Bude kryptoanalýza v Česku trestána vězením?

Vlastimil Klíma, kryptolog, http://cryptography.hyperlink.cz

Pokud s tím něco páni poslanci neudělají, tak až skončím přednášku o kryptoanalýze na MFF UK, půjdu se přihlásit na Policii, že jsem spáchal trestný čin. A ti, kdo provádí penetrační testy nebo administrátoři sítí, kteří testují slabá hesla, půjdou asi také.

V letmé informaci jsem se dostal k projednávanému textu vládního návrhu trestního zákona. Jeho § 205 mě vyvedl z míry, protože by postavil kryptoanalýzu mimo zákon a penetrační testování do složité situace. Přečtěte si přiložené znění tří vyjmutých paragrafů v dodatku a pak posuďte sami, jestli jsou následující obavy zbytečné. Doufám, že ano nebo že bude přijat pozměňovací návrh.

Začněme výňatky. Upozorňuji, že citlivě, ale přece jen jsou vytrženy z kontextu návrhu trestního zákona - viz rámeček.

> § 204: ... Kdo ... **neoprávněně získá přístup k počítačovému systému** ... bude potrestán odnětím svobody až na jeden rok...
> § 205: ... Kdo **neoprávněně ... zpřístupní... počítačové heslo**, pomocí nichž lze získat přístup k počítačového systému..., bude potrestán odnětím svobody až na jeden rok...

Říkáte si, že to je žert? Bohužel není.

Na MFF UK studenty učím tuto definici:
Moderní kryptoanalýza je věda o hledání slabin nebo prolamování matematických metod informační bezpečnosti.

Konkrétní použití kryptoanalýzy směřuje právě k tomu, aby se případné slabiny odstranily. K tomu je nutné je zveřejnit, učit se o nich, publikovat na mezinárodních konferencích. Z druhé strany **je to zcela jistě také možné chápat a využít to jako návod na zneužití rozpoznaných slabin ke skutečné nezákonné činnosti**. Věda slabiny odhaluje, ale nezneužívá. Vědce bychom tedy trestat neměli, měli bychom trestat ty, kdo zneužívají vědecké poznatky k páchání nezákonné činnosti.

Současný návrh § 204-206 trestního zákona však vyvolává velmi vážné pochyby, téměř jistotu, že potrestán bude i vědec.

V sázce je
1) Výuka moderních metod kryptoanalýzy na vysokých školách a univerzitách (konkrétně na MFF UK) .
2) Vědecký příspěvek na mezinárodní konferenci.
3) Vědecký názor na odborném internetovém fóru, webu, poštovní konferenci, diskusní skupině.
4) Publikace vědeckého příspěvku na serveru mezinárodní organizace pro kryptologický výzkum (IACR).
5) Soukromé e-maily s kryptology diskutující kryptoanalytické metody.

6) Účast ve veřejných mezinárodních soutěžích na prolomení kryptografického algoritmu (DES, RSA, ECC, MD,..) - je to dokonce děláno pro značnou finanční odměnu, tedy dalo by se to kvalifikovat jako luštící práce na objednávku.
7) Vědecké granty, financované státem (vysoké školy, univerzity a další státní orgány)
8) a další.

Některé naše příspěvky, které jsme publikovali s kolegou dr. Rosou ve sbornících mezinárodních kryptologických konferencí nebo na webu IACR, **přispěly ke zkvalitnění obrany informačních systémů proti útokům, ale jen proto, že jsme tyto slabiny odhalili**. Například kdyby bylo zneužito publikování útoku na protokol SSL, přineslo by to odhalení přístupových hesel a privátních bankovních informací, tedy právě toho, o čem zákon mluví. Pokud by banky neimplementovaly námi doporučené úpravy a obranu, mohly by vzniknout značné škody v mezinárodním měřítku. Podobně i další naše kryptoanalytické výsledky, které získaly uznání na mezinárodním poli, by mohly být doma oceněny úplně jiným způsobem.

