úřad
pro ochranu
osobních
údajů

informační bulletin
2/ 2005

1. TADY A TEĎ

Vážené čtenářky, vážení čtenáři,
dne 1. 6. 2005 uplynulo pět let od vzniku Úřadu pro ochranu osobních údajů. Rád bych při této příležitosti oslovil Vás všechny, kdo jste prostřednictvím Informačního bulletinu sledovali práci instituce, v jejímž čele stojím od září roku 2000, a vyslovil naději, že bulletin Úřadu pro Vás byl užitečným průvodcem při poznávání faktu, že ochrana osobních údajů v současném světě je důležitou součástí demokratické společnosti.

Po celé toto období Úřad plnil své povinnosti dozorové instituce, která se zabývala jak jednotlivými kontrolami vycházejícími z konkrétních podnětů Vás občanů, tak plánovitě prováděla kontroly v různých oborech a oblastech, kde by mohlo dojít ať už k vědomému, nebo nevědomému porušení zákona o ochraně osobních údajů, a tedy k zásahu do soukromého a rodinného života jednotlivců.

Za celé období pěti let Úřad o své činnosti soustavně informoval veřejnost, především prostřednictvím 24 pravidelných tiskových konferencí. V souladu s povinností, kterou mu ukládá zákon o ochraně osobních údajů, zveřejňoval také každoročně svou výroční zprávu, která je za všechna tato léta trvale přístupná na webových stránkách Úřadu na adrese www.uoou.cz. Za dobu svého působení Úřad vydal rovněž 37 částek Věstníku s oficiálními dokumenty závažnými pro jeho práci ve prospěch občanů, 15 čísel Informačního bulletinu pro širokou veřejnost, vybudoval oborovou knihovnu, z jejíchž zdrojů za poslední dva roky čerpali studenti zabývající se ochranou osobních údajů pro desítku diplomových prací; rozsáhlé webové stránky nabízejí veřejnosti soustavně doplňované a aktualizované informace o ochraně osobních údajů. Tisíce zodpovězených dotazů (jak je patrné z jednotlivých výročních zpráv) a stovky konzultací a přednášek jsou součástí naší každodenní práce. Pracovníci Úřadu vydali také šest ceněných odborných publikací.

S vědomím, že jen dobře informovaný občan dokáže s odpovídajícím sebevědomím hájit své právo na soukromí, jsme v loňském roce vydali informační leták a zahájili rozsáhle projektovanou informační kampaň pro širokou veřejnost.

V souladu s požadavky plynoucími z členství našeho státu v Evropské unii Úřad připravil a předložil novelu zákona o ochraně osobních údajů, která posílila harmonizaci zákona o ochraně osobních údajů s právem evropským a rozvíjel (a rozvíjí) svou dozorovou a rozhodovací činnost, včetně vytváření právně přípustných kroků maximálního poskytování informací veřejnosti. Nové legislativní kroky přinesly Úřadu i nové kompetence (především v souvislosti se zákonem o některých službách informační společnosti a zákonem o elektronických komunikacích). Zároveň však i názory Úřadu ovlivňovaly tvorbu nové legislativy

(zejména poté, co se Úřad stal v rámci legislativního procesu povinným připomínkovým místem); principy ochrany osobních údajů jsou vkládány do nejrůznějších právních předpisů, takže náš právní řád se postupně, z pohledu ochrany soukromí a osobních údajů, harmonizuje s právem EU.

Pracovní a odborná spolupráce a aktivity na mezinárodní úrovni znamenaly pro Úřad nejen významné pozice, které byly jeho pracovníkům svěřeny v evropských expertních orgánech – např. v Radě Evropy, Evropské komisi, společných dozorových orgánech EU (EUROPOLu, Schengenu), ale vyústily rovněž v pověření českého Úřadu, aby v rámci projektu EU/CARDS pomáhal Bosně a Hercegovině harmonizovat zákon o ochraně osobních údajů s evropským právem a napomohl organizačně vybudovat dozorovou instituci pro ochranu osobních údajů (po dobu 14 měsíců bude jako vedoucí tohoto projektu působit v Sarajevu odborník z českého Úřadu). Úřad se tak stal první českou institucí, které Evropská komise svěřila prostředky určené pro zlepšení ochrany dat v nečlenském státě EU (viz také následující článek).

Uvedené mezinárodní uznání profesionálních kvalit práce Úřadu je samozřejmě zavazující. A to nejenom směrem k zahraničním aktivitám, ale v plné míře i vůči občanům České republiky. Pevně věřím, že Úřad si i v budoucnu udrží důvěru občanů svou službou jejich oprávněným zájmům a očekáváním v ochraně soukromí, které jim zaručuje Listina základních práv a svobod. Doufám, že nadále tomuto poslání bude sloužit také Informační bulletin Úřadu a upřímně si přeji, aby Vám i nadále byl přístupným průvodcem i důvěryhodným referenčním periodikem, které přináší poznání o ochraně osobních údajů – tomto klíči k soukromému životu každého z nás.

RNDr. Karel Neuwirt,
předseda Úřadu pro ochranu osobních údajů

Úřad pro ochranu osobních údajů poskytne pomoc partnerům v Bosně a Hercegovině

Úřad pro ochranu osobních údajů se zúčastnil výběrového řízení na udělení projektu „Podpora Komisi ochrany dat Bosny a Hercegoviny". Toto řízení bylo vypsáno v rámci programu CARDS, což je program Evropské unie na podporu stabilizace zemí západního Balkánu.

Úřad se řízení účastnil jako tzv. starší partner, tedy jako primárně odpovědná instituce, a to spolu s partnerským španělským úřadem (Agencia Espaňola de Protección de Datos) v roli tzv. mladšího partnera, tedy instituce odpovědné za vybrané akce v rámci projektu.

Ve výběrovém řízení byl Úřad úspěšný a stal se tak první institucí České republiky, která bude v zastoupení Evropské unie poskytovat pomoc jiným státům.

Cílem projektu je zlepšit situaci Bosny a Hercegoviny v oblasti ochrany osobních údajů s perspektivou budoucího zapojení tohoto státu do Evropské unie.

Projekt má tři hlavní části:

1. Úprava právního prostředí v oblasti ochrany osobních údajů. Hlavním cílem této oblasti bude revize stávajícího zákona na ochranu osobních údajů a příprava novely, která má zákon uvést do souladu s legislativou Evropské unie.

2. Funkce Komise ochrany dat. Český Úřad má rovněž napomáhat při vytváření modelu nezávislého úřadu na ochranu osobních údajů, který bude schopen plnit úkoly v souladu se standardy EU. V této souvislosti se předpokládá také školení zaměstnanců hostitelského úřadu.

3. Popularizační kampaň. Smyslem popularizace bude zvýšit povědomí veřejnosti o problematice ochrany osobních údajů. Kampaň by měla být provázena osvětovou činností jako jsou přednášky, dny otevřených dveří a vydávání informačních publikací.

V současné době se smlouva Úřadu s Evropskou komisí o provedení projektu připravuje k podpisu a začátkem podzimu by měl být projekt zahájen. Úřad tedy čeká odpovědná, možná i složitá mise. Na druhé straně je zřejmé, že se tak práci Úřadu dostalo ocenění a důvěry ze strany EU.

