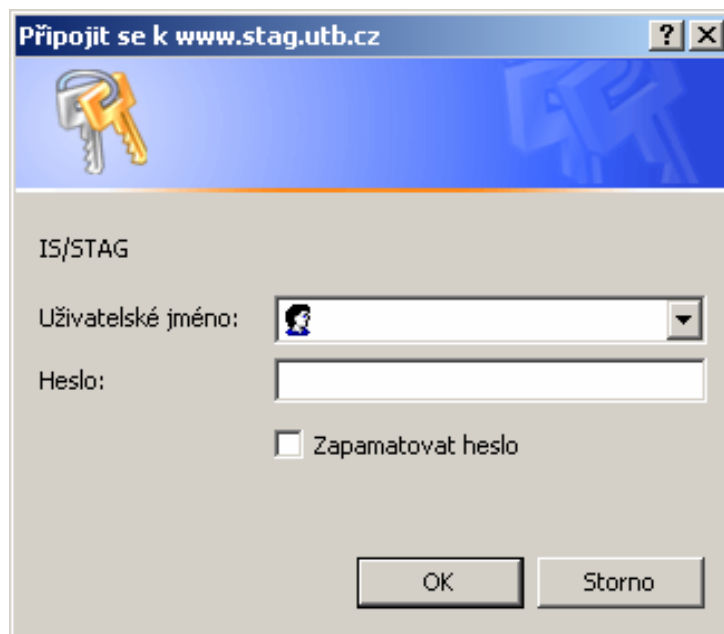
7.1 Přihlášení do systému

Každý uživatel systému musí mít svůj účet. Ten je zpravidla identifikován uživatelským jménem a heslem, které je tajné a chrání před neoprávněným přístupem do systému. Pro správné přihlášení do systému je nutné, abychom znali své uživatelské jméno a heslo.



Obr. 1. Výstraha zabezpečení.

Při přihlašování do STAGu se na obrazovce objeví dialogové okno o zabezpečení serveru. I přes tuto výstrahu pokračuje uživatel systému stisknutím tlačítka Ano.



Obr. 2. Přihlášení do IS STAG.

Když se uživatel přihlašuje do systému, zadá své heslo, a tím přesvědčí počítač, že je opravdu tím, za koho se vydává. Počítač poté zkontroluje, jestli uživatelem zadané heslo odpovídá zadanému účtu. Pokud jsou shodná, může uživatel začít pracovat v systému. Když je heslo zapisováno, systém jej nezobrazuje, čímž je uživatel chráněn v případě, že užívá tiskárnový terminál či mu někdo hledí přes rameno (tzv. shoulder surfing).

IS/STAG chrání osobní data (především rodná čísla, uživatelská jména a hesla) studentů i zaměstnanců UTB proti zneužití. V IS/STAG se rodné číslo vyskytuje u:

- studentů,
- uchazečů o studium,
- zaměstnanců UTB.

Rodná čísla jsou z IS/STAG vykazována na:

- SIMS – studenti (zákon o VŠ),
- ÚIV – uchazeči (zákon o VŠ),
- VZP – studenti (zákon č. 592/1992 Sb. o pojistném na všeobecné pojištění),
- SOC – studenti (zákon č. 592/1992 Sb. o sociálním zabezpečení).

Systém je zabezpečen podle jednotlivých rolí. Přístup k IS/STAG mají:

- studijní referentky,
- pomocná síla u přijímacího řízení,
- tajemník fakulty,
- administrátoři.

Katedry žádají o data studijní referentky (standardní sestavy) a administrátory (nestandardní sestavy).

7.2 Ochrana dat v systému STAG

Bezpečnost tohoto studijního systému je řešena na několika úrovních:

- a) Databázový server – databáze Oracle 9i
- b) Aplikace STAG
- c) WWW rozhraní STAGu.

Tyto úrovně ochrany dat podrobněji popisují v následujícím textu.

7.2.1 Databázový server – databáze Oracle 9i

STAG běží nad databází Oracle 9i. Ochrana dat je zde zajištěna na úrovni databáze, ne tedy na úrovni aplikace samotné. K datům se přistupuje přes VPD (Virtual Private Database), která umožňuje definovat pravidla pro řízení přístupu k datům na úrovni jednotlivých řádků tabulky.

Sdílením klíčových částí systému společně s Oracle 9i je zajištěna spolehlivost, škálovatelnost a dostupnost potřebná pro všechny důležité aplikace provozované v prostředí internetu.

U každého záznamu je evidováno dále to, kdo a kdy ho založil a kým a kdy byl naposledy změněn. U důležitých tabulek se používá také audit, což znamená, že každá změna je uložena do zvláštní tabulky. Audit umožňuje zaznamenávat klíčové události a stavy během provozu, přičemž se současně vyznačuje vysokou mírou odolnosti před zničením či pozměněním pořízených záznamů. Je označován jako tzv. „černá skříňka“ systému.

Přístup k serveru chrání také firewall, který specifikuje, kdo má přístup k serveru a pomocí kterého protokolu. Firewall definuje rovněž porty, které se mohou využívat.

Firewall

Pro unixové servery na UTB se užívají IP filtry. Jsou to brány, které byly původně rozšířené o schopnost filtrování, později pak specializované filtrovací brány. Další kategorií jsou tzv. stavové filtry.

Pro ochranu operačních systémů Windows Server (kartová databáze, menza, přístupové systémy na čipové karty) je užíván Kerio ServerFirewall. Tato brána nabízí administrátorům informačních a bezpečnostních technologií efektivní nástroj k ochraně serverových systémů před červy, přepsáním zásobníku a dalšími bezpečnostními hrozbami z internetu.

Kerio ServerFirewall umožňuje UTB chránit své operační systémy Windows Server před zákeřnými útoky zvenčí i z jejích vlastních interních sítí.

Systém prevence útoků blokuje útoky, které by jinak byly propuštěny jako legitimní komunikace, a brání zneužití bezpečnostních chyb v operačním systému a aplikacích, pro něž dosud neexistují záplaty.

Filtr síťové komunikace řídí veškerou příchozí i odchozí síťovou komunikaci a nabízí bohaté a přizpůsobivé filtrovací možnosti k vytvoření účinné bezpečnostní politiky.

Kerio ServerFirewall zahrnuje systém prevence proti napadení zaměřený na dva klíčové problémy, které nejčastěji sužují serverové systémy, a to pokusy o napadení na IP úrovni a pokusy o falšování systémových otisků.

Kerio ServerFirewall může být využit celou řadou způsobů, od zabezpečení intranetových, databázových, CRM a poštovních serverů, až po ochranu serverů umístěných v kolokačních zařízeních.

Magnetické pásky

Nedílnou součástí zabezpečení a celkové ochrany dat je ze strany databázových platform podpora zálohovacích mechanismů. Důležité databáze a data jsou zálohována pravidelně na magnetické pásky, což se děje přibližně jednou za 14 dní, vždy v noci. Magnetické pásky jsou poté uschovány na příslušné místo. Toto místo ale není nijak zabezpečeno, čehož následkem může být případná ztráta (odcizení) pásek a zneužití dat na nich, pokud se dostanou do rukou neoprávněným osobám.

Serverovna

Všechna data jsou uložena v serverovně, což je místnost s počítači a bezpečnostním alarmem. Do této místnosti mají přístup jen pracovníci CVT (Centrum výpočetní techniky na UTB), správci serveru a správci telefonní ústředny. Na centrálních serverech jsou databáze s veškerými daty.

7.2.2 Aplikace STAG

Přístup k aplikaci je řešen přes uživatelská konta s hesly. Každému uživateli je přiřazena určitá role. U této role je potom definováno, ke kterým záznamům má daná role přístup a které objekty může využívat.

Uživatelské role a jejich přístup k funkcím IS/STAG téměř věrně kopírují odpovědnost za funkce ve skutečnosti.

7.2.3 WWW rozhraní STAGu

Pro zajištění bezpečného přístupu k osobním stránkám podporuje webový server STAGu technologii SSL, jež automaticky vytváří kanál pro šifrovanou komunikaci mezi serverem a klientem. Služby běžící na webovém serveru mají vygenerovány své certifikáty, které jsou podepsány certifikační autoritou UTB. Tyto certifikáty si stahují internetové prohlížeče automaticky sami a uživatelé je většinou jen potvrdí. To se děje při každém startu klienta či jen jednou do doby, než jejich platnost vyprší a jsou nahrazeny novými.

Webový přístup ke studentskému portálu STAG je realizován protokolem HTTPS, který používá šifrovaný přenos dat a téměř znemožňuje odposlech, jelikož data jsou přes síť posílána šifrovaně. Protokol HTTPS je standardním http nad vrstvou SSL.

Při navazování SSL spojení se používají certifikáty, v nichž je mimo jiné uvedeno, k jaké doméně byl certifikát vystaven.

To byly tedy úrovně bezpečnosti studijního systému, kterými je řešena ochrana dat. Nyní se budu věnovat technologiím užitým v úrovni WWW rozhraní STAGu, jelikož je to z mého pohledu nutné pro vymezení a pochopení síly ochrany dat.

