Masarykova univerzita v Brně

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informační studií a knihovnictví

Ochrana osobních údajů ve veřejné správě

Seminární práce k předmětu Informační politika

Autor: Martin Hájek

UČO: 398415

Typ studia: kombinované

Ročník: 2.NMgr.

Brno

7. 11. 2012

Ochrana osobních údajů ve veřejné správě

1. Legislativní vymezení ochrany osobních údajů

Ochrana osobních údajů ve veřejné správě i v dalších odvětvích se vztahuje na jakékoliv údaje, které se týkají určité osoby, nebo ji přijatelným způsobem identifikují. Může mezi ně patřit jméno, bydliště, údaje o narození, rodné číslo a další specifická data. Na začátek je vhodné uvést vysvětlení některých pojmů.

- **Veřejná správa** – je správa veřejných záležitostí ve prospěch veřejného zájmu občanů a je součástí výkonné moci. Veřejná správa se dělí na další dva subsystémy, a to státní správu a samosprávu. Další vymezení se váže k činnostem, které vykonává

- **Osobní údaj** – **„***jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“* [2, § 4, písm. a]

- **Citlivý údaj** – *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů“* [2, § 4, písm. b]

- **Subjekt údajů** – *„subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují“* [2, § 4, písm. d]

- **Správce** – *„správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak“* [2, § 4, písm. j]

- **Zpracovatel** – *„zpracovatelem každý subjekt, který na základě zvláštního zmocnění nebo pověření správcem zpracovává osobní údaje dle tohoto zákona“* [2, § 4, písm. k]

- **Zpracování osobních údajů** – *„zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava*

nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace" [2, § 4, písm. e]

- **Shromažďování osobních údajů** – *„shromažďováním osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování"* [2, § 4, písm. f]

- **Uchovávání osobních údajů** - *„uchováváním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat"* [2, § 4, písm. g]

Ochrana osobních údajů se v České republice v obecné rovině řídí těmito zákony:

Zákon číslo 101/2000 Sb. O ochraně osobních údajů a o změně některých zákonů.

Směrnicí Evropského parlamentu a Rady 95/94/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Mezi speciální předpisy o ochraně osobních údajů patří tyto zákony:

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

Směrnice Evropského parlamentu a rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu)

Činnost veřejné správy se při své práci neobejde bez osobních údajů občanů. Dnes jsou osobní data evidována v informačních systémech veřejné správy a trend vede ke sjednocování databází, aby byly informace přístupné v každé oblasti. Jak s osobními údaji nakládat vymezuje legislativa. Ze zákona rozlišujeme dva druhy osob. První jsou ti, kteří s osobními údaji určitým způsobem nakládají. Těmi jsou správci osobních údajů a zpracovatelé osobních údajů. Při zpracovávání osobních údajů jsou vytyčeny určité povinnosti. V případě neplnění povinností, hrozí sankce. Každý, kdo nakládá s osobními údaji,

si musí být vědom svých práv i povinností a musí být schopen je realizovat. Ke správné realizaci je vhodné použít nástroje. Ty jsou uzpůsobeny pro potřeby každé instituce zvlášť (nemocnice, školy, obce, kraje,….). Další jsou *subjekty údajů*. To jsou lidé, kteří své osobní údaje poskytují ke zpracování. Ti mají také určité povinnosti, ale v jejich případě zákon určuje hlavně, jaká mají při zpracování osobních údajů práva.

1.1 Zákon číslo 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů

Zákon upravuje ochranu osobních údajů při jakémkoliv nakládání s nimi a to jak manuálně, tak i prostřednictvím automatizovaných informačních systémů, které se dnes již běžně používají v rámci veřejné správy. Zpracovatel osobních údajů má ze zákona povinnost informovat subjekt údajů o jeho právech a dalších pro něj významných skutečnostech. Zákon upravuje práva občana na ochranu osobních údajů a představuje mechanismy, které má k dispozici při řešení situací, kdy by mohlo dojít ke zneužití osobních údajů. V rámci IV. hlavy § 28 tohoto zákona byla mimo jiné definována role Úřadu pro ochranu osobních údajů, který je vybaven kontrolními, vyšetřovacími, registračními a metodickými funkcemi pro ochranu osobních údajů občanů. Plné znění zákona je možné dohledat na stránkách úřadu. [2, § 28]