úřad
pro ochranu
osobních
údajů

Setkání komisařů ochrany osobních údajů

Zámek Slovenské akademie věd ve Smolenicích přijal na konci května ve svých reprezentativních prostorách účastníky 7. konference komisařů ochrany osobních údajů ze střední a východní Evropy. Zástupci ČR, Polska, Maďarska, Slovenska, států Pobaltí, Bulharska, Chorvatska a Rumunska byli přijati s velkou pozorností ze strany hostitelů – slovenského Úradu na ochranu osobných údajov a za velké pozornosti slovenské vlády: Zahájení se zúčastnil vicepremiér Slovenské republiky pro evropskou integraci, lidská práva a minority pan Pál Csáky, který se ve svém proslovu věnoval ochraně osobních údajů v kontextu základních lidských práv, a jednání pozdravil a jeho prvního dne se zúčastnil také předseda Výboru pro lidská práva, národnosti a postavení žen Parlamentu Slovenské republiky pan László A. Nagy.

Pracovní náplní zasedání byla tradiční a vždy vzájemně inspirativní výměna informací o legislativních změnách v oblasti ochrany osobních údajů v jednotlivých státech. Velmi zajímavé je pochopitelně vystoupení představitelů států, které dosud nejsou členy Evropské unie. Zejména z jejich strany bývají oceňovány konzultativní rozhovory vedené detailně rovněž mimo hlavní jednání.

Tematicky se 7. setkání soustředilo na problematiku ochrany osobních údajů v oblasti statistiky, zdravotnictví a soudnictví a na jejich bezpečnost v informačních systémech. Zvláštní pozornost byla tentokrát věnována problematice zpracování biometrických údajů.

Deklarace, která byla slavnostně přijata na závěr jednání, zdůraznila mj. společnou vůli ke spolupráci při šíření znalosti práv na ochranu soukromí mezi občany jednotlivých států a podpořila záměr, který zazněl na půdě Rady Evropy: Prohlásit 28. leden 2006, den vyhlášení Úmluvy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat, za evropský Den ochrany osobních údajů.

Pravomocně rozhodnuté případy ve správním trestání 10. 3. 2005 – 10. 6. 2005

Deliktní jednání	Sankční opatření	Nápravná opatření
nepřijetí a neprovedení dostatečných opatření směřujících k zabezpečení osobních údajů zákazníků, v důsledku čehož došlo ke zpřístupnění osobních údajů celkem 1144 zákazníků, a to tím, že tyto údaje byly v podobě tabulky programu Excel odeslány, aniž by předtím byl tento soubor jakkoli zabezpečen, elektronickou poštou na nesprávnou adresu § 13 odst. 1	pokuta 55.000 Kč	ano
zpracování osobních údajů zájemců o zařazení do databáze vedené jako „komparsní rejstřík České republiky“, a to včetně citlivých osobních údajů, aniž by správce osobních údajů disponoval souhlasem subjektů údajů (v případě nezletilých osob souhlasem jejich zákonných zástupců), který by naplňoval všechny požadavky souhlasu se zpracováním citlivých osobních údajů § 9 písm. a)	pokuta 20.000 Kč	ano
zpracování osobních údajů v informačním systému evidence obyvatel podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), které spočívalo v uchovávání osobních údajů obyvatel, kteří neměli trvalý pobyt v příslušném správním obvodu, ve vlastní počítačové aplikaci evidence obyvatel, a zpracování osobních údajů, bez přijetí dostateč-	pokuta 15.000 Kč	ano

ných opatření, aby nemohlo dojít k neoprávněnému přístupu zaměstnanců ke zpracovávaným osobním údajům § 5 odst. 1 písm. e), § 13 odst. 1		
ztráta 147 písemností společnosti, jejíž písemnosti byly archivovány na základě mandátní smlouvy, obsahujících osobní údaje 240 osob kontaktovaných s nabídkou investovat prostřednictvím fondů, a to v rozsahu jméno, příjmení a rodné číslo, z toho ve 122 případech také adresa, bydliště a vlastnoruční podpis, v důsledku nepřijetí opatření při zabezpečení těchto údajů § 13 odst. 1	pokuta 40.000 Kč	ne
zveřejňování osobních údajů fyzických osob, účastníků správních řízení a řízení o přestupku, vedených v souvislosti s výkonem pravomoci České inspekce životního prostředí, na internetových stránkách § 5 odst. 1 písm. f)	pokuta 30.000 Kč	ano
použití osobních údajů v rozsahu jméno, příjmení, rodné číslo, adresa trvalého pobytu a číslo pasu pro založení devizového účtu bez souhlasu klienta § 5 odst. 2	pokuta 15.000 Kč	ne
nakládání se zdravotnickou dokumentací obsahující osobní údaje včetně citlivých údajů vypovídajících o zdravotním stavu, a to způsobem, který nezabezpečoval, že nedojde k neoprávněnému přístupu k těmto osobním údajům § 13 odst. 1	pokuta 3.000 Kč	ne
zpracování citlivých osobních údajů osob evidovaných v úředních záznamech Městské policie v M., vypovídajících o národnosti evidovaných osob, tj. údajů, které neodpovídají stanovenému účelu a v rozsahu nikoli nezbytném pro naplnění stanoveného účelu, bez souhlasu subjektů údajů § 5 odst. 1 písm. d), § 9 písm. a)	pokuta 30.000 Kč	ano

2. NEMĚLO BY VÁM UNIKNOUT

Úřad pro ochranu osobních údajů k cestovním dokladům s biometrickými údaji

Vláda předložila dne 29. 7. 2005 Poslanecké sněmovně návrh zákona, kterým se mění některé zákony na úseku cestovních dokladů, k němuž Úřad uplatnil řadu návrhů.

Jeho zásadní připomínky vyplývají ze zásad Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Úřad požaduje, aby v zákoně bylo jednoznačně stanoveno, jak se s citlivými údaji, mezi něž biometrické údaje patří, bude nakládat a jakým způsobem bude zabezpečena jejich ochrana.

Vzhledem k tomu, že nový cestovní pas (a další doklady) bude obsahovat RFID čip, v němž budou uloženy nejen psané údaje, ale také digitální fotografie a později i otisky prstů, Úřad upozornil na rizika zneužitelnosti osobních údajů. Z radiofrekvenčního čipu, jak bylo prokázáno, lze totiž pro-

střednictvím speciálních čtecích zařízení přečíst údaje i na dálku, a to bez vědomí majitele cestovního dokladu.

Úřad zastává názor, že z pohledu ochrany osobních údajů navrhovaná novela neřešila ani způsob zabezpečení biometrických údajů při výrobě, přenosu a uchovávání nosiče dat s těmito údaji, ani nakládání s doklady, které obsahují tento nosič dat.

S ohledem na uvedená fakta Úřad k novele zákona uplatnil následující zásadní připomínky:

- v zákoně je nutné výslovně ustanovit, že to budou pouze orgány státu, vůči kterým bude muset občan strpět povinnost ověření pravosti cestovního dokladu obsahujícího nosič dat s jeho biometrickými údaji tak, že budou porovnány biometrické údaje zapsané v čipu s biometrickými údaji aktuálně poskytnutými,
- kromě orgánů státu nikdo jiný nesmí mít technickou možnost čtení biometrických údajů z tohoto nosiče dat,
- je nezbytné zkrátit lhůtu pro likvidaci pořízených biometrických údajů a lhůtu pro zničení daktyloskopických otisků prstů.

Úřad chce svými připomínkami a postoji v rámci novelizace zákona o cestovních dokladech zabránit situaci, kdy by se nové cestovní doklady mohly stát dalším potenciálním nástrojem a prostředkem ke sledování občanů a narušování jejich soukromí. Úřad bude projednávání nového zákona v Parlamentu ČR dále sledovat.

Informace o situaci v zavádění biometrických pasů v zahraničí jsou k dispozici v rubrice Co nového v zahraničí na s.10-13.