7.2.4 Protokol HTTPS

Jedná se o http data přenášená pomocí Secure neboli bezpečného protokolu. HTTPS (Hypertext Transfer Protocol Secure) je zkratkou pro HTTP + SSL, což jsou dva různé protokoly fungující na různých portech (443 a 80). Tento protokol vypadá téměř jako původní http protokol, jediný rozdíl je v tom, že jsou data před odesláním zašifrována a poté elektronicky podepsána. Šifrovacím a podpisovým protokolem může být SSL nebo TLS. O bezpečnosti algoritmů, na kterých jsou založeny, nejsou zatím známy žádné pochyby.

Šifrování znemožňuje, aby měla k datům po cestě k příjemci přístup jiná osoba. Elektronický podpis zase zajišťuje, že je na opačné straně ta osoba, s níž chceme být v kontaktu.

7.2.5 SSL protokol

SSL (Secure Socket Layer) je protokol pro vytváření zabezpečených komunikačních kanálů, které chrání přenášené informace (např. heslo či číslo platební karty) před neoprávněným zachycením na internetu.

SSL certifikát je šifrovací klíč, jímž jsou data chráněna proti zneužití třetími osobami. Tento klíč zajišťuje bezpečnou komunikaci mezi počítačem koncového uživatele a navštívenými webovými stránkami. To zajišťuje, že mezi počítačem a serverem se stránkami může dojít k neoprávněnému zachycení, zneužití a pozměnění přenášených dat. Mezi nejcitlivější data patří určitě přihlašovací jméno a heslo, číslo platební karty, rodné číslo a další důvěrné informace.

SSL technologie má tyto funkce:

- ✓ umožňuje šifrování informačního toku mezi klientem a serverem,
- ✓ vytváří základ pro vzájemnou autentizaci klient/server,
- ✓ zajišťuje autentizaci klienta.

Princip SSL

SSL je založeno na vytvoření zabezpečeného kanálu mezi klientem, tedy prohlížečem, a serverem. Takový kanál zaručuje důvěrnost každé zprávy, která je jím přenášena. SSL nešifruje žádná data uložená na klientu či serveru. Zabezpečuje aplikační protokoly jako např. Telnet, HTTP, NNTP apod. SSL umožňuje naprosto bezpečnou výměnu informací při inicializaci TCP/IP spojení, při němž se klient a server domluví na konkrétní podobě užití bezpečnosti a poté provedou vzájemnou autentizaci certifikáty. Šifrování je tedy aktivováno a od tohoto okamžiku SSL šifruje a dešifruje proud bytů použitého aplikačního protokolu. Jinak řečeno, všechny informace v HTTP požadavku i v HTTP odpovědi jsou plně zašifrovány, včetně URL, potvrzených obsahů formulářů, přístupových autorizačních informací a všech dat vrácených klientovi serverem.

SSL používá kryptografii s veřejným klíčem pro výměnu klíče sezení mezi klientem a serverem. Tento klíč je generovaný pro všechna spojení mezi klientem a serverem a je použit pro šifrování HTTP transakcí, tedy požadavku a odpovědi. Kryptografie s veřejným klíčem se užívá pouze pro vzájemné ověření a k zašifrování klíče sezení. SSL používá šifrování se soukromým klíčem při šifrování další výměny informací. Ke každé transakci je potřeba jiný klíč sezení, což je dobré v situaci, kdy hodlá útočník zcizit jeden klíč, který mu ale nijak nepomůže v další komunikaci.

SSL certifikát

SSL vyžaduje, aby měl server důvěryhodný certifikát vydaný důvěryhodnou certifikační autoritou. Tento certifikát zaručuje kromě šifrování dat také autentičnost webové stránky, a to tím, že dokáže identifikovat provozovatele dané webové stránky.

UTB má svou vlastní certifikační autoritu, která je volně k dispozici na webu univerzity (www.stag.utb.cz/web/certifikaty/certifikaty.htm) a kdokoli si ji může stáhnout. Je možné si také ověřit její platnost a nainstalovat si ji do svého prohlížeče. Poté už nebude uživatel přístupu dotazován na bezpečnost a zabezpečení se pro něj stane zcela transparentní.

Každý vyspělý webový prohlížeč identifikuje připojení ke stránkám zabezpečeným SSL certifikátem, zpravidla to bývá symbol zámku v dolní liště. Pokud na něj uživatel dvakrát klikne, zobrazí se mu informace o certifikátu, dále pak název www serveru a název certifikačního úřadu, který tento certifikát vydal. Je důležité, aby byl certifikát vydán důvěryhodným certifikačním úřadem, jinak mohou být informace v certifikátu nepravdivé. Na tyto nesrovnalosti upozorňuje vyspělý prohlížeč automaticky.

Pokud se jedná o důvěryhodný certifikační úřad, může uživatel zjistit, jaké společnosti patří stránky a podle toho se rozhodnout, zda jí poskytne důvěrná a citlivá data či nikoli.

SSL certifikát by měl používat každý kdo je buď provozovatelem webového portálu, elektronického obchodu nebo webových stránek, kdy je potřeba, aby uživatel zadal své přihlašovací jméno, heslo či jiné důvěrné informace. Díky tomuto certifikátu je uživatelům poskytnuta jistota, že jejich data nebudou zneužita. Zavedení SSL certifikátu je tedy jistotou jak po stránce technické, tak po stránce psychologické.

Nestačí jen SSL certifikát zavést, je důležité, aby byl použitý SSL certifikát důvěryhodný, tzn. že ho vydala důvěryhodná certifikační autorita. Pokud by tomu tak nebylo, zobrazilo by se při přístupu na webové stránky v zabezpečovacím režimu varování, což by vyvolalo nedůvěru ze strany návštěvníků stránek.

Existují dva typy certifikátů určených pro použití ve webových serverech. Dělí se podle počtu bitů v použité šifře, jež jsou základním faktorem jejich síly, čímž se myslí zejména kvalita a odolnost proti prolomení.

Jedná se o 40-ti bitové certifikáty (používané na velkém množství webových serverů) a 128 bitové tzv. „super-certifikáty“ (se silným šifrovacím klíčem, používané zvláště v kritických aplikacích nakládajících s přísně důvěrnými nebo tajnými daty).

Super-certifikáty s délkou klíče 128 bitů jsou doporučovány pro užití v takových projektech, kde se pracuje s daty chráněnými podle zákona č. 101/2000 Sb., o ochraně osobních údajů.

SSL proces

SSL používá sérii klient/server výměn a vytváří zabezpečené sezení. Dvě hlavní fáze SSL protokolu jsou:

- a) vytvoření soukromé komunikace,

b) klientská autentizace.

Proces SSL se může jevit jako značně komplikovaný a dlouhý, ale pracuje konkrétně transparentně k uživateli a probíhá ihned po vytvoření spojení mezi klientem a serverem.

Využití SSL přináší tyto výhody:

- ✓ SSL probíhá transparentně – tzn., že uživatel není nijak zatěžován, jeho jedinou povinností je mít nainstalovaný certifikát od důvěryhodné certifikační autority,
- ✓ autentizace probíhá vzájemně – klient se autentizuje serveru a naopak,
- ✓ veškerá komunikace je šifrována,
- ✓ SSL podporuje většina moderních serverů a prohlížečů.

7.2.6 SSH

SSH (Secure Shell) je metoda vzdáleného přístupu na server. Ve spojení s použitím veřejných klíčů se jedná o velmi spolehlivé zabezpečení sítě. SSH umožňuje bezpečné přihlášení na vzdálený počítač. Jedná se o kód nabízející konzolovou komunikaci mezi síťovým zařízením a lokálním počítačem prostřednictvím internetu. Tato komunikace využívá kryptografické techniky pro zabezpečení uživatelské autorizace a k zabezpečení toku dat mezi počítači.

SSH je volně šiřitelný nástroj, který je určen především k zabezpečení sítí. Představuje řešení na bázi TCP/IP zahrnující bezpečný protokol typu klient-server, určený pro transparentní, mimořádně spolehlivé šifrování a přenos dat v síti.

SSH umožňuje autentizaci uživatelů podle hesla, výchozího hostitele nebo veřejného klíče. Zabezpečuje vzdálená přihlášení, přenos souborů a podporuje směrování (tunneling), díky němuž lze šifrovat i jinak nezabezpečené síťové aplikace.

SSH navíc používá moderní, bezpečné šifrovací algoritmy a je natolik efektivní, že jej můžeme nalézt i v aplikacích, které jsou kritické pro chod i těch nejvýznamnějších společností. [15]

SSH pomáhá administrátorům i koncovým uživatelům efektivně zabezpečit přenos dat a síťové aplikace, jež by jinak zůstaly zranitelné.

7.2.7 PGP

Data vykazovaná do statistik jsou podepisována PGP klíči. Tím je zajištěno, že veškeré důvěrné informace na UTB jsou chráněny silným zabezpečením nezávisle na tom, kde jsou uloženy.

PGP je v současnosti jedním z nejsilnějších prostředků zabezpečení obsahu zpráv, které jsou posílány elektronickou poštou. Tento systém je možno používat pod různými operačními systémy. Díky složitosti faktorizace čísel je zabezpečeno spolehlivé zašifrování dokumentů pomocí veřejných klíčů. Za dokument je možné také přidat elektronický podpis, čímž se zamezí rozesílání zpráv od falešného odesílatele.

