zneužití identity a trestná činnost s tím spojená

PhDr. Miroslav SCHEINOST, JUDr.Zdeněk KARABEC,CSc.,
Institut pro kriminoloii a sociální prevenci, Praha

1. Úvodem

Technologický vývoj a nové způsoby komunikace s ním spojené podstatně ovlivnily většinu oblastí moderního života. Tradiční způsoby komunikace mezi lidmi a institucemi se mění, jsou doplňovány a zčásti i nahrazovány novými formami, umožněnými rozvojem elektronické komunikace, internetu, e-mailového spojení apod. Nelze považovat za překvapující, že na tyto nové možnosti komunikace reagují také pachatelé trestné činnosti, kteří je nejen využívají jako operativní a hůře zachytitelný způsob spojení, ale jejich prostřednictvím napadají a neoprávněně využívají, resp. zneužívají uložené nebo sdělované dokumenty, data, informace atd. V důsledku toho i trestné činy natolik klasické a tradiční, jako jsou krádež a podvod, mohou nabývat nových forem páchání. Jejich podstata se nemění, to, co je činí zvláštními, je *způsob, jakým jsou páchány*, tedy modus operandi.

Spáchání podvodu, při kterém se pachatel vydává za někoho jiného, není žádnou zbrusu novou formou kriminality. Zvláštním, resp. novým se stává, využívá-li moderních komunikačních struktur našeho současného světa, páchá-li se jejich prostřednictvím a odehrává se v jejich prostředí. Jsme stále více propojeni prostřednictvím komunikačních technologií, které slouží nejen ke sdělování informací v elektronické podobě, ale také k jejich vytváření a uchovávání. Masové rozšiřování informačních a komunikačních sítí umožňuje v podstatě v kterémkoli okamžiku propojení subjektů na globální i lokální úrovni. Britský kriminolog a specialista na ekonomickou a finanční kriminalitu prof.

Michael Levi v této souvislosti použil termín „glocal dimension".[1] V referenčním rámci této "glocal dimension" přestává fyzická vzdálenost hrát podstatnou roli. Kromě toho při přijímání elektronických informací, pokynů apod. není už obvykle potřebný hmatatelný doklad k ověření identity odesilatele.

Naše identita byla dříve potvrzována *listinnými dokumenty* – vandrovní knížkou, glejtem, rodným listem, cestovním pasem, občanským průkazem, řidičským průkazem, spořitelní knížkou a jinými průkazy a legitimacemi, jejichž součástí posléze často bylo i zobrazení podoby držitele.

Nyní, ve virtuálním světě počítačů, serverů, sítí, databází, elektronicky sdělovaných a sdílených informací nevystupujeme ani osobně, ani prostřednictvím fyzických dokladů, ale také „jen" virtuálně. Naše identita je vyjadřována a určována různými *kódy, PINy, hesly, passwordy,* které nám umožňují přístup k našim účtům, k naší poště, opravňují nás k nakládání s našimi či firemními prostředky, umožňují použití mobilního telefonu, vstup do databází k údajům, které v nich uchováváme atd.

Zatímco jsme dříve drželi své listinné identifikační doklady tak říkajíc v ruce a jejich ztrátu či zcizení jsme v relativně krátké době snadno zaznamenali, „žijí" nyní naše identifikační údaje ve virtuálním světě databází a sítí jaksi vedle nás a mimo nás. K jejich „ukradení" v tom smyslu, že by nám zcela zmizely, v podstatě nedochází (pokud nejsou nějakým zásahem zničeny, resp. vymazány; pak se ale obvykle nejedná o „krádež", ale o poškození nebo zničení), a proto jejich zneužití většinou zjišťujeme, až když shledáme, že jsme byli nějakým způsobem poškozeni my, nebo s použitím našich identifikačních údajů někdo jiný.

[1] LEVI, M.: Identity fraud: the „glocal" dimension. Referát na mezinárodní konferenci ISPAC, Courmayeur 30.11.-2.12.2007

Stále větší závislost společnosti na informačních a komunikačních systémech tak zvyšuje naši zranitelnost kriminalitou, zasahující tyto systémy.[2] Tzv. krádež a zneužití cizí identity proto nepředstavuje ve své podstatě nový jev, ale jev, který nabyl některých nových forem vázaných na moderní informační systémy, který se v současných podmínkách rychle šíří, působí značné škody a je předmětem intenzivní diskuse.