Ochrana osobních údajů a šíření smrtelně nebezpečných chorob

V průběhu dubna letošního roku diagnostikovali lékaři u patnáctiletého chlapce, jednoho z žáků zvláštní školy v Rokycanech, otevřenou tuberkulózu. Případ vyvolal u místních obyvatel velké znepokojení a řadu oprávněných obav.

Začátkem května vyšly najevo další skutečnosti. Touto smrtelně nebezpečnou chorobou trpí i chlapcovi prarodiče a podezření na TBC vzniklo také u dalších osob. Bylo třeba okamžitě reagovat: Lékaři začali prověřovat všechny, kteří s těmito lidmi přišli do styku. Postižená lokalita prošla přísným protiepidemiologickým šetřením.

Tuberkulóza, která byla dříve potlačena díky dobře propracovanému systému prevence, se tedy s rozvojem turistiky a migrace obyvatelstva znovu objevuje i v ČR. Jedním z hlavních preventivních opatření proti TBC je očkování prováděné již u dětí.

Lékařka plicního oddělení rokycanské nemocnice uvedla, že závažné zdravotní problémy se objevují právě u jednotlivců, kteří se s preventivními opatřeními vůbec nesetkali. Řada romských dětí například unikla systému prevence stěhováním romských rodin do Velké Británie.

Představitel rokycanské diakonie (která s romskými dětmi ze sociálně slabších rodin dlouhodobě spolupracuje) rovněž klade důraz na dobře koordinovanou součinnost lékařů, sociálních kurátorů a škol.

A právě zde se dostáváme k jádru problému: Podle vyjádření uvedené lékařky (a podobný názor zastává i řada dalších lékařů) nezbytnou výměnu údajů znemožňuje ochrana osobních údajů. Zákon o ochraně osobních údajů prý komplikuje efektivní vyšetřování osob, jež přišly s nakaženým do styku, a výměna údajů mezi jednotlivými institucemi je těžkopádná a zdlouhavá.

Také v některých regionálních tištěných i elektronických médiích se následně začaly objevovat informace o tom, že nesmyslná, zákonem nařízená ochrana dat je jednou z hlavních příčin šíření tuberkulózy v ČR, neboť znemožňuje výměnu informací mezi institucemi.

Zákon o ochraně osobních údajů tak byl hrubě dezinterpretován. Je třeba zdůraznit, že tento zákon nejen nebrání v daném případě výměně informací mezi příslušnými institucemi, nýbrž dokonce s takovými situacemi počítá a respektuje zvláštní právní úpravy.

(Zvláštními zákony při výkonu správy v oblasti zdravotnictví jsou zejména zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, a zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.)

Prostudování příslušných zákonů vede k závěru, že ochrana osobních údajů pacientů neznemožňuje výměnu údajů mezi institucemi. Pouze určuje pravidla pro zacházení s těmito informacemi a odkazuje na zvláštní zákony, které stanoví pravomoc příslušných orgánů nakládat s citlivými údaji. V této souvislosti je užitečné prostudovat si rovněž materiál ***Úřad pro ochranu osobních údajů k problémům z praxe č. 1/2005: Sdělení Úřadu k informacím o šíření TBC.*** Tento materiál byl publikován ve Věstníku Úřadu č. 38 a je k dispozici rovněž na jeho webových stránkách, a to na adrese www.uoou.cz/stan_praxe_1_2005.php3.

Ti, kdo poskytují různé informace médiím, by tedy měli projevit (a to předtím, než napadnou zákon o ochraně osobních údajů) větší znalost právních předpisů, jimiž by se při výkonu své profese měli řídit.

Jaké je z pohledu zákona o ochraně osobních údajů postavení pojišťovacích agentů, obchodních zástupců, zprostředkovatelů a dalších osob zabývajících se obdobnou činností?

Výjimka z oznamovací povinnosti pro pojišťovací agenty, obchodní zástupce, zprostředkovatele a další obdobné činnosti

Úřad pro ochranu osobních údajů se v praxi setkává velmi často s případy podávání oznámení o zpracování osobních údajů podle § 16 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, osobami jako správcem ve smyslu § 4 písm. j) citovaného zákona, které však v tomto postavení nejsou.

Ujasněme si pojmy správce osobních údajů a zpracovatel osobních údajů. Správcem je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za ně. Zpracovatelem je subjekt, který zpracovává osobní údaje na základě smlouvy se správcem, tedy pouze v rozsahu a za podmínek, které stanovil správce. Z ustanovení zákona o ochraně osobních údajů po poslední novelizaci, provedené zákonem č. 439/2004 Sb. vyplývá, že oznamovací povinnost se vztahuje pouze na správce osobních údajů. Na zpracovatele se oznamovací povinnost nevztahuje.

V případě pojišťovacích zprostředkovatelů je třeba vycházet z toho, jak je zákonem č. 38/2004 Sb., o pojišťovacích zprostředkovatelích a samostatných likvidátorech pojistných událostí a o změně živnostenského zákona, v platném znění, definována činnost a postavení vázaného pojišťovacího zprostředkovatele, podřízeného pojišťovacího zprostředkovatele, pojišťovacího agenta, pojišťovacího makléře a samostatného likvidátora pojistných událostí, kteří se zapisují do registru vedeného Ministerstvem financí ČR.

Z dikce tohoto zákona vyplývá, že pojišťovací zprostředkovatel, pojišťovací agent a samostatný likvidátor pojistných událostí jsou vázáni smlouvou s pojišťovnou a jednají jejím jménem. Pokud tedy při své činnosti zpracovávají osobní údaje, jsou z hlediska zákona o ochraně osobních údajů v postavení zpracovatele, který oznamovací povinnost nemá.

Trochu odlišná situace je v případě pojišťovacího makléře a podřízeného pojišťovacího zprostředkovatele. Pojišťovací makléř je vázán smlouvou uzavřenou se zájemcem o pojištění, je tedy v postavení správce. Protože však provádí zpracování stanovené zvláštním předpisem, nemusí plnit oznamovací povinnost dle výjimky § 18 odst. 1 písm b) zákona o ochraně osobních údajů. V rámci zákonem předpokládaného zpracování je nicméně povinen dodržet ostatní ustanovení zákona o ochraně osobních údajů.

Podřízený pojišťovací zprostředkovatel může mít smlouvu uzavřenu buď s makléřem (v tom případě je zpracovatelem), nebo s agentem (v tom případě je jinou osobou, která zpracovává osobní údaje na základě smlouvy se zpracovatelem, ve smyslu § 14 a 15 zákona o ochraně osobních údajů). I v tomto případě se tedy ustanovení o oznamovací povinnosti na tento subjekt nevztahuje.

Závěr

Oznamovací povinnost podle § 16 zákona o ochraně osobních údajů se na subjekty v postavení pojišťovací zprostředkovatel, pojišťovací agent a samostatný likvidátor pojistných událostí podle zvláštního zákona nevztahuje, neboť jsou z hlediska zákona o ochraně osobních údajů v postavení zpracovatele, který oznamovací povinnost nemá.

V případě pojišťovacího makléře, který vystupuje v roli správce, tato povinnost obecně existuje, je však ve smyslu § 18 odst. 1 písm. b) zákona o ochraně osobních údajů liberována pro situace, kdy tento subjekt při své činnosti postupuje podle zvláštního zákona a rozsah zpracování osobních údajů odpovídá zvláštním zákonem stanovenému účelu.

Poznámka:
Úřad se k této problematice vyjadřuje ve Stanovisku č.1/2005, které je publikováno ve Věstníku Úřadu v částce 38. Plné znění stanoviska je také k dispozici na internetové adrese Úřadu v rubrice Stanoviska, www.uoou.cz/stan_stanoviska.php3. Bližší informace o aplikačním postupu jsou rovněž k dispozici na internetových stránkách Úřadu www.uoou.cz v rubrice Registrace.