1.2 Práva a povinnosti při zpracování osobních údajů

Správce osobních údajů je povinen zpracovávat pouze přesné údaje se souhlasem subjektu údajů. Každá instituce musí stanovit účel, k němuž jsou osobní údaje zpracovávány, prostředky a způsob jejich zpracovávání. Dále smí zpracovávat osobní údaje pouze v takovém rozsahu a po tak dlouhou dobu dokud je to nezbytné pro naplnění účelu sběru osobních údajů. Po uplynutí nezbytně dlouhé lhůty mohou být osobní údaje uchovávány pouze pro statistické, vědecké nebo archivní účely. Dále je možné osobní údaje zpracovávat pouze v souladu s účelem, k němuž byly shromážděny. K jinému účelu je lze zpracovávat pouze se souhlasem subjektu údajů a to jen v mezích ustanovení §3 odstavce 6 Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. V neposlední řadě není možné sdružovat na jednom místě osobní údaje získané k rozdílným účelům. [2, § 5]

Správce nebo zpracovatel osobních údajů může bez souhlasu subjektu údajů zpracovávat osobní údaje, jestliže provádí zpracování nezbytné pro dodržení povinností správce, nebo pro dodržení smlouvy, jejíž jednou stranou je právě subjekt údajů. Dále je zpracování osobních údajů bez souhlasu možné v případě, že se jedná o záchranu života nebo zájmů

subjektu údajů. Ihned, jak to bude možné, je ovšem nutno získat souhlas subjektu. Zpracovat údaje bez souhlasu je možné i v případě, že se jedná o veřejnou nebo veřejně činnou osobu a osobní údaje vypovídají o jejím veřejném konání. [2, § 5, odst. 2]

1.3 Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů je nezávislý orgán sídlící v Praze, jeho činnost je vymezena zákonem číslo 101/2000 Sb. o ochraně osobních údajů a změně některých zákonů a některými dalšími zákony, právními předpisy a smlouvami. Úřad má ve veřejné správě kontrolní funkci. Provádí dozor nad dodržováním zákonných povinností při zpracování osobních údajů. Vede registr povolených způsobů zpracování osobních údajů. Přijímá stížnosti, podněty a návrhy občanů na porušení zákona. V čele úřadu stojí předseda, kterého jmenuje prezident republiky. Prezident také jmenuje 7 inspektorů úřadu. Ti provádějí kontrolní činnost a řídí ostatní zaměstnance při kontrole. Při porušení zákona o ochraně osobních údajů, má úřad možnost udělit přísné sankce. V případě fyzické osoby se může jednat o sankce do výše 5 000 000 Kč. U právnické osoby se může výše sankce vyšplhat až k 10 000 000 Kč. Udělování sankcí a další postih je popsán v § 44 až 46 zákona o ochraně osobních údajů. [16]

Úřad pro ochranu osobních údajů v rámci platného zákona číslo 111/2009 Sb. o základních registrech a jeho změna zákonem číslo 100/2010S Sb., spustil v červenci roku 2012 nový projekt IS ORG. Projekt si klade za cíl nahradit dosavadní rodné číslo jakožto univerzálního identifikátoru systémem samostatných bezvýznamných identifikátorů. Pro každou agendu bude jiný identifikátor a na základě znalosti jednoho identifikátoru bude možné dohledat údaje o fyzické osobě i v jiné agendě. Všechny identifikátory budou uloženy právě v systému IS ORG ovšem bez informací umožňujících jejich přiřazení fyzické osobě.[17]

1.4 Specialita jménem rodné číslo

Rodné číslo je speciální tím, že bylo přiděleno všem obyvatelům České republiky a samo osobě je unikátním identifikačním znakem. O svém nositeli vypovídá snad nejvíce ze všech ostatních osobních údajů (datum narození, pohlaví). Rodné číslo může být použito jako důležitý klíč při vyhledávání subjektů ve všech informačních systémech veřejné správy.