2. Aktivity orgánů OSN

Tímto jevem se na vrcholné úrovni zabývala v roce 2007 Komise OSN pro prevenci kriminality a trestní justici, která projednávala obsáhlou studii, zpracovanou skupinou expertů [3]. Dále byla tato problematika na pořadu jednání Ekonomické a sociální rady OSN (ECOSOC), která přijala rezoluci o krádeži identity ve vztahu k ekonomické kriminalitě. Jako hlavní téma se krádež a zneužití identity objevily na jednání ISPAC (International Scientific and Professional Advisory Council of the UN) v roce 2007.[4]

Jen pro ilustraci – v roce 2005 se v USA pohyboval odhad škod způsobených krádeží a zneužitím identity kolem 56 miliard USD; od roku 2004 je viktimizace touto formou kriminality sledována v USA v rámci tzv. National Crime Victimisation Survey, který je prováděn pravidelně dvakrát ročně na reprezentativním souboru 49 000 domácností. To představuje cca 100 000 osob, což dokládá význam, který se této formě kriminality v USA přikládá.[5]

Jaké je tedy vymezení tohoto jevu? Jedná se o získání cizí identity, resp. personálních dat jiné osoby bez jejího vědomí

---

[2] SEGER, A.: Cybercrime and identity theft: the challenges. Referát na mezinárodní konferenci ISPAC, Courmayeur 30. 11.-2. 12. 2007.

[3] International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. Results of the study on fraud and the criminal misuse and falsification of identity. RE/CN.15/2007/8.

[4] CHRYSSIKOS, D. - PASSAS, N. - Ram, C. D. (eds.): The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity. ISPAC, Milano 2008

[5] ŠTEFUNKOVÁ, M.: Victimisation Surveys. PhD. thesis, Bratislavská vysoká škola práva. Bratislava 2009 (zatím nepublikováno).

a souhlasu a jejich zneužití ke spáchání trestné činnosti. Michael Levi hovoří o tom, že nejde v pravém smyslu o krádež identity, protože poškozené osobě její identita samozřejmě zůstává, ale že jde spíše o duplikaci, resp. „klonování" identity; pachatel „zkopíruje" identitu a tuto zkopírovanou identitu použije.

V této souvislosti Levi rozlišuje tři fáze :

- získání dat charakterizujících jinou individuální nebo korporativní identitu;
- přeměnu těchto dat obvykle na finanční instrumenty;
- použití těchto instrumentů k nezákonnému obohacení.[6]

V průběhu tohoto kriminálního jednání lze odlišit dva cíle útoku – nejprve jde o poškození oběti, jejíž identita je neoprávněně získána a zneužita (identity theft); ve druhé fázi jde o další cíl útoku, který je napaden za pomoci zcizené identity (identity fraud). Tento další cíl útoku nemusí být totožný s tím, jehož identita byla zneužita, ale na druhou stranu může být původní oběť vícenásobně poškozena, tj. nejen zneužitím její identity, ale i následným finančním či jiným poškozením. Trestný čin je „dvoustupňový" – nejprve je neoprávněně získána cizí identita, pak je použita k jinému trestnému činu. Nejprve tedy musí být spáchána „krádež" identity, aby za pomoci této neoprávněně získané identity mohl být spáchán podvod. Pokud necháme stranou část této kriminality, kde může být cizí „elektronická" identita používána k získávání tajných informací (ekonomická a vojenská špionáž), je převážným cílem zneužívání elektronických dat majetkový prospěch, ale případně může sloužit např. také k praní špinavých peněz.