3. TÉMA: Fishing, phishing, rhybaření…

(Není rybář jako rhybář)

Je léto. Vyznavači Petrova cechu se radují – rybářská sezóna je v plném proudu! Přejme všem rybářům dobrý lov a pohodu při rybaření.

Jsou však ještě jiní „rybáři", kteří z ticha vod nepřinášejí radost z úlovků sobě i druhým. Právě naopak! Sice také trpělivě sedí, ne u břehů řek či rybníků, ale u svých počítačů a „loví" v nekonečných vodách internetu. Ano, řeč je o „rhybaření", o phishingu. Phishing je nebezpečná technika podvodného „lovení", tj. získávání osobních údajů uživatelů sítě internet.

Existují dva výklady původu tohoto slova. Jedna verze vysvětluje vznik slova hovorovou úpravou anglického výrazu fishing – rybaření, kdy „f" bylo zaměněno za dvojici písmen „ph". Druhá verze nabízí variantu zkratky: Password Harvesting Fishing – sběr hesel rybařením.

Rozmach internetu rozvinul i nejrůznější metody jeho zneužití. Internet nabízí velké množství služeb. Právě tyto služby mohou hrát roli jakéhosi prostředníka při útoku počítačových virů nebo ataků individuálních útočníků. Elektronická pošta je jednou z nich. Phishingem lze nazvat podvodné e-maily, kdy na velké množství e-mailových adres jsou rozesílány podvodné dopisy, které ovšem na první pohled vypadají velice věrohodně. Uživatelům je rozeslán například e-mail, že vyhráli vysokou cenu v mezinárodní loterii nebo prosba o pomoc při převodu obrovské částky peněz s nabídkou provize. Naivním příjemcům těchto zpráv, kteří se nechají nachytat, jsou pak předkládány falešné doklady i podvodné odkazy na finanční instituce.

Princip tohoto počítačového podvodu spočívá v tom, že oběti podvodných e-mailů jsou lákány na peníze, dochází k apelu na jejich svědomí a city, nebo jsou přiváděny do vypjatých situací. Je potřeba vždy zpozornět v případě, že objevíme e-mail s požadavkem potvrdit své jméno, adresu, aktualizovat číslo bankovního účtu, přístupový kód v bance, či údaje z platební karty s důrazným upozorněním, že v případě, že tak neučiníme nás může postihnout veliká finanční újma a podobně. V těchto zkratových situacích, kdy vše vypadá velice věrohodně, mnozí lidé jednají ukvapeně a své osobní údaje prozradí.

Odesilatel podvodného e-mailu se snaží, aby jeho požadavek byl urgentní, aby příjemce zprávy znejistěl, moc nepřemýšlel a hlavně rychle konal. Cílem je získat osobní údajů uživatele internetu. Ukvapenou a neopatrnou navigací po internetu, s následkem prozrazení našich osobních údajů, tak můžeme přijít nejen o peníze v bance, ale někdy může dojít i k odcizení identity.

Obdobné praktiky existovaly již v minulosti. I dříve byly běžnou poštou a později faxem podvodné dopisy rozesílány. Lze říci, že phishing je nový trend v podvodných dopisech.

Změna spočívá v tom, že internet nabízí rychlé rozšíření zpráv k mnoha adresátům najednou, a tak umocňuje množství „úlovků", které se podvodníkům podaří nachytat. Úspěšnost „rhybářů" je

znepokojivě vysoká – na udičku jim skočí přibližně pět procent z oslovených adresátů. Technologie „rhybaření" se neustále zdokonaluje a profit útočníků roste. Hackeři čekají na sebemenší chybu uživatele sítě, ale využívají i mezery a chyby operačního systému.

V poslední době se rozšiřují podvodné e-maily od smyšlených bank a dochází tak k nárůstu zneužívání osobních údajů občanů. Scénář je vždy obdobný – uživatelé sítě obdrží e-mailovou zprávu s odkazy, které vypadají na první pohled jako stránky jejich banky. Jsou požádáni o potvrzení či aktualizaci osobních a bankovních údajů. Tyto informace jsou následně zneužívány k provádění finančních operací jménem podvedených zákazníků.

Klíčovým nástrojem na ochranu před phishingem je zdravý lidský rozum a dodržování základních pravidel bezpečného chování při práci na internetu.

Dokonalá softwarová ochrana zatím neexistuje. Útočníci stále více spoléhají na neopatrnost a zvědavost uživatelů. Důležité je neklikat ukvapeně na každou e-mailovou zprávu, neotvírat e-maily s neznámou přílohou. Nejlepší a nejbezpečnější prevence před zneužitím osobních údajů je správné nakládání s nimi – v případě e-mailové adresy to například znamená pečlivě si rozmyslet, komu svou adresu dáme a komu budeme cestou e-mailu odpovídat.

Tak jako reálný svět má i internet své konvence a stanovená společenská pravidla. Každý uživatel počítačové sítě by si měl uvědomit svou odpovědnost v přístupu k širokému spektru nabídky služeb internetu a ke všem jejím uživatelům. Trochu zvláštní slůvko „netiketa" vzniklé spojením slov net a etiquette vysvětluje etiketu při používání počítačové sítě.

DESATERO PŘIKÁZÁNÍ POČÍTAČOVÉ ETIKY
(převzato z The Computer Ethics Institute)

Nepoužiješ počítače ke škodě jiného.
Nebudeš ničivě zasahovat do práce druhých lidí.
Nebudeš slídit v souborech jiných lidí.
Nepoužiješ počítače ke krádeži.
Nepoužiješ počítače pro křivé svědectví.
Nepoužiješ nebo nepořídíš kopii softwaru, který jsi nezaplatil(a).
Nepoužiješ neoprávněně počítačového zdroje jiných lidí.
Nepřivlastníš si intelektuální dílo jiného.
Budeš přemýšlet o společenských následcích programu, který jsi stvořil(a).
Budeš používat počítače ohleduplně a s úctou.

Používání počítačové sítě je výsada, ne právo, a může být dočasně zrušena kdykoliv z důvodu nevhodného chování v síti. Toto chování může zahrnovat např. umístění nezákonných informací v systému, používání hanlivých nebo jinak nežádoucích výrazů ve veřejných nebo soukromých zprávách, rozesílání zpráv, které by pravděpodobně mohly vést ke škodám v příjemcově práci nebo ke škodám v systémech, zasílání řetězových dopisů nebo posílání zpráv skupinám či jednotlivcům a další způsoby používání sítě, které mohou způsobit zahlcení sítí nebo mají jiné negativní důsledky pro práci druhých.

Opakované zneužívání počítačové sítě může skončit i trestním řízením před soudem.

Převzato z volného překladu článku Uživatelův průvodce po síti a netiketa – originál textu je dostupný na ftp://ftp.lib.berkeley.edu/pub/net.training/FAU/netiquette.txt

V souvislosti s nárůstem podvodných útoků v síti internet lze hovořit o zločinu na internetu. „Phishing je zločin", prohlásil na setkání s novináři při své návštěvě Prahy letos v květnu pan David Perry, jeden z nejuznávanějších odborníků na počítačové viry a škodlivý kód. Svět vidí jako jednu velkou síť, která může sloužit k šíření zákeřných hrozeb.

Je potřeba si uvědomit, že kriminality s využíváním nových technologií bude v budoucnu ještě přibývat. Ocitli jsme se v éře tak zvaného kyberzločinu, tuto skutečnost je nutné vzít na vědomí a podle toho se chovat.