7.3 Správce STAGu

Správce studijního systému STAG na UTB má na starosti:

- ✓ uživatelskou část,
- ✓ webové rozhraní,
- ✓ výkazy se studijní agendou,
- ✓ samostatnou databázi, na níž vše běží,
- ✓ zálohování,
- ✓ zřizování přístupu ke STAGu,
- ✓ kompletní STAG.

8 SYSTÉM SAP

8.1 Ekonomický informační systém SAP

Pro řešení ekonomických záležitostí se na UTB využívá ekonomický systém SAP VARIAS Education (SVE) . Hlavním důvodem pro volbu tohoto systému byl fakt, že SAP podporuje standardizované postupy akceptované v EU. V oblasti vzdělávání garantuje korektní a kvalitní procesy uvnitř organizace.

Jedná se o celopodnikové integrované řešení informačního systému, který nabízí využití technologie pro zpracování velkých objemů informací, jež byla v praxi ověřena v různých odvětvích průmyslu na celém světě.

SAP VARIAS Education je na UTB implementován v těchto modulech:

- Finanční účetnictví,
- Investiční majetek,
- Controlling,
- Řízení lidských zdrojů,
- Prodej,
- Materiálové hospodářství a nákup,
- Řízení projektů,
- Báze systému (a v doplňkových řešeních Docházka a Cestovní náhrady).

8.2 Ochrana dat v systému SAP

Ochrana dat je, podobně jako v systému STAG, řešena na několika úrovních:

- 1) *Ochrana přístupu ze sítě na server.*

Server připouští připojení ze sítě pouze z přesně určených adres klientských počítačů a správu provádí pouze administrátor.

2) *Ochrana vstupu do systému.*

Přístup do systému je chráněn přihlášením se pomocí jména a hesla. Toto heslo nelze nikým v systému přechít. Je zde nastavená maximální doba platnosti hesla, po níž musí uživatel své heslo do systému změnit. Také je nastavená minimální délka hesla z důvodu vyšší bezpečnosti. Do systému se nesmí uživatel přihlásit z více počítačů naráz. Správa je prováděna administrátorem.

3) *Ochrana dat z hlediska prováděných činností.*

Uživatel má omezený okruh dat, které smí v systému prohlížet, a dále má přesně vymezený okruh činností, jež smí v systému provádět. Správa je prováděna administrátorem.

4) *Ochrana dat z hlediska chyb zadání uživatele či chybné činnosti programu.*

Většina činností v systému má nastaveny různé kontroly vazeb, které se provádějí už při samotném zadávání dat. Téměř všechny důležité informace jsou evidovány v tzv. měnových dokladech, odkud je možné vyčíst autora nebo čas změny. Systém zaznamenává mnoho prováděných činností a chyb do logů.

5) *Zálohování systému.*

Pro případ havárie systému jsou všechna data pravidelně zálohována. Média se zálohami jsou pečlivě uschována. Správu provádí administrátor.

8.3 Uživatelé

Uživatelé SVE jsou rozděleni na klíčové a koncové uživatele. Klíčový uživatel je jmenován kvestorem UTB jako pracovník, který poskytuje základní servis a školení pro daný modul SVE v rámci své součásti.

Koncovým uživatelem je zaměstnanec UTB nebo jí ovládané společnosti, který v průběhu provozu používá SVE jako nástroj pro podporu své práce a bude s ním v přímé interakci.

Kvestor UTB dále jmenuje garanta modulu pro doplňkové řešení SAP a tzv. vlastníka systému (oba zaměstnanci rektorátu UTB).

Každému uživateli je přiděleno uživatelské jméno a heslo, které je nepřenositelné a každý uživatel odpovídá za jeho zneužití. Bezpečnostní nastavení SVE vyžaduje pravidelnou změnu uživatelského hesla.

8.4 Funkce SAPu

Systém SAP má mnoho funkcí, které svědčí o jeho vyspělosti v rámci ekonomických systémů aplikovaných v podnicích a organizacích různého typu. Systém má následující funkce:

- je globálním standardem v oblasti integrovaného aplikačního softwaru typu klient/server,
- zahrnuje aplikační komponenty pro logistiku, finance, personalistiku, business workflow a připojení na internet,
- je plně konfigurován přesně tak, aby vyhovoval požadavkům organizace,
- poskytuje optimální podporu všem podnikovým procesům, které v organizaci probíhají,
- nabízí podporu více než 800 podnikových procesů formou speciálních branžových řešení,
- zajišťuje automatické propojení mezi jednotlivými komponentami,
- umožňuje přístup všech komponent a funkcí k centrálním sdíleným datům,
- nabízí uživatelům široký rozsah doplňkových služeb, včetně konzultací, školení, technické podpory apod.,
- podporuje mezinárodní prostředí firem, přičemž zohledňuje různé jazyky, měny a národní legislativní požadavky,
- nabízí řešení problematiky spojené se zavedením měny euro, včetně speciálních funkcí a služeb,
- nabízí vlastní metodiku pro vedení projektů – ASAP.

Systém SAP je možné nainstalovat na různých hardwarových platformách s využitím nejmodernějších operačních systémů.

8.5 Systém SAP na jiných VŠ

V současnosti tento systém využívají následující vysoké školy:

- Janáčkova akademie múzických umění v Brně,
- Mendlova zemědělská a lesnická univerzita v Brně,
- Univerzita Palackého v Olomouci,
- Univerzita Tomáše Bati ve Zlíně,
- Vysoká škola báňská – Technická univerzita Ostrava,
- Vysoké učení technické v Brně.

Na závěr této kapitoly bych uvedla, že systém SAP se vyznačuje vysokým stupněm zabezpečení, o čemž svědčí jednotlivé úrovně ochrany dat. Každý uživatel má omezený okruh dat, které si může prohlížet a má také vymezený okruh činností, které smí v systému provádět.

9 ANTIVIROVÁ OCHRANA

Na centrálním poštovním serveru UTB je antivirová ochrana řešena antivirovým systémem NOD32, který kontroluje veškerou příchozí a odchozí poštu. Tento systém funguje v současnosti k plné spokojenosti. Antivirový systém NOD32 byl zvolen zejména na základě cenové politiky, ale i vyšší rychlosti, což hraje určitě důležitou roli.

Na některých pracovních stanicích UTB se dosud používá AVG nebo Avast, ale v budoucnu se plánuje přejít také na antivirový systém NOD32.

9.1 Antivirový systém NOD32

NOD32 je komplexní antivirové řešení pro:

- ✓ stanice (Microsoft Windows 95, 98, ME, NT, 2000, XP, 2003),
- ✓ souborové servery (Windows NT 4, 2000, 2003, Novell),
- ✓ poštovní servery (Linux-SendMail, Qmail, Postfix, MS Exchange Server, Lotus Domino).

Tento systém se stal uznávaným mezi světovou špičkou. Náleží mu prvenství v rychlosti testování (často mnohonásobně vyšší než je u konkurence) při zachování těch nejlepších detekčních schopností. Čtvrtá generace tohoto systému nabízí v současnosti nové špičkové technologie, jakou je například rozšířená heuristická analýza, která umí odhalit HLL WIN32 viry šířící se elektronickou poštou.

Mezi další vlastnosti skenovacího motoru patří:

- virtuální emulátor kódu, který umožňuje detekci nejsložitějších polymorfních a metamorfních virů,
- detekce virů v interně komprimovaných souborech a archivech (ZIP, RAR, ARJ apod.),
- heuristické a algoritmické metody pro odstraňování virů (včetně makrovirů),
- nízká spotřeba systémových zdrojů a minimální zatížení systému,
- plná podpora UNICODE.

9.2 Antispamová ochrana

Na centrálním mailovém serveru UTB je v současné době testován a implementován antispamový systém Spam Assassin.

Tento systém je založen na bázi heuristické analýzy, kdy je provedena analýza obsahu souborů z hlediska jejich naprogramování a následné nalezení virů. Systém funguje na bázi umělé inteligence a je založen na získávání zkušeností a na sebeučení. Systém se umí chovat inteligentně; dokáže najít neznámý spam a dokonce aktualizovat sám sebe a svou databázi spamů. Funguje tak, že nevyžádaná pošta je rozeznávána na základě slov a symbolů, jež spamy většinou obsahují.

Díky tomuto systému je zpřesněno vyhodnocování spamů. Uživatelům je poskytnuta 99% jistota, že jejich emailová schránka bude zbavena nevyžádané pošty. Všechny takto označené spamy jsou uživateli automaticky přesunovány do stejnojmenné složky v jeho osobní schránce.

10 RIZIKOVÁ MÍSTA OCHRANY DAT NA UTB

10.1 Selhání lidského faktoru

K úniku nebo ke zneužití dat, která by měla být chráněna, dochází ve většině případů v důsledku selhání lidského faktoru, což bývá velmi často úplně opomíjeno.

Největší bezpečnostní slabinou a zároveň rizikovým místem ochrany dat v rámci informačního systému UTB je tedy *selhání lidského faktoru*. Tato selhání bývají většinou zapříčiněna:

- Neoprávněným zpřístupněním osobních dat třetím osobám.
- Sdělováním interních informací třetím osobám.
- Poskytnutím (sdělením) hesla cizí osobě.
- Zvolením hesla s lehce odvoditelnými údaji či nezměněním hesla v databázové platformě.
- Nevědomým zanecháním uživatelského jména a hesla poblíž počítače. Často se stává, že uživatelé nechávají svá hesla k uživatelským účtům napsaná na lístečkách nalepených na monitorech počítače, u něhož pracují.