V zájmu přesnosti je třeba říci, že sice získání cizí identity je ve *většině případů zneužíváno ke spáchání ekonomické nebo majetkové kriminality,* tedy s cílem dosažení

[6] Viz pozn.č.1

hmotného prospěchu, ale není to účel výhradní. Tady lze nalézt určitý rozdíl mezi zneužitím elektronických dat a listinných dokumentů. Listinné dokumenty, zejména pasy, jejichž význam pro identifikaci osoby neklesá a zachovávají hmotnou podobu, i když obsahují stále více elektronicky čitelných údajů, jsou nadále velmi žádané. Zatímco krádež a zneužití „elektronické identity" prvořadě slouží k dosažení neoprávněného majetkového prospěchu formou podvodu, zneužití listinných dokumentů slouží do značné míry i jiným účelům. Jsou-li zneužity listinné dokumenty sloužící k prokázání *identity „face-to-face"*, jako pasy, řidičské průkazy atd., jsou obvykle získány krádeží, upraveny a slouží buď ke krytí nelegálního pohybu osob (migrantů, teroristů apod.), nebo ke skrytí vlastní identity za účelem vyhýbání se vyhoštění, dohledu, trestnímu stíhání, k prevenci odhalení apod. Mohou ale samozřejmě sloužit i k majetkové kriminalitě (získání půjčky, úvěru, objednání zboží na přivlastněné jméno atd.).

Podle britského výzkumu, kdy byla v roce 2007 provedena studie o pachatelích 517 případů podvodu s pomocí zcizené identity a jejich motivaci, bylo zjištěno, že ve 45 % případů bylo motivem získání půjčky a získání hotovosti; v dalších případech šlo o získání zaměstnání, skrytí dluhu, získání nové identity.[7]

Pokud jde o data, sloužící k *elektronické identifikaci* (kreditní a platební karty, PIN, čísla účtů, přístupová hesla atd.), probíhá jejich získání nejčastěji prostřednictvím zneužití informačních technologií. Děje se tak například tzv. skimmingem (zkopírováním údajů z platební karty nebo jiného média bez vědomí jejího držitele), krádeží přes neoprávněné vniknutí do počítače, resp. databáze (hackerství, sledování mailové pošty...) apod. Jinou formou je získání údajů z databází nebo celých databází za úplatek. Jako technika

[7] MCNULTY, K.: Identity related crime and economic fraud. Referát na mezinárodní konferenci ISPAC, Courmayeur 30.11.-2.12.2007

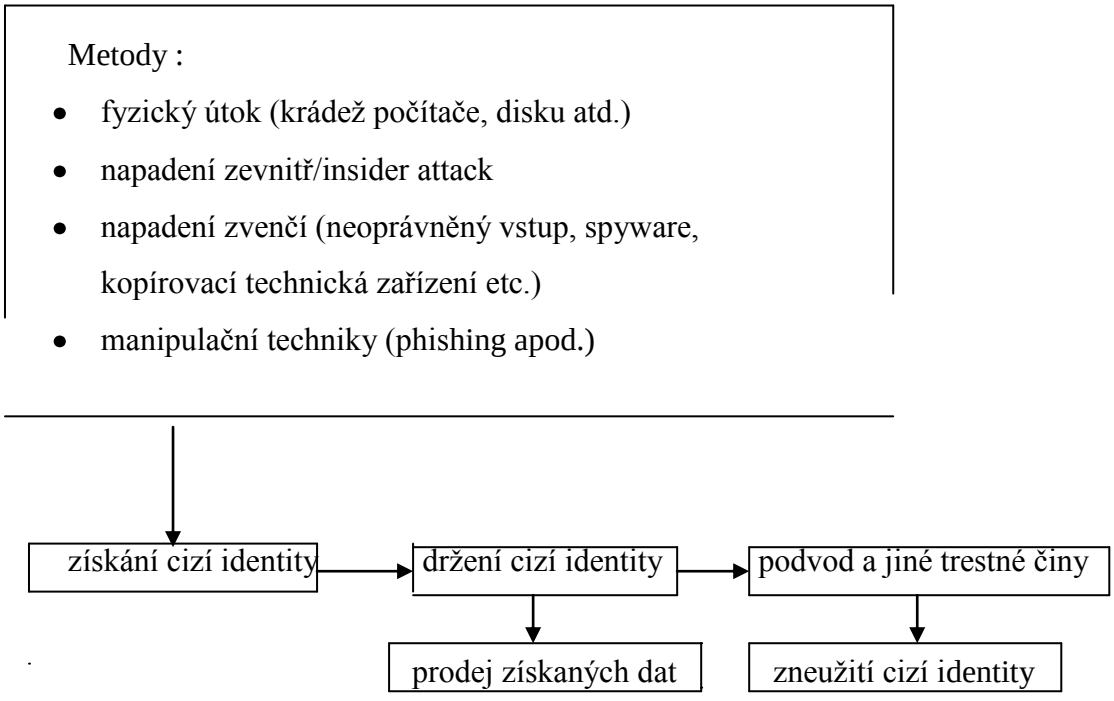
„sociálního inženýrství“ je někdy označován tzv. phishing (je to vlastně druh manipulace spočívající ve vylákání osobních nebo důvěrných údajů a informací prostřednictvím náhodně rozesílaných klamných mailů, předstírajících, že jejich autor je důvěryhodná osoba nebo instituce s cílem přimět adresáta ke sdělení těchto informací).