Směrnice a nařízení v případě rodného čísla hovoří jasně. Každá země si své vnitrostátní identifikační číslo upravuje v souladu se zákony, které u nich platí. V České republice je rodné

číslo upraveno Zákonem číslo 133/2000 Sb. O evidenci obyvatel a rodných čísel. Bez souhlasu nositele rodného čísla jej smí zpracovávat pouze správní orgány a další subjekty v případech přesně stanovených zákonem. [3]

1.5 Zneužití osobních údajů

Zneužití osobních údajů je v podstatě jakékoliv neoprávněné nakládání s osobními údaji, které jsou chráněné a jejich zneužití se trestá podle zákona 101/2000 Sb. O ochraně osobních údajů. Každý kdo informace shromažďuje, zpracovává nebo uchovává, musí učinit taková opatření, aby nedošlo k jejich zneužití, zničení, ztrátě nebo odcizení.

Trestní zákoník hovoří v této věci zcela jasně. Podle § 180 trestního zákoníku č. 40/2009 Sb., ve znění pozdějších předpisů, je vymezena skutková podstata trestného činu neoprávněného nakládání s osobními údaji. Trestného činu se dopustí ten, kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné moci a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. V případě zneužití osobních údajů jsou udělovány sankce ve formě pokut. Pokuty jsou vyměřovány s ohledem na závažnost činu a podle uvážení Úřadu pro ochranu osobních údajů s přihlédnutím ke zpracovateli osobních údajů.[1, § 180]

2. Ochrana osobních údajů v informačních systémech

Základem každého informačního systému jsou informace. Stejně je tomu u informačních systémů veřejné správy. Mezi informace řadíme samozřejmě i osobní údaje. Všechny informace jsou v systému uchovávány ve formě dat v určitých databázích. Tato data je nutné v rámci systému dobře chránit, aby nedošlo k jejich zcizení a zneužití. Klasická bezpečnostní opatření lze rozdělit do několika na sebe navazujících úrovní.

2.1 Informační systémy veřejné správy

Informační systémy veřejné správy jsou souborem informačních systémů sloužících pro výkon veřejné správy. Patří mezi ně i činnosti podle zvláštních zákonů. Mezi správce těchto informačních systémů můžeme zařadit ministerstva, správní úřady a územní samosprávní celky (orgány veřejné správy).

Portál veřejné správy – informační systém veřejné správy zajišťující přístup k informacím státních orgánů, orgánů územních samosprávních celků a orgánů veřejné moci, které však nejsou státními orgány ani orgány územních samosprávních celků [4, § 2, písm. e]

Kontaktní místa veřejné správy – Pro kontakt s veřejnou správou a pro případné podání správním orgánům slouží kontaktní místa, mezi která patří:

a) Notáři
b) Krajské úřady
c) Matriční úřady
d) Územní samosprávní celky – např. obecní úřad, městský úřad…
e) Zastupitelské úřady

2.2 Tři úrovně bezpečnostní architektury

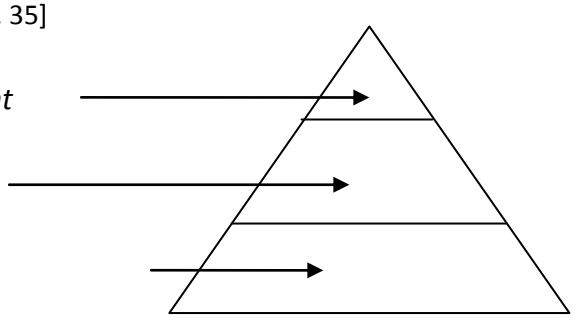
Data jsou proti odcizení a zneužití v informačních systémech chráněna na několika úrovních bezpečnostní architektury. Jejich dodržování by mělo zaručit ochranu a bezproblémové zabezpečení systému.