Většina bezpečnostních incidentů pochází od zaměstnanců, jelikož ti mají větší možnost proniknout k datům.

Zaměstnanci, jakož i studenti UTB by se těchto selhání měli vyvarovat a dále by měli dbát deseti nejdůležitějších opatření pro vyšší bezpečnost, které uvádím v 11. kapitole.

Způsoby a metody ochrany dat využívané na UTB, jež jsem analyzovala v praktické části, jsou téměř stoprocentní. Odtud by tedy neměla hrozit ztráta dat či možný únik informací.

Správa hesel a celý management uživatelských i systémových identit je na UTB řešen dodržováním Pravidel provozu počítačové sítě UTB.

III. PROJEKTOVÁ ČÁST

11 PROSTŘEDKY PRO VYŠŠÍ BEZPEČNOST

Pro vyšší zabezpečení dat na UTB a potažmo také v jiných organizacích by se mimo jiné nemělo zapomínat na následujících 10 opatření:

1. Používat bránu firewall pro připojení k internetu.
2. Instalovat aktualizaci softwaru.
3. Používat aktuální antivirový systém.
4. Používat silná hesla včetně pravidelné obměny.
5. Zajistit fyzické zabezpečení.
6. Procházet web „opatrně“.
7. Používat e-mail bezpečně.
8. Pravidelně zálohovat a provádět obnovu.
9. Připojit bezpečně (šifrovaným kanálem) vzdálené uživatele.
10. Zabezpečit bezdrátovou síť kryptografickými nástroji.

Databáze v architektuře klient – server by neměly být přístupné uživatelům ani nežádoucím návštěvníkům. Databázové soubory by tak měly být před okolními zraky skryty, aby nebylo možné data odcizit.

12 ZAVEDENÍ E-PODPISU NA UTB

Hlavním cílem zavedení elektronického podpisu na UTB je vyšší a bezpečnější využívání elektronické komunikace.

Jedním z nejdůležitějších bezpečnostních požadavků při procesu zpracování, ukládání a přenosu informací je zajistit integritu těchto dat, tzn., že data nebudou neoprávněně modifikována. U samostatných dokumentů je toho dosaženo tím, že se k datům připojí určitá informace, která prokazuje totožnost odesílatele. Autentičnost dat na papírových médiích je zajištěna manuálním podpisem, což přináší potřebu nahradit spolehlivě a efektivně manuální podpis podpisem elektronickým. Elektronický podpis může být využit pro identifikaci a autentizaci původní informace všude tam, kde podpis manuální. Elektronický podpis je užíván také pro kontrolu, že nebyla informace po podepsání nijak pozměněna, čímž je zajištěna integrita informace.

Elektronický podpis může být použit v různých aplikacích, jako např. v systémech elektronické pošty, elektronického provádění plateb apod. Může být také zabudován do velkého množství obchodních aplikací vyžadujících elektronickou náhradu běžného podpisu.

V databázových aplikacích je obvykle velmi důležitá integrita dat uložených v databázi (DB). Dokument může být podepsán před vložením do databáze. Po pozdějším vyhledání dokumentu v DB je elektronický podpis zkontrolován. Pokud je správný, uživatel má jistotu, že nebyl nikým modifikován.

Zrychlování výpočetní techniky nemůže ohrozit bezpečnost elektronického podpisu v potřebném časovém horizontu. Útočník, který nezná soukromý klíč subjektu, nemůže vypočítat jeho elektronický podpis. Z toho plyne, že elektronický podpis nemůže být podvržen.

Výhody elektronického podpisu, a to zejména ve vztahu k podpisu vlastnoručnímu, jsou nesporné.

12.1 Elektronický podpis

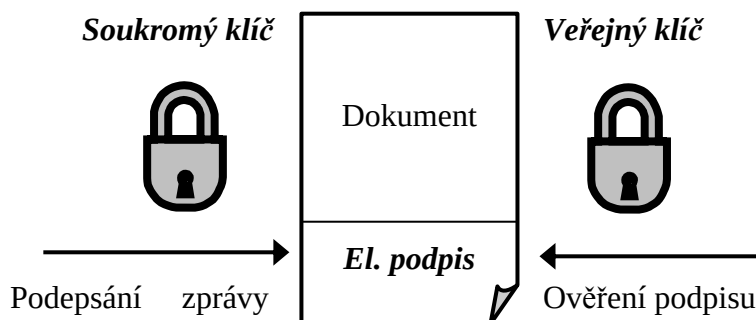
Ve webovém prostředí se objevuje riziko odposlechu citlivých dat, je tedy třeba zamyslet se nad silnějším zabezpečením přihlašování. Problém zvýšení úrovně ochrany osobních dat by mohlo vyřešit zavedení elektronického či digitálního podpisu. Elektronický podpis je velmi složitý, zašifrovaný číselný kód, jež je ojedinělý pro každého uživatele a lze jej právně ověřit. Jeho podstata tkví v označení elektronického dokumentu, z něžž je zřejmá nezpochybnitelná identita autora. Pro šifrování s elektronickým podpisem se v ČR užívá asymetrická kryptografie. K podpisu dokumentu slouží soukromé klíče, k jeho čtení a ověření podpisu pak klíče veřejné.

Metoda elektronického podpisu tkví v tom, že se dokument zašifruje privátním klíčem a následně se dešifruje klíčem veřejným za účelem ověření, kdo dokument zašifroval svým soukromým klíčem.

Princip elektronického podpisu je takový, že data šifrovaná veřejným klíčem je možné dešifrovat pouze v případě, že jsem vlastníkem privátního klíče a naopak. Soukromý klíč je tedy utajený. Pokud znám vlastníka veřejného klíče, znám i odesílatele. Pokud chci zajistit, aby měl k šifrované zprávě přístup jen její adresát, je nutné vlastnit jeho veřejný klíč. Email zašifrovaný veřejným klíčem adresáta lze rozšifrovat jen párovým soukromým klíčem adresáta. Pro podepsání zprávy lze tedy k elektronickému dokumentu připojit jen tentýž dokument zašifrovaný soukromým klíčem. Pro ověření pak stačí dešifrovat zašifrovanou část pomocí veřejného klíče a porovnat ji s nešifrovanou zprávou. Jestliže se obě shodují, byla zpráva zašifrována majitelem soukromého klíče. Je téměř nemožné odvodit z jednoho klíče druhý párový klíč. To znamená, že nelze takovýto podpis zfalšovat.

Asymetrické šifrování je výpočetně dosti náročné, proto se nešifruje zpráva celá, ale jen její „otisk“.

Elektronický podpis zajišťuje autenticitu, integritu dokumentu a nepopíratelnost autora elektronického podpisu.



Obr. 4. Podepsání dokumentu elektronickým podpisem.

12.1.1 Hashovací funkce

Asymetrické šifrování má jednu nevýhodu – je pomalé. Při podepisování rozsáhlejších datových zpráv by uživatel čekal delší dobu na dokončení šifrování, proto se u elektronického podpisu využívá hashovací funkce.

Hashovací funkce je jednocestná matematická operace, kdy vstupem je libovolný dokument či soubor a výstupem je soubor dat o přesně dané velikosti – hash (otisk), tento odpovídá hashovanému dokumentu. Jinak řečeno, vstup má libovolnou délku (obvykle celý diskový soubor), a vytváří malou hodnotu. Ze stejného vstupu vytváří vždy stejný výstup. Výstup je tedy mnohem menší než vstup, a proto musí pro nejméně jednu výstupní hodnotu existovat více vstupních kombinací.

Pro vytvoření výtahu zprávy se používá rychlý algoritmus. Poté je tato malá hodnota podepsána soukromým klíčem. Když zašifrovanou hodnotu příjemce obdrží, může ji dešifrovat veřejným klíčem. Ze vstupního souboru se snadno vytvoří hashovaná hodnota. Pokud se obě hodnoty shodují, je jisté, že příjemce obdržel stejnou zprávu, jež byla odeslána.

Všechny náležitosti spojené s elektronickým podpisem upravuje Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Tento zákon upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností tímto zákonem stanovených a sankce za porušení povinností, jež jsou tímto zákonem stanoveny.

12.1.2 Jak vytvořit elektronický podpis

Pro elektronický podpis potřebujeme dvojici spojených klíčů pro asymetrické šifrování. Pro generování klíčů se používají generátory náhodných čísel, které otestují prvočíselnost vygenerovaného čísla. Pravděpodobnost, že je číslo číslem složeným, je nejvýše 2^{-60} . Nejdříve je vygenerován fyzikální šum (chaos) a poté je kryptograficky a statisticky upraven.

Generování dvojice čísel je většinou součástí žádosti o vydání certifikátu. CA může generovat dvojice klíčů, ale nesmí generovaná data uchovávat. To je důvod, proč většinou probíhá generování dat v počítači žadatele o certifikát.

Vygenerovaný veřejný klíč se přiloží k žádosti o certifikát a soukromý klíč (tj. data pro vytváření elektronického podpisu) si uživatel uloží na médium (většinou na disk). Pro větší bezpečnost je vhodné, aby zůstal soukromý klíč soukromým a aby byl uložen zašifrován s přístupem zabezpečeným heslem.