Část této kriminality, a to jak ve vztahu k neoprávněnému získávání elektronických údajů, tak listinných dokumentů, je páchána organizovaným způsobem. Např. krádeže pasů, jejich případné úpravy a prodej na černém trhu představují velmi prosperující živnost (ceny pasů jednotlivých států jsou přitom diferencované; např. se udává, že cena litevského pasu činí na černém trhu cca 3000 USD). Obdobně známe, a to i z našeho prostředí, organizované nelegální získávání údajů z platebních karet.

3. Způsoby páchání a možnosti odhalování a stíhání

Metody neoprávněného získávání elektronických identifikačních dat a postup následného nakládání s nimi ukazuje následující schéma:

Počítačová kriminalita a krádež identity[8]



Podle A. Segera (Department of crime problems, Council of Europe) dochází za pomoci zcizené identity k posunu v charakteru kyber-útoků; od široce zaměřených, masových a mnohoúčelových napadení informačních systémů přecházejí pachatelé k zaměření na specifické uživatele, skupiny a organizace, tj. ke konkrétně cíleným útokům.[9]

[8] Viz pozn č.2
[9] Tamtéž

Stíhání a odhalování nelegálního získávání a zneužívání cizí identity naráží na různé problémy. Jednotlivé instituce a organizace používají různé způsoby ochrany personálních identifikačních dat (rozličné systémy identifikačních znaků a jejich ochrany); také jejich samotná ochrana je u různých organizací na různé úrovni, od vícečetné a komplikované ochrany až po relativně jednodušší způsoby. Je pochopitelné, že jednotlivé organizace nejsou příliš nakloněny tomu odkrývat své systémy ochrany dat a sdílet je s organizacemi jinými. Také právní ochrana se v jednotlivých zemích liší jak ve formulaci relevantních skutkových podstat (nebo jejich absenci), tak v míře postihu, tj. v otázce sankcí a případně prostředků nápravy. Diskuse o aproximaci relevantní legislativy až po formulaci a přijetí společné "mezistátní" skutkové podstaty usnadňující přeshraniční a společné stíhání této formy trestné činnosti je teprve v počátcích, v kontrastu s touto formou kriminality, která samozřejmě národní hranice již dávno v řadě případů překračuje.

Je tu i problém *rozsahu a intenzity ochrany* identifikačních dat. Tato ochrana by na jedné straně měla zaručovat relativní bezpečí dat a nemožnost jejich získání či zneužití neoprávněnou osobou, ale na druhou stranu by úroveň a způsob ochrany neměly bránit operativnímu používání tímto způsobem zabezpečených stávajících instrumentů v běžném životě a nekomplikovat tak naopak nadměrně život oprávněnému uživateli. Prevence při ochraně dat je v tomto (a nejenom v tomto) ohledu účinná, pokud nezačne limitovat legální používání.

Významnou složkou prevence je informovanost veřejnosti o rizicích zneužití osobních elektronických údajů, o možnostech jejich neoprávněného získání i o možných způsobech obrany. Tato informovanost se u nás sice v poslední době zlepšuje, ale povědomí o těchto rizicích stále není dostatečně rozšířené.