a) **Základní úroveň zabezpečení** – chrání před útoky a proti neoprávněnému přístupu do systému. Patří sem antivirové programy, firewallové zabezpečení a kontrola oprávněných přístupů do systému
b) **Střední úroveň zabezpečení** – log management – tento systém sbírá a ukládá obrovské množství bezpečnostních záznamů s možností vyhledávání a zobrazení
c) **Nejvyšší úroveň** – SIEM (security information and event management) jedná se o monitorování činnosti jednotlivých uživatelů v rámci systému, kontrola toho k jakým datům přistupují a jak s nimi nakládají [10, s. 35]

SIEM – Security information and event management

Log Management – IDS/IPS, scanování systému

Základní úroveň zabezpečení – firewall, antivirus



Obr. 01 Tři hlavní úrovně bezpečnostní architektury [10, s. 35]

2.3 Metody ověřování identity uživatele

Pro přístup do systému je potřeba ověřit identitu uživatele, stejně je tomu i v případě informačních systémů veřejné správy. To se provádí několika základními způsoby – autentizací nebo identifikací uživatele. Při autentizaci předkládá uživatel tvrzení o své identitě, tu následně systém ověřuje. Oproti tomu při identifikaci prochází systém databázi identifikačních záznamů, aby našel shodu.[7, s. 11]

2.4 Autorizace

Informační systém umožňuje v rámci autorizačního procesu přidělení práv pro přístup jednotlivým uživatelům. V každém informačním systému má každý uživatel specifická přístupová práva omezená buď jen do určité části, nebo jen na určité úkony. Většinou se to liší podle pracovní náplně. Přístupová práva přidělují síťový administrátoři a pracovníci servisu pro uživatele, na které se uživatel při zřizování přístupu do systému musí obrátit. Každý uživatel má právo se obrátit na servis v případě problému.

2.5 Bezpečné heslo jako základ autentizace

Autentizace do informačního systému nebo do jiného druhu systému je proces, při kterém uživatel dokazuje, že je tím, kým je. Existuje několik způsobů. Prvním a nejčastěji využívaným je autentizace na základě znalostí. Uživatel potvrzuje svoji identitu na základě znalosti (nejčastěji jméno, heslo). [7, s. 32]

Druhým způsobem, často využívaným třeba v bankovním sektoru, je autentizace na základě vlastnictví. Aby byl proces úspěšný, je potřeba mít identifikační kartu nebo token. [7, s. 35]

Třetím způsobem je autentizace na základě určitých vlastností (biometrika). Uživatel se přihlašuje do systému například otiskem prstů, sítnice nebo jiné vlastnosti, která jej identifikuje. [7, s. 38]

V neposlední řadě existuje víceúrovňová autentizace, kdy se dohromady kombinuje více metod. Tento postup se využívá hlavně v místech, kde je vysoký stupeň zabezpečení informací a omezený počet přístupů. [7, s. 42]

Při procesu autentizace na základě znalostí se nejčastěji zadává přihlašovací jméno a heslo. Uživatelé si běžně volí taková hesla, aby byli schopni si je lehce zapamatovat. Někdo dává přednost svému příjmení, jménu svého mazlíčka, maminky za svobodna či svému

oblíbenému filmu nebo kapele. Tohle všechno je samo o sobě neúčinné, protože v případě, kdy se do systému snaží dostat někdo, kdo uživatele zná, stačí mu k tomu jen několik málo minut a úspěch je zaručen. Někdy jsou tato hesla pro zlepšení ochrany doplněna o kombinaci čísel. I zde uživatelé vycházejí z toho, co znají. Velmi často se používá rok narození, datum svatby, výročí nebo rok narození dětí.