Nejlepší variantou pro uložení certifikátu je USB token, což je malá tyčinka vybavená flash pamětí, která uchovává data i bez přísunu energie a nehrozí tak jejich ztráta jako u disket. Existují aktivní USB tokeny vytvořené speciálně jen pro elektronický podpis. Obsahují mikročip, který zajišťuje kryptografické operace a umožní použít klíče pouze po zadání hesla, což je mnohem bezpečnější způsob uchování klíče.

Další možností je využití čipové karty, jejíž velikost se rovná velikosti platební karty. Karta má z jedné strany kontaktní plochy pro komunikační rozhraní čtečky a pro svou práci vyžaduje rovněž PIN (osobní identifikační číslo). Klíč zůstává v kartě bezpečně uložen.

12.1.3 Podepisování

Samotné podepsání zprávy elektronickým podpisem provedeme následovně:

- 1) Zprávu necháme projít hashovací funkcí. Získáme její krátký otisk.
- 2) Tento otisk podepíšeme (zašifrujeme soukromým klíčem) a připojíme jej k datové zprávě.
- 3) Datovou zprávu s podepsaným hashem odešleme příjemci.

Příjemce, který před chvílí zprávu dostal, z certifikátu pozná, kdo ji poslal, a podle toho použije příslušný veřejný klíč.

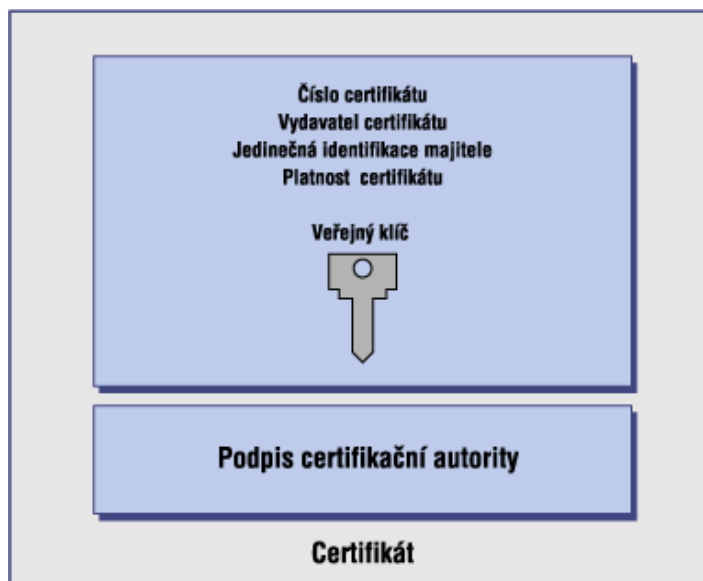
Dále si ověří, že mu zprávu odeslal skutečně držitel certifikátu, a to tak, že rozšifruje hash veřejným klíčem uvedeným v certifikátu. Poté spočítá z datové zprávy svůj hash a porovná jej s dešifrovaným hashem odesílatele. Pokud jsou oba stejné, obsah datové zprávy nebyl od doby jejího podepsání nijak změněn. Tímto krokem si příjemce ověřil integritu obsahu zprávy.

12.2 Certifikační autorita a certifikáty

Certifikát veřejného klíče je datová zpráva, kterou vydává poskytovatel certifikačních služeb neboli certifikační autorita (CA). Tato zpráva slouží k důvěryhodnému předání dat pro ověřování elektronických podpisů (veřejného klíče) podepisující osoby. Certifikát spojuje data pro ověřování podpisu s podepisující osobou a spolehlivě a věrohodně ověřit, ke které fyzické osobě se data pro ověřování elektronických podpisů vztahují. Certifikát používají osoby, které jsou příjemci elektronických podpisů, k tomu, aby si pomocí veřejného klíče v certifikátu ověřili, kdo elektronický podpis vytvořil.

Aby se organizace mohla elektronicky podepisovat, potřebuje kvalifikovaný certifikát, což je jakýsi elektronický průkaz pro používání elektronického podpisu. Pro vydání osobního kvalifikovaného certifikátu je třeba splnit několik kroků a svůj počítač na elektronický podpis připravit.

Certifikační autorita se podobá státnímu notáři. Při komunikaci vystupuje jako třetí nezávislý a důvěryhodný subjekt. Certifikační autorita zaručuje správnost certifikátu, který sama vydala, dále odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá jen v domluvě o společně uznávané CA. Utajovaná data na straně klienta se redukuje jen na bezpečné uchovávání privátního klíče, vše ostatní je řešeno certifikáty. Ty je možné si ověřit kdykoliv, pokud známe veřejný klíč certifikační autority, resp. jím vydaného certifikátu.



Obr. 5. Certifikát. [21]

12.2.1 Tvorba a životnost certifikátu

Generování klíčů. Každý potenciální žadatel o certifikát si nejprve sám pomocí dostupného SW vybavení vygeneruje dvojici klíčů pro použití v asymetrické kryptografii.

Příprava identifikačních dat. Žadatel o certifikát shromáždí podle požadavků certifikační autority osobní identifikační materiály nutné pro vydání certifikátu, jako IČO, DIČO, resp. číslo OP, rodné číslo a podobně.

Předání veřejných klíčů a identifikačních údajů certifikační autoritě. Žadatel předá certifikační autoritě data nutná pro vydání certifikátu spolu s doklady o jejich pravosti.

Ověření informací. Certifikační autorita si na příslušných místech ověří, že může vydat žadateli certifikát.

Tvorba certifikátu. Certifikační autorita vytvoří digitální dokument příslušného formátu a ten poté podepíše svým privátním klíčem.

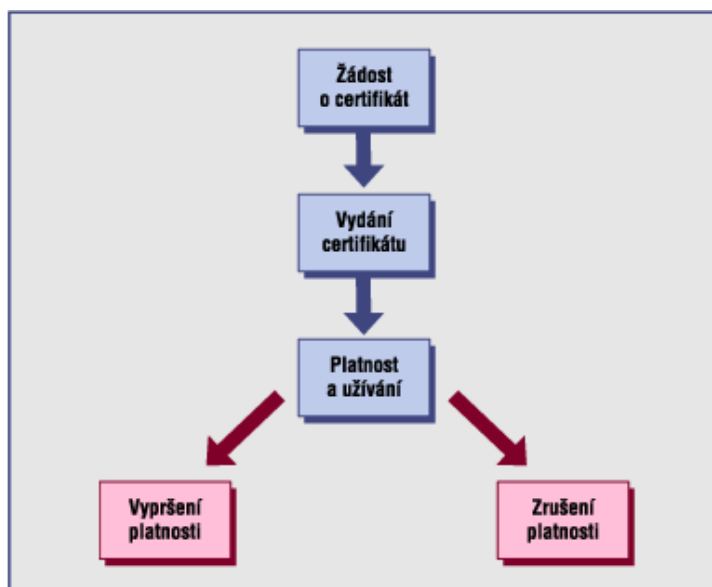
Předání certifikátu. podle dohody je certifikát žadateli předán (disketa), zaslán, nebo zveřejněn.

[21]

Doba platnosti certifikátu je omezená a je uvedena v každém certifikátu, což je velmi důležité. Pokrok ve zvyšování výkonnosti výpočetní techniky a možnost objevení mezer v protokolech či algoritmech by mohl ve větším časovém horizontu zapříčinit nespolehlivost certifikátů.

Běžné certifikáty jsou proto vydávány s platností 6 měsíců, nejvíce však 1 rok. Během této doby je možné platnost certifikátu zrušit, například z důvodu vyzrazení privátního klíče.

Zrušený certifikát je zařazen do seznamu zneplatněných certifikátů. Tento seznam je tedy jakousi „černou listinou“, na níž jsou uvedeny neplatné certifikáty, jejichž doba platnosti ještě nevypršela. Certifikační autorita nemůže klientovi zabránit v užívání certifikátu. Při každé transakci pomocí certifikátů je možné si certifikát díky černé listině ověřit. Seznam zneplatněných certifikátů je veřejnou listinou, která je podepsaná certifikační autoritou a je tedy chráněná stejným způsobem jako certifikát.



Obr. 6. Životní cyklus certifikátu. [21]

12.2.2 Komerční a kvalifikované certifikáty

Tyto dva druhy certifikátů se neliší v použité technologii, ale v účelu jejich možného využití, ve způsobu ověření totožnosti žadatele o certifikát a v neposlední řadě také v tom, kdo může být podepisujícím subjektem.

Pro oba tyto certifikáty existuje odlišná certifikační politika v oblasti vytváření, správy a použití certifikátů.

Kvalifikovaný certifikát je přísně řízen zákonem č. 227/2000 Sb., o elektronickém podpisu a slouží výhradně pro elektronickou oblast.

Komerční certifikát je použitelný také pro oblast digitálního podpisu.

12.3 Certifikační autorita I.CA

První certifikační autorita, a.s. (I.CA), vznikla na pevných základech špičkového světového i tuzemského know-how a týmů kvalitních odborníků v oblasti bezpečnostních technologií a certifikačních autorit.