Potíže při odhalování a stíhání krádeže a zneužívání osobních identifikačních údajů činí také *spolupráce státního a*

privátního sektoru při ohlašování této formy trestné činnosti, při sdílení informací a údajů a spolupráce při odhalování pachatelů. Obecně platí, že soukromý sektor, zejména instituce finančního sektoru, nejsou příliš nakloněny tomu tyto a obdobné útoky na sebe a na své klienty hlásit orgánům činným v trestním řízení. To se týká jak útoků zvenčí, tak zejména napadení zevnitř, tj. vlastními zaměstnanci (insider attacks). Častá je snaha tyto útoky nezveřejňovat, neoznamovat, řešit je pokud možno vlastními prostředky a neriskovat tak např. poškození důvěryhodnosti instituce a pověsti bezpečného finančního ústavu v očích zákazníků. Zjednodušeně by se dalo říci, že „bohatší" instituce takovými útoky sice více ztrácejí, ale o to méně je ohlašují.

4. Některé viktimologické aspekty

Oběti trestné činnosti spočívající v nelegálním získání a následném zneužití identifikačních osobních údajů se obvykle dostávají do velmi složité situace. To je dáno zejména tím, že krádež jejích identity je mnohdy provedena velmi sofistikovaným způsobem (pokud nejde o prosté odcizení osobních dokladů, platebních karet, listinných dokumentů apod.) při využití počítačových dat a systémů a celý průběh viktimizace se odehrává ve virtuální oblasti. Oběť mnohdy pozná, že došlo ke zneužití její identity, až se značným časovým odstupem. Škody, které oběti vzniknou, někdy nelze zpočátku rozpoznat jako důsledek trestné činnosti, ale mohou být považovány za důsledek administrativního omylu, nedostatků v evidenčních systémech, za selhání byrokratického aparátu apod. Důkazní břemeno tak spočívá na oběti, která se sama musí domáhat nápravy stavu umožňující trestnou činnost, kterou byla poškozena.

Další podstatnou okolností zhoršující postavení oběti, je závažnost způsobených škod. Australasijské středisko

policejního výzkumu[10] třídí důsledky způsobené krádeží a zneužitím identity takto:

- přímé finanční škody - včetně ztráty úspor; náklady na zjištění a předcházení finančních škod; náklady na obnovení důvěry;
- nepřímé finanční škody - včetně snížení ratingu peněžních ústavů; poškození obchodní a profesní pověsti; zápis do policejních evidencí;
- psychologické důsledky – ty značně závisí na tom, jak byly identifikační údaje zneužity; může jít i o existenční důsledky pro celou rodinu, jejíž člen se stal obětí zneužití identity;
- o závažné důsledky jde tehdy, když zneužití identity vede k další trestné činnosti, jako je například terorismus, obchodování s lidmi, drogová kriminalita.

Viktimologické aspekty trestné činnosti spočívající v odcizení a zneužití cizí identity se postupně dostávají do středu pozornosti. Stojí za zmínku, že například v USA teprve poté, kdy byla krádež identity prohlášena za federální zločin (stalo se tak v roce 1998 zákonem Identity Theft Assumption Deterrence Act), se uskutečnily solidnější výzkumy této trestné činnosti na početnějších souborech poškozených osob a institucí. V této oblasti se angažují zejména nevládní organizace, protože při zneužití identity se poškozené osoby často dostávají do situací, kdy mají potíže s vystavením nových platebních karet, s uzavíráním různých typů pojištění, se získáním bankovních úvěru nebo spotřebitelských půjček apod.

Samostatným problémem, z viktimologického hlediska, se v některých zemích stává odcizení a zneužití osobních údajů v oblasti zdravotnictví. V systémech převážně placené lékařské péče se vyskytují snahy vylákat úhradu poskytnutých

[10] Australasian Centre for Policing Research (ACPR)(2006).“Review of the legal status and rights of victims of identity theft in Australasia“ – http:// www.acpr.gov.au/pdf/ACPR145-2.pdf

medicinských úkonů a služeb na podkladě odcizených identifikačních údajů o zdravotním pojištění. To může vést i k tomu, že ve zdravotní dokumentaci některého pojištěnce se objeví lékařské informace o léčbě nebo zákrocích, které byly provedeny pod falešnou identitou, což může ohrozit „pravého" pacienta.