Opravdu bezpečné heslo musí být silné. To znamená, že není možné jej v přijatelném čase prolomit a dostat se do systému. Každé takové heslo by mělo být delší než 8 znaků, sestávat se z kombinace čísel a písmen, která ovšem nesmí tvořit smysluplné slovo. A co je nejdůležitější, heslo by nemělo být odvozeno od ničeho, co je s daným uživatelem jakkoliv spojeno. Když si není uživatel jistý, zda je jeho heslo bezpečné, existují nástroje, které umožňují jeho prověření. Něco podobného umisťuje spousta webových služeb přímo do registrace. Uživatel po zadání zvoleného hesla vidí, zda je či není bezpečné. V případě, že není, je vyzván k jeho změně, jinak není možné registraci dokončit. Svá hesla a další přístupové údaje by si za žádnou cenu neměli uživatelé nechávat zapsaná na viditelných místech. Třeba heslo pro přístup do bankovního systému či pin nesmí být položeno hned vedle platební karty. Další rady a doporučení pro uživatele z hlediska bezpečnosti naleznete na konci tohoto dokumentu.[7 s. 29-42]

3. Lidský faktor při ochraně osobních údajů

Kromě legislativního vymezení a technického zabezpečení je důležitou součástí systému ochrany osobních údajů uživatel, a to jak v roli správce informací, tak v roli subjektu údajů. Svoji roli zde sehrává mnoho faktorů, od tvorby vhodného hesla, přes udělení nevhodného přístupu k informacím v rámci informačního systému (obojí bylo již probráno), až k lidské neopatrnosti a touze pomáhat ostatním. Toho využívá zejména sociální inženýrství.

3.1 Sociální inženýrství

Sociální inženýrství je činnost, kdy sociotechnik manipuluje s lidmi za účelem provedení určité činnosti, nebo k získání důležité informace s využitím informačních a komunikačních technologií. Cílem každého klamu je vytvořit v dotyčném pocit, že situace je jiná, než ve skutečnosti je. Sociotechnici rádi využívají na první pohled bezvýznamných informací ke vzbuzení důvěry. Na základě získané důvěry se pokoušejí dostat k informaci, která je jiným způsobem nepřístupná, chráněná nebo dokonce tajná. V případě veřejné správy se může

jednat o cokoliv od rodného čísla, adresy, přes sociální zabezpečení, obor pracovní činnosti až po platební schopnost.

Prostředků, které může sociotechnik využít je mnoho. Nejjednodušší je použití telefonu k uskutečnění hovoru. V něm se dotyčný představí, třeba jako osoba, o které hledá informace a pak za pomoci jednoduché manipulace a dobře volených slov získá, co potřeboval vědět. Dnes se nejčastěji setkáváme s tzv. phishingovými útoky, kdy jsou pomocí e-mailů rozesílány podvrhy e-mailů či webových stránek. Takto podvržené stránky stačí jen otevřít a už může být počítač infikován zákeřným kódem, díky kterému je sociotechnik schopen získat potřebné informace, či jinak naložit s počítačem oběti. V případě podvrženého webu je uživatel vyzván k zadání třeba přihlašovacích údajů, ty jsou pak pochopitelně ihned odeslány zpět sociotechnikovi. Díky takto získaným údajům může být poškozena jakákoliv osoba, a to například, tak, že přijde o své finanční prostředky.

3.2 Rady a doporučení pro ochranu osobních údajů

- Používat silná hesla, která mají více jak 8 znaků a jsou tvořena kombinací písmen a čísel.
- Heslo a pin si nezapisovat k platební kartě, kterou používáte.
- Důležitá hesla je doporučeno měnit každých 90 dní.
- Nesdělovat důležitá hesla nikomu z rodiny, přátel, nebo kamarádů.
- Dávat si pozor na to, komu sdělujeme své osobní údaje. Při jednání s kýmkoliv po telefonu nesdělovat své osobní údaje. Jen pokud máme stoprocentní jistotu.
- Při používání veřejného internetu nebo veřejných počítačů, například v knihovně neukládat historii procházení, používat anonymní mód.
- Při používání veřejných počítačů neukládat v prohlížeči své přihlašovací údaje.
- V rámci firemního zabezpečení používat jasně stanovená pravidla.
- Při ztrátě identifikačních dokladů ihned nahlásit Policii ČR, aby nedošlo k jejich zneužití.
- Při telefonním kontaktu s neznámou osobou nesdělovat žádné osobní údaje.