Závislost na internetu vzrůstá jak v našem osobním, tak i ve veřejném životě. Čím více databází instituce veřejného sektoru vytvářejí, tím větší je zájem o krádeže údajů z těchto databází, jejich zneužívání či prodej. Například obchod s e-mailovými adresami začal být pro různé skupiny velice zajímavý. Činnosti, které ještě v nedávné minulosti byly doménou pouze vandalů nebo jedinců, kteří tak činili pro potěšení, zábavu či pocit jakéhosi zadostiučinění, se nyní přesunují do rukou opravdových zločinců pro zisk.

Situace u nás

Zkušenost s nárůstem počítačové kriminality mají i české orgány činné v trestním řízení, jejichž příslušníci, popřípadě zaměstnanci, se denně setkávají s trestnými činy, při jejichž páchání zločinec zneužil počítač či internet. Jak se bránit? Především osobním přístupem k ochraně svého soukromí a osobních údajů, a to nejen při práci na počítači a při užívání sítě internet, ale vůbec v našem běžném životě. Pro otázky kriminality v počítačových technologiích a v síti internet musí ovšem existovat také kvalitní zákony. Internetoví operátoři například musejí po stanovenou dobu uchovávat data o tom, kdo a kam se z jejich klientů přihlásil.

Internetovou kriminalitou se však v současné době rovněž zabývá návrh novely trestního zákona, kterou se zavádí nový trestný čin „neoprávněný přístup k počítačovému sytému". Explicitně tento trestný čin není v právním řádu České republiky v současné době upraven. V návrhu nového trestního zákona, který je nyní v rámci legislativního procesu ve druhém čtení v Poslanecké sněmovně, je specifikována nová skutková podstata trestného činu porušování tajemství přenášených zpráv, a to včetně neveřejného přenosu (§157 odst. 1 písm. c) – viz Sněmovní tisk č. 744).

Informace ze zahraničí

■ Boj s počítačovou kriminalitou se neobejde bez mezinárodní spolupráce. Přehled aktivit EU v oblasti kybernetického zločinu je k dispozici na internetové adrese:
http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime

■ Významnou roli na poli mezinárodního boje proti kybernetickému zločinu zastává také APWG – Anti-Phishing Working Group. Tato oborová asociace, založená v roce 2004, sdružuje 800 jednotlivců z přibližně 490 firem z oblasti finančních služeb, poskytovatelů služeb a státních zákonodárných úřadů. Asociace se zaměřuje na zamezení krádežím identit a podvodům a snaží se vytvořit bezpečný a důvěryhodný prostor pro řešení problémů spojených s phishingem. Cílem aktivit této organizace je sdílení informací o phishingu, určení rozsahu tohoto problému a vytváření optimálních postupů pro zastavení a odstranění těchto nekalých aktivit. Zatím jsou nejvíce postiženy banky v anglicky mluvících zemích a také například služby typu PayPal a eBay. V rámci osvětové činnosti propaguje APWG jako nejúčinnější ochranu opatrnost a zdravý lidský rozum. Nabízí však i technická opatření, jak ohroženým institucím (blokování serverů, objednávka sledování webu a včasného zachycení podvodných stránek, sledování poštovních serverů), tak i uživatelům služeb. Těm nabízí využívání antispamových prostředků, ale především zdokonalování autentizačních metod.

■ Firma Harris Interactive je organizace zaměřená na průzkum a poradenství v oblasti virtuálního obchodování. Pro společnost Websence, Inc. uskutečnila výzkum se zaměřením na problematiku phishingu na pracovištích. Z výsledků průzkumu zpracovaných ve zprávě nazvané Phishing Trends Study vyplývá, že 67 % z dotazovaných zaměstnanců se s phishingem ještě nesetkalo, 4 % oslovených připustila, že se „nechala nachytat" a že při práci na počítači na pracovišti neprozřetelně klikla na phishingovou adresu. Rozdílně odpovídali vedoucí pracovníci z oblasti informačních technologií. 82 % z nich prohlásilo, že jejich zaměstnanci se stávají častým cílem phishingových útoků při používání e-mailů a URL a IM urgentních zpráv. Rozpor v odpovědích může být způsoben tím, že za-

městnanci jsou při práci s e-mailovými zprávami ve velmi obtížné situaci: Při otevření zprávy nepoznají zda e-mail, či zpráva IM je pravdivá, nebo zda se jedná o falešnou adresu. Tento názor potvrzuje i vyjádření 50 % dotazovaných IT vedoucích pracovníků, kteří jsou přesvědčeni, že jejich zaměstnanci opravdu nejsou schopni podvodný e-mail rozeznat.

Zdroj: http://www.onrec.com/content2

■ Filipínské vydání periodika Business World publikovalo letos v květnu rozhovor s antivirovým expertem, který působí jako marketingový specialista v jižní Asii. Ve phishingu vidí jeden z hlavních problémů bezpečného virtuálního obchodování. Míra nebezpečí je navýšena jednoduchou a neprůhlednou metodou realizace tohoto typu kyberpodvodu – jediným mylným poklepem na klávesnici lze ztratit opravdu mnoho. Varující jsou čísla útoků: Jestliže například v USA obdrželo 57 milionů lidí takový podvodný e-mail a 3 % z nich na něj odpovědělo, stalo se tak 1,8 milionů lidí rybičkou chycenou v síti internetových „rybářů". Přestože existuje antivirový software, nelze ani při jeho aplikaci spoléhat na dokonalou ochranu. Věci v oblasti IT jdou velice rychle – každých dvacet minut se na světě objeví nový počítačový virus. Uvedený expert zdůrazňuje nezbytnost osvětových kampaní v boji proti útokům hackerů jakéhokoliv typu. Uvádí, že např. vláda v Singapuru dvakrát za rok organizuje edukativní akce, na kterých jednoduchou formou vysvětluje zájemcům, co je to například spyware, trojský kůň, phishing a také doporučuje způsob ochrany. Přednášející se snaží lidem vysvětlit, že hodně záleží na jejich osobním přístupu a na tom, co vše sami mohou pro ochranu svých PC a tím všech svých údajů udělat. Upozorňují například na skutečnost, že i při používání bezdrátového spojení nejsou mimo nebezpečí. Pro názornost uvádí příklad: Sedíte třeba v letištní hale a poslední chvíle před odletem využíváte k práci na svém notebooku vybaveném pro bezdrátovou komunikaci. Pro hackera je celkem jednoduché do vašeho zařízení instalovat program typu „key loggers". Ten už pak jenom čeká na moment, kdy si začnete vyřizovat své finanční náležitosti cestou internetového bankovnictví a zadáte svůj PIN a číslo účtu. Tímto krokem, v případě, že nemáte zabudováno adekvátní softwarové zabezpečení, jsou vaše osobní údaje předány do nepovolaných rukou.

Volně zpracováno podle Business World, 17. 5. 2005

4. CO NOVÉHO V ZAHRANIČÍ

Spolkový komisař ochrany dat Schaar trvá na vysoké úrovni ochrany dat v biometrických pasech

U příležitosti prezentace biometrických pasů německým ministrem vnitra vydal Peter Schaar, spolkový komisař ochrany dat, následující prohlášení:

„Ustanovení právních předpisů EU k zavedení biometrických pasů mají být uplatněna nejpozději do poloviny roku 2006. Vyzývám německého ministra vnitra, aby využil této doby k dosažení nejvyšší možné úrovně ochrany dat a bezpečnosti u biometrických pasů. V této souvislosti má zásadní význam technický koncept bezpečnosti pro ochranu dat uložených v rádiových čipech. Přístup k takovému bezpečnostnímu konceptu mi dosud nebyl umožněn. Při vývoji tohoto konceptu nabízím svou spolupráci."