V moderní společnosti, kdy každý jedinec i instituce vstupují do složitého předíva vztahů, povinností a oprávnění, se stává ochrana a zachování vlastní identity naléhavou nezbytností. Viktimnost, tedy riziko, že se staneme obětí trestné činnosti ohrožující a zneužívající naše identifikační data, je vysoká.

5. Jaký je stav v České republice

Lze říci, že v České republice byly vytvořeny dostatečné zákonné podmínky pro náležitý trestní postih kriminality spojené s odcizením a zneužitím identifikačních dat. Protože jde zejména o problematiku spojenou z využitím výpočetní techniky a počítačových programů a systémů, byla značná pozornost věnována výstižnému formulování skutkové podstaty trestného činu poškození a zneužití záznamu na nosiči informací podle § 257a trestního zákona. Tento trestný čin se stal součástí trestního zákona od 1. ledna 1992 na základě zákona č.557/1991 Sb., kterým byl trestní zákon novelizován. V případech některých jiných trestných činů může být důvěrnost, integrita a dostupnost počítačových dat a systémů objektem sekundárním, nevyjádřeným ve skutkové podstatě jiného trestného činu .[11]

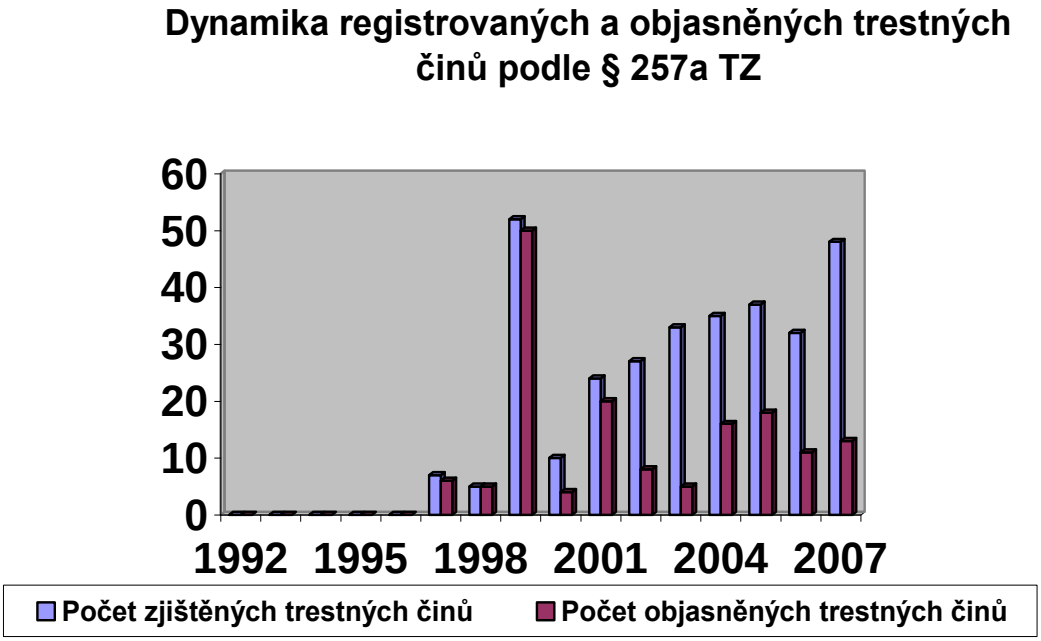
Zákonem č. 134/2002 Sb. bylo zpřesněno ustanovení § 257a tr. zák. v prvém odstavci tak, aby nevznikaly pochybnosti, že získání přístupu k nosiči informací musí být provedeno již v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch. Je zřejmé,

[11] Srov.: NOVOTNÝ, O. - VANDUCHOVÁ, M. A KOL.: Trestní právo hmotné – I. Obecná část. Praha: ASPI, a.s., 2007, s. 153.