Závěr

Ochrana osobních údajů je velmi složitá problematika, na kterou by si měl každý dát pozor v zájmu zachování vlastní bezpečnosti. Ve veřejné správě je to o to závažnější, že jsou v jejích informačních systémech uloženy údaje občanů České republiky a v době, kdy se vše sjednocuje, aby bylo vyhledávání jednodušší, je potřeba dbát na bezpečnost. Zpracovávat a nakládat s osobními údaji je možné pouze v souladu se zákonem. V případě jeho porušení jsou Úřadem pro ochranu osobních údajů udělovány sankce. Každý člověk by si měl dávat pozor na to co, komu a kdy sděluje. Nejdůležitější ze všech údajů je rodné číslo, které bude ale možná v budoucnu nahrazeno bezpečnějším systémem údajů, které se nedají tak jednoduše zneužít. Celkově vzato je to problém, který se dotýká každého občana a při jeho řešení je zapotřebí brát v úvahu legislativní, hardwarovou a uživatelskou stránku.

Použitá literatura

1. Česká republika. 40/2009 Sb., Trestní zákoník:In: 2009. Dostupné z: http://portal.gov.cz/app/zakony/zakonStruct.jsp?idBiblio=68040&nr=40~2F2009&rpp=15#local-content

2. Česká republika. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. In: 2002. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20

3. Česká republika. Zákon číslo 133/2000 Sb. O evidenci obyvatel a rodných čísel. In: 2000. Dostupné z: http://portal.gov.cz/app/zakony/zakonStruct.jsp?idBiblio=49303&nr=133~2F2000&rpp=15#local-content

4. Česká republika. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: 2000. Dostupné z: http://www.pristupnost.cz/zakon-365-2000-sb-o-informacnich-systemech-verejne-spravy/

5. HENDRYCH, Dušan. *Správní právo: obecná část*. 8. vyd. Praha: C.H. Beck, 2012, xxxiv, 792 s. Právnické učebnice (C.H. Beck). ISBN 978-807-1792-543.

6. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

7. MATYÁŠ, Vašek; KRHOVJÁK, Jan. Autentizace uživatelů a autorizace elektronických transakcí : příručka managera. Praha : Tate International, 2007. 318 s. ISBN 9788086813141.

8. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Informační systém o informačních systémech veřejné správy* [online]. 2007 [cit. 2012-11-06]. Dostupné z: http://www.sluzby-isvs.cz/ISoISVS/Applets/DefaultSSL.aspx

9. MITNICK, Kevin. *Umění klamu*. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.

10. NYÍRI, Ladislav. Ochrana osobních údajů v informačních systémech. *Parlamentní magazín*. 2011, č. 10. ISSN 1804-9729. Dostupné z: http://issuu.com/parmag/docs/pm102011?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true

11. ŠMÍD, Vladimír. *Ochrana osobních údajů a informační systémy: dva roky v nových podmínkách* [online]. 2011 [cit. 2012-11-01]. Dostupné z: http://www.fi.muni.cz/~smid/ts02od.html

12. Ochrana osobních údajů. *BusinessInfo* [online]. 2011 [cit. 2012-11-01]. Dostupné z: http://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-opu-4637.html

13. Ochrana osobních údajů. *Povinnosti správce osobních údajů* [online]. 2011 [cit. 2012-11-01]. Dostupné z: http://www.oou.cz/index.php?file=osobni_udaje_povinnosti_spravce

14. Portál veřejné správy České republiky [online]. 2011 [cit. 2011-04-21]. Úvodní stránka. Dostupné z WWW: http://portal.gov.cz/wps/portal/_s.155/6966/place.

15. Právní předpisy vztahující se k ochraně osobních údajů. *Ochrana osobních údajů* [online]. 2011 [cit. 2012-11-05]. Dostupné z: http://www.oou.cz/index.php?file=personal_data_protection_law

16. Úřad pro ochranu osobních údajů. *Úřad* [online]. 2012 [cit. 2012-11-01]. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=13

17. Úřad pro ochranu osobních údajů. *O projektu IS ORG* [online]. 2012 [cit. 2012-11-01]. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=884&submenu=885&loc=886

18. Úřad pro ochranu osobních údajů. *Zákon o ochraně osobních údajů* [online]. 2012 [cit. 2012-11-01]. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5