Konference spolkového a zemských komisařů ochrany dat přijala v této věci usnesení následujícího znění:

Usnesení Konference spolkového a zemských komisařů ochrany dat ze dne 1. června 2005 k zavedení biometrických prvků do průkazů totožnosti.

Ačkoliv nařízení č. 2252/2004 Evropské rady ze dne 13. prosince 2004 zavazuje členské státy, aby zahájily vydávání biometrických pasů občanům EU nejpozději do poloviny roku 2006, v Německu mají být první pasy vydány již v tomto roce.

Konference spolkového a zemských komisařů ochrany dat je toho názoru, že vydávání elektronicky snímatelných biometrických průkazů totožnosti by mělo začít teprve tehdy, až bude zaručena technická vyzrálost, ochrana dat a bezpečnost organizačního uspořádání chystané procedury. Tyto požadavky však zatím nejsou zabezpečeny na odpovídající úrovni.

Proto, ze všeho nejdříve, v zájmu ochrany práva na informační sebeurčení, musí být stanovena technická a organizační opatření v důkladném konceptu ochrany dat a bezpečnosti informační technologie. Dále je nezbytné, aby zákon o pasech obsahoval ustanovení k přesnému vymezení účelu použití dat.

Konference vítá podporu Evropského parlamentu, který obhajuje potřebu závazných minimálních požadavků na biometrické pasy s cílem předejít zneužití, zejména skrytému snímání nebo manipulaci s údaji. Konference však lituje, že pasy mají být zavedeny bez odpovídající předchozí diskuse o přínosech a rizicích této technologie. Za zvláště problematickou považuje skutečnost, že toto rozhodnutí učinila Evropská rada, složená z představitelů vlád, v rozporu s postojem Evropského parlamentu a národních zákonodárců z členských států EU.

Konference spolkového a zemských komisařů ochrany dat prohlašuje, že zavedení biometrických prvků nepovede automaticky k vyšší bezpečnosti. Některé postupy biometrické identifikace stále vykazují vysoký počet nesprávných identifikací a často se dají obelstít i těmi nejjednoduššími prostředky. Průkazy totožnosti, které se zdají být velmi bezpečné, se tak zavedením nespolehlivých biometrických postupů náhle stávají rizikovým faktorem. Kromě toho chyby v identifikaci mají vážné důsledky pro subjekty údajů, které jsou vystaveny velkému tlaku a dodatečným kontrolním opatřením v situaci, kdy jsou nuceny uvádět věc na pravou míru.

Konference spolkového a zemských komisařů ochrany dat proto požaduje objektivní zhodnocení biometrických postupů a přimlouvá se za zveřejnění výsledků příslušných výzkumů a pilotních projektů a za projednání těchto výsledků s vědci a s širokou veřejností. Elektronicky snímatelné biometrické průkazy totožnosti by neměly být vydávány dříve, než bude prostřednictvím právních, organizačních a technických opatření zabezpečeno, že

- biometrické prvky budou využívat výhradně úřady odpovědné za pasovou kontrolu,
- data uložená v průkazech totožnosti s biometrickými prvky nebudou používána jako referenční údaje za účelem kombinování dat z různých systémů a v různých souvislostech,
- zařízení používaná k výrobě a pro snímání budou certifikována nezávislým orgánem v souladu s mezinárodními standardy,
- používaná snímací zařízení budou v pravidelných intervalech ověřována ústředním orgánem,
- budou závazně určeny orgány pověřené vydáváním dokumentů nebo mající přístup pro účely verifikace,
- před zavedením biometrických průkazů totožnosti budou stanoveny postupy k prevenci zneužití dat při shromažďování referenčních údajů (bezpečný zápis), během dalších procedur a při používání karet,
- takto stanovené postupy budou vyhodnocovány nezávislým orgánem.

Navíc by mělo být zaručeno, že se nebudou vytvářet žádné centrální nebo v síti propojené biometrické databáze. Biometrické identifikační údaje mají být uloženy pouze v příslušném průkazu totožnosti. O to by se mělo usilovat cestou standardů na mezinárodní úrovni a stejně tak i prostřednictvím předpisů a dohod určujících, že údaje z průkazů totožnosti shromažďované při hraničních kontrolách mají být zpracovávány pouze v souladu s jednotným vysokým standardem ochrany dat a bezpečnosti informační technologie. Tento standard je nutno ještě stanovit.

Zdroj: Tisková zpráva (18/05)
Spolkový komisař ochrany dat
Bonn, 1. června 2005

Biometrický pas vytváří iluzi

Německé noviny Die Tageszeitung přinesly v dubnu tohoto roku rozhovor se spolkovým komisařem ochrany dat. Peter Schaar se v něm vyjadřuje k biometrickým pasům a ke snaze německé vlády o jejich zavedení ještě letos na podzim. A jelikož se biometrickým cestovním dokladům nevyhnou ani naši občané, považujeme za užitečné vybrat z výše uvedeného rozhovoru hlavní myšlenky.

Peter Schaar především hovoří o iluzi bezpečnosti, kterou cestovní pasy s biometrickými prvky (obraz obličeje a otisky prstů) vytvářejí. Problém budoucnosti podle něj nepředstavují padělané pasy, nýbrž pravé pasy s falešnou totožností. Novou, nepravou identitu si lze vytvořit podvodem, a v některých zemích dokonce velmi snadno – především tam, kde je vysoká korupce. Za úplatek tamní úřady vystaví biometrický cestovní doklad i na smyšlené jméno. Na dotaz novináře, zda jsou proti takovým praktikám biometrické prvky v pase neúčinné, Schaar odpověděl, že ano. Tyto prvky pomáhají pouze při prověřování, zda se pas shoduje s jeho držitelem. Ovšem pokud je už samotná totožnost majitele pasu falešná, pak takový doklad vytváří jen iluzi bezpečnosti.

Schaar se také domnívá, že zavedení biometrických pasů je ze strany státu převážně symbolickým krokem a snahou o demonstraci úsilí o větší ochranu proti terorismu. Navíc je tu i zájem policie, která prý ve využívání biometrických údajů v pasech spatřuje nové možnosti pro svá pátrání.

Ani přes tento kritický pohled se Schaar nestaví a priori proti zavedení biometrických pasů. Volá pouze po hlubším vyhodnocení rizik z hlediska ochrany osobních údajů a navrhuje přizvat do diskuse odbornou i laickou veřejnost. Hlavní problém vidí v možnosti vytvářet databáze s biometrickými údaji. Schaar požaduje, aby data byla uložena pouze na čipu v biometrickém pasu. Příslušné orgány by tak musely okamžitě po zhotovení pasu biometrické údaje likvidovat. Tím se zajistí, že tato data budou sloužit jen ke kontrole, zda pas a osoba patří k sobě.

Schaar dále v rozhovoru upozorňuje na bezpečnostní aspekty vyplývající ze skutečnosti, že biometrické údaje mají být v pasu ukládány na RFID čip. Existuje zde riziko tajného odečtení osobních dat v pase na dálku a jejich následného zneužití. Data proto podle Schaara musejí být chráněna šifrováním a v optimálním případě by měl ke každému pasu existovat individuální klíč.

Neméně sporným bodem je spolehlivost fungování čtecích zařízení na stanovištích pasové kontroly (např. na letištích). Současné systémy dokážou spolehlivě zjistit totožnost jen u 80 procent majitelů pasu. Ten, koho zařízení odmítne, bude muset podstoupit mnohem přísnější kontrolu úředníkem pasové kontroly.