že přístup k nosiči informací, např. při výkonu zaměstnání nebo funkce, je často získán bez takového určitého úmyslu a uvedený úmysl je pojat až dodatečně. Dílčí doplnění byla provedena i v písm. b) a c) tohoto odstavce. Zákonem č. 253/2006 Sb. byla provedena další dílčí změna § 257a tr. zák. v tom směru, aby při ukládání trestu bylo možno uložit trest propadnutí nejen věci, ale též jiné majetkové hodnoty.

Celkový počet stíhaných, obžalovaných a odsouzený osob pro trestný čin poškození a zneužití záznamu na nosiči informací podle § 257a tr. zák. v ČR v letech 1992-2007 je uveden v tabulkách.

Tabulka č.1



Pramen: Policejní statistika

Tabulka č.2

Počet stíhaných, obžalovaných a odsouzených osob za trestný čin podle §

Rok	Počet osob	Počet osob obžalovaných	Počet osob odsouzených
1992	0	0	0
1993	1	1	0
1994	4	4	0
1995	4	2	0
1996	6	6	1
1997	14	14	1
1998	14	6	0
1999	11	7	2
2000	18	15	0
2001	22	14	2
2002	22	14	8
2003	14	7	0
2004	17	14	7
2005	33	27	1
2006	18	16	3
2007	14	12	1

Pramen: justiční statistika

Nový trestní zákoník (zákon č. 40/2009 Sb.) s účinností od 1. ledna 2010 rozšiřuje okruh trestných činů zaměřených na ochranu důvěrnosti, integrity a dostupnosti počítačových dat a systémů. Konkrétně budou upraveny tyto trestné činy:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230).
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231).
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).
- Porušení tajemství dopravovaných zpráv (§ 182).

Lze proto předpokládat, že počty spáchaných trestných činů a počty stíhaných a odsouzených osob pro tento druh kriminality se budou v příštích letech citelně zvyšovat.

S tím souvisí i problematika latence této kriminality. Již bylo naznačeno, že například bankovní ústavy a jiné finanční instituce, ve kterých došlo k poškození klientů

v důsledku zneužití jejich identifikačních dat, nemají zájem hlásit tyto skutečnosti orgánům činným v trestním řízení, protože se obávají snížení své důvěryhodnosti a raději přímo svým poškozeným klientům finanční ztráty uhrazují. Tyto finanční instituce také utajují modus operandi, kterým došlo ke zneužití identifikačních dat, aby nevyzrazovaly podstatu a rozsah svého systémového zabezpečení. Poškozený se tak ani nedoví, že je předmětem zájmu pachatelů. Další důvody latence mohou spočívat také v tom, že část poškozených nechce oznamovat finanční ztráty způsobené zneužitím jejich identifikačních údajů, protože se chtějí vyhnout nežádoucí publicitě. Připomeňme například zprávy, které proběhly ve světovém tisku v říjnu 2007 o tom, jak se stal obětí zneužití identifikačních dat starosta New Yorku Michael Bloomberg, nebo medializaci případů poškození světově známého filmového režiséra Stevena Spielberga či populárního golfového hráče Tigera Woodse. Přehnaný zájem medií by bylo možno považovat i za sekundární viktimizaci.

6. Závěry z konference ISPAC

Nelegální získávání cizích identifikačních údajů, jejich zneužívání a další trestná činnost s tím spojená představují tedy jednu z výzev, které před nás klade vývoj kriminality. Pachatelé i v této oblasti dokázali pružně zareagovat na technologický pokrok a využít, resp. zneužít možnosti, které otevřel. Tradiční podstata trestných činů krádeže a podvodu se v této oblasti oděla do nové formy, využívá nových nástrojů a vyžaduje proto příslušnou reakci. Zatím probíhá diskuse o podstatě a fenomenologii této trestné činnosti, která by měla vyústit v diskusi o společných, tj. mezinárodních řešeních. Konference ISPAC v roce 2007 v Courmayeuru [12] ve svých závěrech doporučila:

- vymezit rozsah a povahu problému,

[12] The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity. International conference, ISPAC, Courrnayeur 30.11.-2.12.2007

- charakterizovat oběti a analyzovat formy a způsoby viktimizace,
- najít existující právní mezery v legislativě jednotlivých států a v možnostech mezinárodní spolupráce orgánů činných v trestním řízení při postihu této trestné činnosti, pokud překračuje státní hranice (což je nezřídka),
- provést inventuru existujících právních a dalších nástrojů postihu a spolupráce, zjistit, které postačují a co je třeba zavést nově,
- zlepšit spolupráci státního a soukromého sektoru,
- stanovit potřeby a priority s ohledem na stanovení přijatelné míry ochrany a regulace.