Certifikační autorita I.CA zahájila poskytování svých služeb v roce 1996 jako součást produktového portfolia společnosti PVT, a.s. Postupně I.CA přerostla hranice projektu a tak byla počátkem roku 2001 založena dceřiná společnost PVT, a.s. s názvem První certifikační autorita, a.s. Tato společnost převzala od mateřské společnosti veškeré činnosti, které bezprostředně souvisí s poskytováním certifikačních služeb. V současnosti je společnost vlastněna několika významnými společnostmi, a to:

- Česká spořitelna, a.s.
- Československá obchodní banka, a.s.
- Eurotel, s.r.o.
- PVT, a.s.
- Státní tiskárna cenin s.p.

I.CA je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice. Svoje služby poskytuje také na Slovensku. Pro zajištění realizace požadavků svých klientů provozuje infrastrukturu tzv. registračních autorit a v současnosti jich spravuje více než 300 po celém území ČR a SR.

Tato kontaktní pracoviště umožňují optimální dostupnost nabízených služeb. Počty vydaných certifikátů jsou dnes evidovány řádově ve statisících.

Úřad pro ochranu osobních údajů udělil První certifikační autoritě, a.s. I.CA akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 18. 3. 2002.

I.CA takto úspěšně ukončila akreditační proces a je oprávněna zahájit poskytování služeb v oblasti kvalifikovaných certifikátů.

Vydávání kvalifikovaných certifikátů určených zejména pro komunikaci v oblasti orgánů veřejné moci I.CA zahájila dne 25. 3. 2002 plně v intencích uvedeného zákona. [18]

12.3.1 Časová razítka

Pojem časového razítka je spojován s využíváním elektronických podpisů. Elektronický podpis dokumentu neposkytuje informaci o tom, kdy byl ten či onen elektronický podpis vytvořen či zda existoval elektronicky podepsaný dokument v určité podobě včera nebo až dnes. Proto se začalo u aplikací a systémů, kde hraje čas provedené operace významnou roli, využívat časových razítek.

Časové razítko je nástroj zajišťující přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům apod. Toto je nezbytné především pro účely jejich zpětného ověřování v budoucnu.

Časové razítko je tedy elektronický důkaz o existenci určitého dokumentu v daném čase. Toto razítko vydává důvěryhodná autorita (I.CA) na základě žádosti o něj. V žádosti je obsažena miniatura (otisk) dat, pro něž má být razítko vystaveno. Obsahuje-li žádost všechny náležitosti, vytvoří časová autorita odpověď obsahující opět otisk dat (a to ten, co byl součástí žádosti) doplněný o aktuální údaj a další parametry, a zašle ji zpět žadateli. ČA využívá k vkládání času tzv. časový zdroj, jež musí být důvěryhodný.

Nejčastější způsoby využití:

- ✓ práce s dokumenty,
- ✓ ochrana logových záznamů v auditních souborech,
- ✓ elektronické podatelny,
- ✓ notářské služby,

- ✓ ochrana programových kódů,
- ✓ uzavírání elektronických smluv,
- ✓ on-line obchody,
- ✓ aplikace s nutným stanovením časového rámce.

12.3.2 Reference

Produkty I.CA využívají v současnosti tyto společnosti:

- ČSOB, a.s. (*ČSOB Homebanking 24, ČSOB Internetbanking 24*)
- ČNZP (*E-ČNZP*)
- RM-Systém, a.s. (*I – zákazník*)
- SCP ČR (*Výpis z registru emitenta*).

12.3.3 Ceník služeb I.CA

Následující ceník služeb I.CA, a.s. je platný od 1. května 2004. Uvedené ceny jsou včetně DPH v zákonné výši (19 %).

Tab. 1. Ceník služeb I.CA. [22]

Komerční certifikát standard	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	322,--s DPH
Komerční certifikát standard	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	580,--s DPH
Komerční certifikát comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací SW I.CA	1-9 ks: 1556,-- s DPH 10 a více ks : 1492,-- s DPH následný (obnovený) komerční certifikát : 580 ,-- s DPH
Kvalifikovaný certifikát standard	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	752,-- s DPH

Kvalifikovaný certifikát comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací SW I.CA	1-9 ks: 1728-- s DPH 10 a více ks : 1663-- s DPH následný (obnovený) kvalifikovaný certifikát : 752 ,-- s DPH
Certifikát pro server	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	1073-- s DPH
Certifikát pro server	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	1931-- s DPH
Nahrání CRL na disketu	Podmínky jsou stejné pro oblast komerčních i kvalifikovaných certifikátů	10-- s DPH
Tištěná certifikační politika I.CA	Podmínky jsou stejné pro oblast komerčních i kvalifikovaných certifikátů	30-- s DPH
Zneplatnění certifikátu	Podmínky jsou stejné pro oblast komerčních i kvalifikovaných certifikátů	0--

12.3.4 Certifikační politika I.CA

Každá certifikační autorita vydává svou certifikační politiku. To je dokument, v němž CA specifikuje postup ověřování identity žadatele o certifikát, jaké nároky na něj klade, za jakých podmínek vydává certifikáty a jakým způsobem se stará o bezpečnost.

Následující politika je určena pro osobní kvalifikované certifikáty. Osobní kvalifikované certifikáty jsou kvalifikované certifikáty určené jako osobní pro ověřování podpisu (např. v rámci elektronické pošty).

Klienti

Osobní kvalifikované certifikáty I.CA jsou komerčně nabízenou službou a jsou přístupné každému, kdo se smluvně zaváže jednat podle této Certifikační politiky.

I.CA požaduje minimální věk 15 let pro osobu, která žádá o vydání osobního kvalifikovaného certifikátu. Žadatelé ve věku 15 – 17 let musí žádat prostřednictvím svého zákonného zástupce.

V případě fyzické osoby může být klientem pouze osoba, která je způsobilá k právním úkonům dle příslušné právní normy.

Pokud žadatel neposkytuje služby RA (registrační autority) přímo pro sebe, ale zastupuje jinou osobu, musí mít oprávnění tuto osobu zastupovat. [14]

Použitelnost

Párová data související s osobními kvalifikovanými certifikáty, které vydává I.CA klientům, mohou být používány v aplikacích pro následující účely:

- pro ověřování elektronických podpisů,
- pro bezpečné ověřování elektronických podpisů,
- k zajištění neodmítnutelnosti odpovědnosti.

K jiným než výše uvedeným aplikacím není osobní kvalifikovaný certifikát určen.

Povinnosti zúčastněných stran

I.CA je povinna dodržovat příslušná ustanovení právních norem upravujících oblast poskytování certifikačních služeb nebo obchodní činnost s tímto spojenou. Dále se zavazuje řídit se vlastními normativními dokumenty, jež vydává. I.CA se taktéž zavazuje vytvářet dokumenty upravující činnost smluvních partnerů, zajišťovat jejich zveřejnění a dohlížet na jejich dodržování. Je povinna zajistit, aby se každý mohl ujistit o její identitě a musí zajistit dostupnost svého kvalifikovaného certifikátu. Vztah mezi I.CA jakožto poskytovatelem certifikačních služeb a klienty je striktně dán smlouvou. I.CA nevystupuje v žádném případě jako zmocněnec nebo jiný zástupce klientů. Totéž platí pro smluvní partnery.

Registrační autority (RA) jsou povinny řídit se dokumenty, normami a směrnicemi, které I.CA vydává a které upravují jejich činnost (Certifikační politika, Certifikační prováděcí směrnice, Směrnice pro RA, apod.).

Držitelé osobních kvalifikovaných certifikátů jsou povinni:

- používat osobní kvalifikované certifikáty výhradně v souladu s touto Certifikační politikou,
- dodržovat veškerá ustanovení této Certifikační politiky,
- dodržovat veškerá ustanovení příslušné smlouvy o vydání OQC.

Kromě jmenovaných mají i další povinnosti vyplývající např. ze Zákona o elektronickém podpisu.

Uživatelé kvalifikovaných certifikátů jsou povinni užívat osobní kvalifikované certifikáty v souladu s platnou Certifikační politikou pro tyto certifikáty a s příslušnými právními normami (jako např. ZoEP), zejména pak kontrolovat platnost osobního kvalifikovaného certifikátu, především:

- časové údaje o platnosti,
- podpis osobního kvalifikovaného certifikátu certifikační autoritou,
- výskyt osobního kvalifikovaného certifikátu na seznamu kvalifikovaných certifikátů, které byly zneplatněny,
- důvěryhodnost odpovídajícího kvalifikovaného certifikátu poskytovatele certifikačních služeb.

Odpovědnost a záruky

I.CA ručí za to, že použije vlastní soukromé klíče příslušné svým kvalifikovaným certifikátům pouze k podepisování jí vydaných certifikátů a seznamu zneplatněných kvalifikovaných certifikátů.

I.CA poskytuje záruku na zneplatnění osobního kvalifikovaného certifikátu, pokud byla žádost o ukončení platnosti osobního kvalifikovaného certifikátu podána způsobem definovaným v Certifikační politice.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen, pokud klient neporušil povinnosti plynoucí mu ze smlouvy mezi ním a I.CA, a z Certifikační politiky. Klient uplatňuje vždy záruku u Registrační autority, která jej zaregistrovala.

Pokud není smluvní partner schopen vyřídit záruční nároky ve své pravomoci, postoupí je k řízení I.CA a o této skutečnosti vyrozumí klienta. Na používání certifikátu, který I.CA nevydala, se záruky nevztahují.