Zbývá dodat, že v poslední době nabrala diskuse o zavedení biometrických pasů v Německu na intenzitě. Zejména vztahy mezi spolkovým komisařem ochrany dat a spolkovým ministrem vnitra jsou velmi napjaté, o čemž svědčí několik ministrových ostrých výpadů proti Schaarovi v německém tisku.

Zpracováno podle internetového vydání deníku Die Tageszeitung ze dne 19. 4. 2005
Internetový odkaz: www.taz.de

Dojde ke střetu mezi EU a USA kvůli biometrickým pasům?

Jak informoval Daily News na internetovém serveru EurActiv dne 26. dubna 2005, bruselský výzkumný tým Přátelé Evropy zorganizoval debatu zástupců EU a USA o anti-terorismu. Debata uskutečněná 25. 4. 2005 přes satelit především vynesla na světlo zásadní rozpory mezi EU a USA v oblasti biometrických pasů.

Spojené státy původně stanovily, že od října 2004 budou při vstupu do USA požadovat biometrické, strojově čitelné pasy od občanů těch členských států EU, které jsou v současné době vůči USA zproštěny vízové povinnosti. Kvůli technickým problémům Kongres tento termín sice odsunul až na říjen 2005, ale jelikož se zdá, že i tento nový termín může být splnitelný pouze pro 14 členských států, požádala Evropská komise o další prodloužení přípravné doby. Po posouzení této žádosti orgánem amerického parlamentu – Soudním podvýborem pro imigraci a bezpečnost hra-

nic (US House Judiciary Subcommittee on Immigration and Border Security) – se ukázalo, že ani samy Spojené státy nebudou do 26. října 2005 na toto připraveny a že zařízení schopná číst biometrické pasy ještě nebudou do uvedeného termínu k dispozici na všech celnicích, jak připustil mluvčí Odboru pro vnitřní bezpečnost.

Zajímavé je také to, že po USA se začlenění žádných biometrických prvků do amerických pasů nepožaduje. Z tohoto důvodu EU zvažuje zavedení vízového styku pro americké občany cestující do Evropy.

Richard Falkenrath (hlavní odborný asistent na Brookings Institution a bývalý náměstek amerického poradce pro vnitřní bezpečnost) se domnívá, že další oddálení data pro povinné zavedení biometrických prvků do evropských pasů je nevhodné a že splnění těchto požadavků je nezbytné pro ochranu USA před „pochybnými pasy" (lousy passports).

Ellen Tauscher (poslankyně amerického parlamentu) konstatovala, že tato záležitost je sporná obzvláště vzhledem k existujícím obavám z přistěhovalectví, které přiměly civilní stráž hlídkovat na americko-mexických hranicích. Domnívá se také, že někteří členové Kongresu možná chtějí „potrestat" státy EU za jejich postoj k problematice Iráku tím, že budou hlasovat proti oddálení výše zmíněného termínu.

Gijs de Vries (koordinátor Evropské unie pro antiterorismus) upozornil, že Spojené státy by měly zvážit následky, pokud odmítnou termín prodloužit. Uvedl, že tento problém může přinést veliké rozhořčení, což se nesmí dopustit.

Jonathan Faull (generální ředitel pro Spravedlnost, svobodu a bezpečnost EU) vyjádřil názor, že program Evropské unie pro biometrické pasy není řízen Amerikou. Unie pracuje podle svého vlastního časového rozvrhu pro uvedení biometrie do všech cestovních pasů, víz a povolení k pobytu a plnila by tento program, „i kdyby Spojené státy neexistovaly". Celkově vzato, technologie evropských pasů by měla být ještě vyspělejší než technologie americká. A J. Faull dodává: „Naše pasy nejsou o nic „pochybnější" než ty americké".

Podle novější zprávy z EurActiv ze dne 16. května 2005 skutečně dochází k určitému oddálení hrozby zavedení vízové povinnosti pro občany z EU, a to do 26. října 2006. K tomuto datu se také oddaluje požadavek na cestovní doklady vybavené biometrickými prvky v plném rozsahu, tj. včetně otisků prstů, případně obrazu rohovky. Pasy s digitální fotografií budou požadovány již od 26. října 2005.

Zdroj:
www.euractiv.com/Article?tcmuri=tcm:29-138583-16&type=News&_lang=EN&email=1528

Soud ve Francii rozhodl: Kontrola pracovní doby za použití otisků prstů je nepřiměřená

Nejvyšší soud v Paříži vydal dne 19. dubna 2005 rozhodnutí, kterým zakázal zavedení biometrické kontroly pracovní doby. Potvrdil tak nezbytnost dodržování principů účelu a přiměřenosti u biometrických systémů používaných pro kontrolu využívání pracovní doby.

Jedna francouzská společnost, která poskytuje různé zákaznické služby na vlakových nádražích (např. transport zavazadel, pomoc osobám se sníženou schopností pohybu), se rozhodla zavést biometrický systém využívající otisků prstů ke kontrole pracovní doby zaměstnanců. Firma toto opatření konzultovala s francouzským dozorovým orgánem pro ochranu dat (CNIL) a s podnikovou radou. S předstihem také informovala všechny své zaměstnance.

Soud shledal, že předem dohodnuté podmínky provozu byly dodrženy. Přesto však používání tohoto systému zakázal. Ve svém rozhodnutí se opírá o rozbory a doporučení CNIL. Soud považuje používání otisků prstů za oprávněné tam, kde jde o bezpečnost nebo ochranu činností vykonávaných pouze ve specifických prostorech. Ale nasazení takové technologie, která využívá lidského těla a ohrožuje tak svobodu jednotlivce, není odůvodnitelné v případech pouhé kontroly pracovní doby.

Toto rozhodnutí vychází z francouzského zákoníku práce, který v článku L.120-2 pojednává o principu proporcionality mezi kontrolou zaměstnance a sledovaným účelem, a dále z článku 6 evropské směrnice 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Volně přeloženo z francouzského originálu,
který je k dispozici na internetových stránkách
CNIL: www.cnil.fr

5. OSOBNÍ ÚDAJE V ŠIRŠÍCH SOUVISLOSTECH

Evropská cena za technologie pro informační společnost za čipovou kartu (Cena IST – Information Society Technology za rok 2005)

Švédská firma Cypak vyhrála jednu ze tří prestižních cen IST za rok 2005 za čipovou kartu, u které se zadává PIN na kartě, takže je chráněna proti zneužití při platbách přes internet.

Tato cena ve výši 200 tis. EUR pro každého z vítězů je udělována Euro-CASE (European Council of Applied Sciences, Technologies and Engineering) pod patronací a s finanční podporou Evropské komise.

Čipová karta má zabudovanou klávesnici, na které se zadává PIN, když je prováděna platba, při níž je karta vložena do čtečky připojené k počítači. Při tomto způsobu platby není třeba zadávat podrobné údaje týkající se karty. Při zadávání osobních údajů, údajů o kartě, PIN nebo hesla na klávesnici počítače lze totiž některými metodami příslušné údaje, PIN či heslo odhalit a následně zneužít. Při použití nové čipové karty zůstávají osobní údaje, PIN a bezpečnostní klíče bezpečně uloženy na čipové kartě.