Které oblasti je třeba přitom považovat za základní?

- Prevenci – osobní opatrnost, informovanost o rizicích, zabezpečení dat ve veřejném i státním sektoru;
- legislativu (kriminalizace nelegálního vstupu do datových systémů, vytvoření specifické skutkové podstaty, stanovení odpovědnosti za zabezpečení dat);
- postih (spolupráce veřejného a soukromého sektoru, usnadnit ohlašování útoků, shromažďování a analýza informací);
- mezinárodní spolupráce.

Prameny

CHRYSSIKOS, D. - PASSAS, N. - RAM, C. D. (EDS.): The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity. ISPAC, Milano 2008

GŘIVNA, T.: Rozhodování soudů o skutcích posouzených podle § 257a TZ. Zpracováno v rámci výzkumu IKSP Výzkum a analýza závažných forem trestné činnosti. Dosud nepublikováno.

International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. Results of the

study on fraud and the criminal misuse and falsification of identity. Dokument OSN RE/CN.15/2007/8

LEVI, M.: Identity fraud: the „glocal" dimension. Referát na mezinárodní konferenci ISPAC, Courmayeur 30.11.-2.12.2007

MCNULTY,K.: Identity related crime and economic fraud. Referát na mezinárodní konferenci ISPAC, Courmayeur 30.11.-2.12.2007

SEGER, A.: Cybercrime and identity theft: the challenges. Referát na mezinárodní konferenci ISPAC, Courmayeur 30.11.-2.12.2007

ŠTEFUNKOVÁ, M.: Victimisation Surveys. PhD. thesis, Bratislavská vysoká škola práva. Bratislava 2009 (zatím nepublikováno)

Scheinost, M. – Karabec Z.

zneužití identity a trestná činnost s tím spojená

SOUHRN

Článek se zabývá relativně novu formou kriminality, tzv. „identity fraud" a „identity theft", která se stala v poslední době předmětem zvýšeného zájmu mezinárodních organizací i odborné veřejnosti. Jedná se v zásadě o získání cizí identity, resp. personálních dat jiné osoby bez jejího vědomí a souhlasu a jejich zneužití ke spáchání trestné činnosti. Tato činnost se děje obvykle s využitím elektronických komunikačních a archivačních systémů. Autoři informují o charakteru této formy kriminality a hlavních problémech spojených s jejím odhalováním, postihem a prevencí.

Scheinost, M. – Karabec Z.

Identity fraud and related criminal action

SUMMARY

The article focuses on a relatively new form of crime, the so-called „identity fraud" and „identity theft", which has lately become subject to increased interest among international organisations as well as the expert public. It basically consists in obtaining another person's identity, or personal data of another person without the person's awareness and approval, and their misuse for committing criminal activity. This activity usually takes place using electronic and archiving systems. The authors inform about the nature of this form of crime and the main problems related to its detection, sanctions and prevention.

Scheinost, M. –Karabec, Z.

Der Missbrauch der Identität und die damit verbundene Straftätigkeit

ZUSAMMENFASSUNG

Der Artikel setzt sich mit einer relativ neuen Form der Kriminalität, der sog. „identity fraud" und „identity theft" auseinander, die in letzter Zeit die Aufmerksamkeit von internationalen Organisationen und der fachlichen Öffentlichkeit auf sich gezogen hat. Es handelt sich im Prinzip um die Erwerbung einer fremden Identität, bzw. der Personaldaten einer anderen Person, ohne ihr Wissen und ihre Zustimmung und um den Missbrauch dieser Daten zur Verübung der Straftätigkeit unter Verwendung von elektronischen Kommunikations- und Archivierungsystemen. Die Autoren des Artikels informieren über den Charakter dieser Kriminalitätsform und über die Hauptprobleme, die mit ihrer Aufdeckung, Bestrafung und Prävention verbunden sind.