Vždy platí limit záruky, který byl sjednán v písemné podobě (Smlouva o poskytnutí služeb). Pokud překračuje výše nárokové ztráty sjednaný limit, poskytne I.CA plnění maximálně do výše limitu. Pokud bylo zjištěno porušení povinností klienta, které má souvislost s uváděnou škodou, záruční plnění se neposkytne. Toto musí být klientovi oznámeno a zaprotokolováno.

RA přejímá závazek za správné vyřízení žádosti o poskytování certifikačních služeb. RA nevyřídí žádost kladně, pokud klient neprokázal hodnověrným způsobem svoji totožnost, odmítá sdělit potřebné údaje či odmítne podepsat příslušné dokumenty.

RA zodpovídá za včasné předání žádosti o ukončení platnosti osobních kvalifikovaných certifikátů k vyřízení na pracoviště CA. Rovněž odpovídá za vyřizování připomínek a stížností klientů.

12.3.5 Certifikáty Standard a Comfort

Osobní kvalifikované certifikáty Standard jsou vhodné především pro elektronickou komunikaci. Jejich využití není omezeno jen na tuto oblast, ale existují i další možnosti, kde tento typ certifikátu využít, jako např. v komerční sféře (B2B, B2C) apod.

Osobní kvalifikované certifikáty Comfort se od těchto liší zejména v použití čipové karty, která zaručuje mnohem vyšší bezpečnost.

Pro certifikaci elektronického podpisu na UTB jsem zvolila kvalifikovaný certifikát Comfort, jehož součástí je čipová karta sloužící jako médium k bezpečnému uložení dat pro tvorbu elektronického podpisu a k bezpečnému vytváření elektronického podpisu. Toto řešení může přinést výrazné zvýšení bezpečnosti uložených dat. Tato karta zajišťuje interní bezpečnost organizací, čímž je míněna především bezpečná autentizace a přihlášení do systému.

12.3.6 Osobní kvalifikovaný certifikát Comfort

Tento certifikát splňuje všechny podmínky pro využití v oblasti orgánů veřejné moci v souladu s § 11 zákona č. 227/2000 Sb., o elektronickém podpisu, jelikož je vydáván akreditovaným poskytovatelem certifikačních služeb.

Prostřednictvím osobního kvalifikovaného certifikátu vydaného společností I.CA je fyzická totožnost subjektu svázána s jeho elektronickou totožností, resp. s jeho daty pro ověřování elektronických podpisů.

Tento typ certifikátu je vhodný zejména pro elektronickou komunikaci ve smyslu výše uvedeného zákona. Jeho využití ale není omezené jen na tuto oblast, nabízí také řadu příležitostí v rámci komerční sféry (B2B, B2C).

Kvalifikovaný certifikát Comfort, jak jsem již výše uvedla, využívá kryptografickou čipovou kartu, která slouží jako prostředník k bezpečnému vytváření elektronického podpisu. Spolehlivě uchovává tajemství jí svěřené (tj. data pro tvorbu elektronického podpisu). Přímo na kartě probíhá nejdříve vlastní generace dat pro tvorbu elektronického podpisu, poté vlastní tvorba elektronického podpisu vlastníka těchto dat. Důvěrná data uživatele se prakticky nikdy nedostanou mimo kartu. Na kartě je zároveň uložen kvalifikovaný certifikát. Platnost dat pro tvorbu elektronického podpisu uložených na kartě je stanovena na 1 rok, přičemž na tuto čipovou kartu je možné uložit celkem tři po sobě následující data pro tvorbu elektronického podpisu. Čipová karta je tudíž určena k používání po dobu tří let.

Tento certifikát je vydáván na základě řádně vyplněné žádosti o kvalifikovaný certifikát.

Předpoklady pro zavedení služby:

- ✓ HW s odpovídajícím výkonem umožňujícím provoz operačního systému Windows 95/98, Windows NT, Windows 2000;
- ✓ Internet Explorer 5.0 a vyšší;
- ✓ čtečka čipových karet.

Postup pro získání osobního kvalifikovaného certifikátu Comfort:

1. Získání čipové karty (přímo u I.CA, a.s.).
2. Čtečka čipových karet (pro využívání služby certifikát comfort je nutné vlastnit čtečku čipových karet).
3. Instalace ovládací aplikace (před zahájením tvorby elektronické žádosti je nutné provést instalaci ovládací aplikace, která umožní pracovat s čipovou kartou).
4. Instalace kořenového certifikátu I.CA – pro oblast kvalifikovaných certifikátů.
5. Vytvoření žádosti o certifikát (prostřednictvím formulářového dialogu na počítači, na němž se bude elektronický podpis používat).
6. Návštěva kontaktního pracoviště I.CA (s vytvořenou žádostí je nutné se dostavit na některé z kontaktních pracovišť I.CA, kde bude operátorce předána disketa se žádostí, osobní doklady a dokumenty k ověření).
7. Instalace kvalifikovaného certifikátu do systému (v uživatelském prostředí počítače podle instrukcí zaslaných na e-mailovou adresu v certifikátu uvedenou).

Objednání čipové karty

Objednávka musí obsahovat tyto náležitosti:

- přesná data odběratele – celou adresu pro dodání zboží a kompletní fakturační údaje,
- počet kusů karet,
- typ služby – čipové karty pro kvalifikovaný certifikát,
- personalizační data – jméno a příjmení držitele karty.

Objednávku je třeba poslat na adresu I.CA, a.s. Termín dodání čipových karet je přibližně 10 – 14 dní od doručení objednávky.

Elektronická žádost je vytvořena pomocí formulářového dialogu. Záleží, zda si vybere žádost pro uživatele či odborníka. V našem případě jsem zvolila Odborníka.

Po stisknutí na tlačítko Odborník se objeví na obrazovce toto dialogové okno, které zájemce vyplní a odešle.

Žádost o certifikát pro	Vyberte možnost
Velikost klíče a platnost certifikátu	1024 bit - platnost 12 měsíců
Non Repudiation	☒
Digital Signature	☒
Key Encipherment	☐
Data Encipherment	☐
Typ klíče	
Jméno klíče	08032005155:
Typ použití klíče	Klíč pro podpis a šifrování
Typ kódování položek certifikátu	BMP_STRING

Obr. 7. Elektronická žádost o certifikát. [20]

Před tvorbou žádosti o kvalifikovaný certifikát je nutné, aby se každý klient seznámil s aktuální certifikační politikou I.CA pro vydávání osobních kvalifikovaných certifikátů. V ní jsou uvedena všechna práva a povinnosti, které souvisejí s používáním certifikátu.

Zavedení elektronického podpisu na UTB by bylo pravděpodobně vícefázové a odpovídalo by podobnému zavedení na veřejné správě.

V první fázi by se toto zavedení týkalo všech vedoucích zaměstnanců jednotlivých pracovišť a pracovníků s ekonomickou odpovědností. Ve druhé fázi by byl elektronický podpis zaváděn u všech dalších, odpovědných zaměstnanců, jež pracují s nějakou formou osobních údajů.

13 RODNÁ ČÍSLA A BUDOUCNOST

Za nejcitlivější osobní údaj bývá označováno rodné číslo, jemuž jsem vymezila prostor v této, poslední, kapitole.

Do certifikátu vydaného I.CA bývá přidáván také identifikátor Ministerstva práce a sociálních věcí, který by měl v budoucnu nahradit rodné číslo. Pro zabezpečení snazší a jednoznačné identifikace osoby je nutný nějaký identifikátor, nejlépe číslo. V evidenci rodných čísel existuje mnoho duplicít a z rodného čísla je možné odvodit, jaké je datum narození dané osoby, zda se jedná o ženu či muže, což je hlavním důvodem pro vývoj nového identifikátoru.

Identifikátor MPSV je náhodně generované číslo, jež nebude mít jiný než identifikační význam. Je to deseticiferné číslo v rozsahu 1 100 100 100 až 4 294 967 295. Tento identifikátor by měl zajistit v budoucnosti větší bezpečnost osobních dat a měl by zabránit jejich duplicitě.

Za 40 let by měla být rodná čísla plně nahrazena.

ZÁVĚR

Na UTB je přísně dodržován Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Data mohou být poskytována na základě písemné žádosti jen soudu a policii, a to v případě přestupku, výživného apod. Zaměstnanci UTB se musejí řídit povinnostmi, které jim ukládá zákon, a dále se řídí pravidly provozu počítačové sítě UTB.

Přístup k datům mají správci systémů, studijní referentky, zaměstnanci knihovny, zaměstnanci personálního oddělení a mzdové účtárny.

Na UTB jsou v současné době zavedeny dva informační systémy, a to systém STAG určený pro studenty, a systém SAP, což je ekonomický informační systém pro zaměstnance univerzity. Ochrana dat v těchto systémech je téměř stoprocentní, na čemž má zásluhu zejména využívání bezpečných šifrovacích kanálů (protokolů) – SSL, SSH, HTTPS a další technologie zajišťující maximální ochranu dat.

Přístup do systémů mají jen pověřené osoby, jež jsou k tomuto kompetentní.