Zdroj:
www.ist-prize.org/winners/detail.html?id=74_77&year=2005
www.euractiv.com/Article?tcmuri=tcm:29-138665-16&type=News

Návštěva Úřadu

Letos v květnu zavítal na Úřad PhDr Vlasti Broucek, významný australský expert v oblasti informačních systémů a technologií – český rodák, absolvent pardubického gymnázia a poté ČVUT v Praze. Dnes – doktor filozofie, správce počítačové sítě na katedře psychologie na Univerzitě v Tasmánii, programátor a školící pracovník ve svém oboru, ředitel pro vědu a programový vedoucí pracovník Evropského institutu pro počítačový antivirový výzkum (EICAR) na období 2004-2008 a …, určitě bychom našli další pokračování výčtu jeho odborných aktivit. Na svou alma mater vzpomíná rád a s vděčností především za kvalitní vzdělání, kterého se mu zde dostalo. Nadále udržuje osobní kontakt i spolupráci na poli pracovním. Bylo milé slyšet tato slova uznání.

Ačkoli ochrana osobních údajů není přímo jeho oborem, jeho specializace na souvislosti a události kolem technických nástrojů s touto problematikou, na kterou nahlíží z filozofického hlediska, úzce souvisí. Jeho současným zaměřením je především ochrana a bezpečnost počítačových infrastruktur, zejména otázky spojené s počítačovou kriminalitou a sociální problémy počítačových virů. Zajímá se rovněž o vyšetřování počítačové kriminality.

Při příležitosti své návštěvy v Praze se setkal s pracovníky ÚOOÚ. Půldenní prezentace jeho zkušeností a názorů mimo jiné ukázala, že je zastáncem nastolení pevných pravidel a mantinelů pro všechny, kdo užívají výhody počítačových sítí. Na své přednášce také zdůrazňoval nezbytnost výchovné činnosti a nutnost mezinárodní spolupráce v této oblasti.

6. Velký bratr dorazil do České republiky

28. října dojde v České republice poprvé k udílení cen pro Velkého bratra. Název ceny byl inspirován postavou ze slavného románu „1984" od britského spisovatele G. Orwella. Udílení cen by mělo proběhnout v pražském divadle Na zábradlí. Ceny pro Velkého bratra jsou každoročně udělovány v řadě zemí – poprvé to bylo ve Velké Británii, 28. října roku 1999.

V čem tato poněkud recesistická cena spočívá (nelze si v této souvislosti nevzpomenout např. na populární českou cenu Ropák roku)? Ruku v ruce s dynamickým rozmachem moderních (zejména počítačových, komunikačních a v poslední době též biometrických a RFID) technologií dochází na celém světě i k jejich závažnému zneužívání k nejrůznějším nekalým účelům. Zneužívání se dopouštějí nejenom soukromé společnosti, ale i státní instituce, přičemž příslušná legislativa je chronicky vždy o několik kroků zpět za rychlým vývojem událostí. Existuje řada firem a institucí, lačných po informacích o našich osobních údajích, vztazích, zvycích, finanční situaci apod. Mnohé z nich ani na chvíli neváhají využít tyto informace ve svůj, většinou hmotný, prospěch. Samozřejmě, že ani zpravodajská komunita v mnoha státech nezůstává v těchto aktivitách pozadu, i když často pod zcela počestnými záminkami (větší bezpečnost občanů, státu, boj proti terorismu...).

A tak se údaje o našem soukromí soustřeďují a vesele kupí v nejrůznějších databázích – legálních i těch protizákonných: Asi bychom se nestačili divit, kdybychom do nich měli možnost nahlédnout... Databáze lze navíc všelijak propojovat a křížit. Bleskové vytvoření velmi solidního profilu naší osobnosti a našeho sociálního či finančního statutu už dnes nepředstavuje žádný problém. I jednotlivé státy si mohou rychle vyměňovat osobní údaje občanů. A případů, kdy kupříkladu zkorumpovaný státní úředník bez zábran kupčí s osobními údaji jednotlivců, obsaženými v nedbale zabezpečených databankách, je ve světě také habaděj.

To vše přivedlo koncem devadesátých let skupinu lidí na pikantní nápad udílet zvláštní ceny těm největším hříšníkům na poli zneužívání základních principů ochrany osobních údajů a soukromí. Cenu fyzicky reprezentuje v hnědé barvě vytvořená skulptura ošklivé boty – křápu tlačícího na vodorovně položenou zmučenou lidskou hlavu.

Soutěží se hned v několika kategoriích:

- Dlouhodobé porušování lidského soukromí (pro soukromé firmy nebo státní instituce)
- Největší firemní slídil (pro komerční firmy)
- Největší úřední slídil (pro státní instituce)
- Nebezpečná nová technologie
- Právní norma Velkého bratra
- Slídil mezi národy
- Výrok Velkého bratra

Mezi nedobrovolnými laureáty se zhusta ocitají čelní představitelé managementu soukromých společností i vysocí státní úředníci, někdy i představitelé vládních kruhů.

Na tomto místě je třeba připomenout, že cena pro Velkého bratra má i svou kladnou složku: Je to ocenění za správně uplatňovanou ochranu soukromí.

Kandidáty na ocenění ve všech těchto kategoriích může navrhovat každý (internetová adresa navrhovacího formuláře na českém webu: www.bigbrotherawards.cz/index.php?p=4). Z navržených kandidátů vybere výherce porota složená z odborníků na nové technologie, právníků, ochránců lidských práv a novinářů.

A teď ještě jedna perlička na závěr:
21. dubna 2004 se mělo v USA konat 6. udílení cen Velkého bratra. Bohužel slavnostní ceremonie byla přerušena hned v počátku. Na pódium se dostavil muž, který se prezentoval jako zvláštní agent Liddy. Oznámil, že udílení cen Velkého bratra zakazuje, protože organizace Privacy International po-

úřad
pro ochranu
osobních
údajů

skytla materiální podporu teroristům tím, že v roce 2003 udělila cenu „Za dlouhodobé ohrožení" Usamu bin Ladinovi.

Zdá se nicméně, že policie nedomyslela přesnou formulaci zákazu. Zakázala udílet cenu Velkého bratra, ale zapomněla zakázat ceremonii jako takovou. Organizátoři zareagovali pohotově a všechny ceny na místě přejmenovali. :–) "Cena Za návrh nejvíce porušující naše soukromí se stala Cenou za nejokatější znásilnění práva, ocenění Firma nejvíce zneužívající právo na soukromí se změnilo na Cenu za zastření hranic mezi veřejným a soukromým sektorem a titul Nejhorší vládní úředník se změnil na cenu Za netečnost státního úředníka.

(Citováno z článku na serveru Privacy International, přeloženého V. Stworou a zveřejněného 31. 7. 2004 na serveru ZVĚDAVEC.CZ)

A zde je ještě několik internetových odkazů týkajících se ceny pro Velkého bratra:
www.bigbrotherawards.cz
www.privacy.org/pi/bigbrother
www.bigbrotherawards.org
http://nomines.bigbrotherawards.eu.org
http://nomines.bigbrotherawards.eu.org/index.php?gng=1

VYDÁVÁ ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
EDITOR: PHDR. HANA ŠTĚPÁNKOVÁ
REDAKTOR: MILENA NEJEDLÁ, BOHUMÍR LUKAJ
GRAFICKÁ ÚPRAVA: MILOSLAV ŽÁČEK
ADRESA REDAKCE: ÚOOÚ, PPLK. SOCHORA 27, PRAHA 7, 170 00
TELEFON: 234 665 286, FAX: 234 665 505
E – MAIL: INFO@UOOU.CZ
INTERNETOVÁ ADRESA: WWW.UOOU.CZ

PERIODIKUM JE ZAPSÁNO V EVIDENCI PERIODICKÉHO TISKU POD ČÍSLEM MK ČR E 10548

DÁNO DO TISKU 2. 8. 2005