Ochrana dat v IS/STAG je zajištěna na úrovni databáze nad databází Oracle 9i. Přístup k serveru chrání také firewall, což je efektivní nástroj k ochraně serverových systémů před červy, přepsáním zásobníku a dalšími bezpečnostními hrozbami z internetu. Všechna data jsou uložena v serverovně, což je místnost k tomuto určená. Průběžně, a to přesně 1x za 14 dní, jsou data zálohována na magnetické pásky. Další úrovní ochrany jsou uživatelská konta s hesly. Zajištění bezpečného přístupu k osobním stránkám podporuje webový server STAG technologií SSL, tzn., že komunikace klienta se serverem probíhá šifrovaně. Data vykazovaná do statistik jsou podepisována PGP klíči, jsou tedy silně zabezpečena.

Ochrana dat v IS/SAP je zajištěna obdobně. Každý uživatel má omezený okruh dat, která smí prohlížet, a vymezený okruh činností, jež smí provádět. Data jsou stejně jako ve STAGu bezpečně zálohována. Server připouští připojení ze sítě pouze z přesně určených adres klientských počítačů.

Další částí je antivirová ochrana systémů na centrálním poštovním serveru UTB, která je řešena antivirovým systémem NOD32 patřícím v současnosti ke špičce v oblasti antivirové ochrany.

Na základě zjištěných skutečností se jediné rizikové místo objevuje v oblasti selhání lidského faktoru, jehož důsledkem bývá nejčastěji prozrazení hesel, umožnění přístupu do sítě neoprávněným osobám apod.

Zavedení elektronického podpisu na UTB, jemuž se věnuji v projektové části, je dobrou úvahou, ale sama UTB na tyto kroky ještě není zcela připravena. Na základě rozhovoru se tato technologie zdá pracovníkům CVT (Centrum výpočetní techniky) prozatím zbytečná.

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE

- [1] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana: kniha pro praxi*. 1.vyd. Praha: ASPI Publishing, 2003. 415s. ISBN 80-86395-50-2.
- [2] NEJEDLÝ, Josef. *Ochrana osobních údajů*. 1. vyd. Vyškov: Irena Spirová, 2004. 160 s. ISBN 80-239-3896-7.
- [3] PŘIBYL, Jiří, KODL, Jindřich. *Ochrana dat v informatice*. 1. vyd. Praha: ČVUT, 1997. 299 s. ISBN 80-01-01664-1.
- [4] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. 1. vyd. Zlín: UTB ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.
- [5] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. 1. vyd. Praha: EUROUNION, 2001. 379 s. ISBN 80-85858-93-2.
- [6] BENDA, Radek, ROSMAN, Pavel, SODOMKA, Petr. *Informatika a výpočetní technika*. 1. vyd. Zlín: VUT v Brně, FaME, 1999. 152 s. ISBN 80-214-1396-4.
- [7] STEINBERGER, J. *Zpracování digitálního podpisu pro autentizaci přístupu Oracle Portal*. Plzeň, 2003. 150 s. Diplomová práce na Fakultě aplikovaných věd Západočeské univerzity v Plzni na katedře informatiky a výpočetní techniky.
- [8] STEGURA, T. *Teorie a praxe elektronického podpisu*. Praha, 2004. 69 s. Bakalářská práce na Fakultě informatiky a statistiky Vysoké školy ekonomické v Praze na katedře systémové analýzy.

INTERNETOVÉ ZDROJE

- [9] Směrnice rektora č. 1 /2001. *Ochrana osobních údajů v informačním systému UTB ve Zlíně* [online]. 2001. Dostupné z WWW: <http://www.utb.cz/czech/rektorat/smernice1.php>.
- [10] Směrnice kvestora. *Uživatelé a provoz informačního systému SAP* [online]. 2005. Dostupné z WWW: http://web.utb.cz/cs/docs/sk2_2005.pdf.

- [11] LUKEŠ, Dan. *HTTPS – bezpečnost jen pro vyvolené?* [online]. 2001. Dostupné z WWW: <<http://www.lupa.cz/clanek.php3?show=1363>>.
- [12] THAYER, Rodney. *SSH: Bezpečné přihlášení na vzdálený počítač* [online]. 2004. Dostupné z WWW: <<http://www.spok.cz/web/cz/security/ssllssh.html>>.
- [13] *Certifikáty webového serveru* [online]. Dostupné z WWW: <<http://www.stag.utb.cz/web/certifikaty/certifikaty.htm>>.
- [14] *Certifikační politika pro vydávání osobních kvalifikovaných certifikátů* [online]. 2000. Dostupné z WWW: <<http://www.ica.cz/qcp/cpqpica02.pdf>>.
- [15] *SSH – Kompletní průvodce – Barrett, Silverman* [online]. Dostupné z WWW: <<http://knihy.cpress.cz/Book.asp?ID=669>>.
- [16] *NOD32 Antivirus System* [online]. 2004. Dostupné z WWW: <<http://www.esetsoftware.cz/d>>.
- [17] *Co je SSL certifikát (informace pro každého)* [online]. Dostupné z WWW: <<http://www.certifikaty.com/>>.
- [18] *Obecné informace. O společnosti* [online]. 2000. Dostupné z WWW: <http://www.ica.cz/ica0_0.html>.
- [19] *Žádost o certifikát. Kvalifikovaný certifikát Comfort* [online]. 2000. Dostupné z WWW: <<http://www.ica.cz/zisk.kva.comfort.html>>.
- [20] *Elektronická žádost o kvalifikovaný certifikát* [online]. Dostupné z WWW: <<https://b.ica.cz/qoc.cgi>>.
- [21] *Certifikační autorita a certifikáty* [online]. 2000. Dostupné z WWW: <http://www.ica.cz/principy_certifikaty.html>.
- [22] *Ceník služeb* [online]. 2004. Dostupné z WWW: <<http://www.ica.cz/cenik.html>>.
- [23] *Kerio ServerFirewall* [online]. Dostupné z WWW: <http://www.kerio.cz/ksf_home.html>.
- [24] *Úvodní stránka IS/STAG* [online]. Dostupné z WWW: <<http://stag.zcu.cz/index.php>>.
- [25] *Popis IS/STAG* [online]. Dostupné z WWW: <<http://stag.zcu.cz/>>.
- [26] *Seznam odkazů* [online]. Dostupné z WWW: <<http://stag.zcu.cz/odkazy.php>>.

- [27] *Electronic signature* [online]. Dostupné z WWW:
<http://www.micr.cz/epodpis/default_en.htm>.
- [28] *Elektronický podpis obcím* [online]. Dostupné z WWW:
<<http://www.micr.cz/scripts/detail.php?id=1998>>.

DOKUMENTACE A ÚŘEDNÍ NORMY UTB

- [29] SÁHA, P. *Postup při podávání a vyřizování žádostí o poskytnutí informace, vydávání rozhodnutí a vyřizování odvolání proti nim na Univerzitě Tomáše Bati ve Zlíně*. Dodatek č. 1 k rozhodnutí rektora č. 6/2002.
- [30] SÁHA, P. *Poskytování informací v souladu se zákonem o svobodném přístupu k informacím*. Rozhodnutí rektora č. 6/2002.
- [31] SÁHA, P. *Dodržování autorského zákona*. Rozhodnutí rektora č. 7/2002.
- [32] *Informace a materiály poskytnuté pověřenými osobami na UTB ve Zlíně*.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASAP	Implementační metodika systému SAP.
AVG	Antivirus Grisoft.
B2B	Business to Business.
B2C	Business to Customer.
CA	Certifikační autorita.
CRL	Certificate Revocation List.
CRM	Customer Relationship Management.
CVT	Centrum výpočetní techniky.
ČA	Časová autorita.
DB	Databáze.
DP	Diplomová práce.
EXE	Execute.
Hash	Otisk.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
HW	Hardware.
I.CA	První certifikační autorita.
IE	Internet Explorer.
IP	Internet Protocol.
IS	Informační systém.
MPSV	Ministerstvo práce a sociálních věcí.
NNTP	Network News Transfer Protocol.
NOD32	Antivirový systém.
OQC	Osobní kvalifikovaný certifikát.

PGP	Pretty Good Privacy – kryptografický produkt.
PIN	Personal Identification Number – osobní identifikační číslo.
RA	Registrační autorita.
SAP	Ekonomický informační systém.
SIMS	Sdružené informace matrik studentů.
SSH	Shell Secure – metoda zabezpečení sítě.
SSL	Secure Societ Layer.
STAG	Studijní agenda.
SVE	SAP VARIAS Education.
SW	Software.
TCP	Transmission Control Protocol.
TeX	Systém pro tisk dokumentů.
TLS	Transport Layer Security.
ÚIV	Ústav pro informace ve vzdělávání.
ÚOOÚ	Úřad pro ochranu osobních údajů.
URL	Uniform Resource Locator.
USB	Universal Serial Bus.
UTB	Univerzita Tomáše Bati.
VPD	Virtual Private Database.
ZoEP	Zákon o elektronickém podpisu.

SEZNAM OBRÁZKŮ

Obr. 1. Výstraha zabezpečení.	36
Obr. 2. Přihlášení do IS STAG.	37
Obr. 3. Nasazení IS/STAG na vysokých školách a vyšších odborných školách.	46
Obr. 4. Podepsání dokumentu elektronickým podpisem.	58
Obr. 5. Certifikát.	61
Obr. 6. Životní cyklus certifikátu.	62
Obr. 7. Elektronická žádost o certifikát.	72

SEZNAM TABULEK

Tab. 1. Ceník služeb I.CA.	65
---------------------------------	----