Protože jsem laik v oboru práva, získal jsem společně s Mgr. Pavlem Vondruškou odpovědi dvou odborníků na znění navrhovaného zákona, viz dodatky níže. Bohužel moje obavy nerozptýlili, spíše je potvrdili. Závěrem je, že text není dobrý, a měl by se změnit.

Poslal jsem proto prosbu paní JUDr. Parkanové, předsedkyni Ústavně právního výboru Poslanecké sněmovny Parlamentu ČR o zařazení pozměňovacího návrhu. Bohužel jsem zatím nedostal odpověď ani potvrzení o přijetí e-mailu. Možná se paní předsedkyně ještě nedostala k e-mailu, ale věřím, že mi odpoví.

Na závěr ještě poznámka. Uvědomil jsem si, že ve stejné situaci budou pravděpodobně i ti, kdo plánují a provádí penetrační testy. Tady se mohu mýlit, takže to přenechávám jim na zvážení a poradu s právníky. Jistě, penetrování je vždy pokryto smlouvou. Jenže zákon je poněkud vyšší norma. To za prvé. A za druhé - je vždy smluvně pokryto vše? Všechny cesty a metody penetrace? A bude i nadále VŠE podle nového zákona zákonné? Nejsem odborník na penetraci ani právo, ale pokud bude v ohrožení kryptoanalýza, zabývající se vědeckými otázkami odhalování slabin a prolamování matematických metod informační bezpečnosti, pak je otázka, nakolik bude právně zajištěna zcela praktická "bílá" hackerská činnost.

Až bude zákon schválen, bude mnohem horší přijmout změny než teď, kdy je na to přímo vyhrazen čas. Proto prosím všechny, kdo mají nějaký zájem na změně, aby se pokusili nějakým způsobem změně připravovaného textu zákona napomoci.

Dodatek č. 1: Trestní zákon - vládní návrh II.

§ 204
Neoprávněný přístup k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací

(1) Kdo poruší bezpečnostní opatření a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá, nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.
(3) Odnětím svobody na šest měsíců až tři léta, propadnutím věci nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.
(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem značnou škodu,
c) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
d) způsobí-li takovým činem vážnou poruchu v činnosti státního orgánu,
jiného orgánu veřejné správy nebo samosprávy, právnické osoby nebo fyzické osoby, která provozuje podnikatelskou činnost podle zvláštního právního předpisu, státního podniku nebo jiného podniku.
(5) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 205
Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo neoprávněně vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k spáchání trestného činu neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),
b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačového systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2) Odnětím svobody až na tři léta, propadnutím věci nebo zákazem činnosti bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.
(3) Odnětím svobody na šest měsíců až pět let nebo propadnutím majetku bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 206
Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1)Kdo z nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté
a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí značnou škodu, bude potrestán odnětím svobody až na šest měsíců, propadnutím věci nebo zákazem činnosti.
(2) Odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Dodatek č. 2: Stanovisko prof. Smejkala, rektora VŠFS, člena Legislativní rady vlády ČR

Plně chápu kryptology, že jsou zneklidněni navrhovaným zněním ust. § 205. Uvažování matematické, natož pak kryptologické totiž k tomuto výkladu, který nazýváme gramatickým, svádí. Obávat se ale dle mého názoru nemusejí, alespoň ne příliš, neboť je třeba dané ustanovení vyložit v širším kontextu, a to jednak použitím rozboru logického či teleologického. Na druhou stranu musím ale konstatovat, že znění ust. § 205 není zcela přesné, a to ani ve vztahu k mezinárodní úmluvě, z níž pochází.
Možná bychom mohli začít příkladem z jiného, byť podobného oboru: zámečník nejen vyrábí zámky a otevírá zabouchnuté dveře, ale také zkoumá, jak jsou zámky vymyšleny a jak by je případně bylo možno otevřít. Pro svoji potřebu, tj. otevírání dveří či trezorů jejich vlastníkům si zhotovil řadu pomůcek, které toto otevírání značně usnadňují. Je nebezpečí, že bude trestně stíhán? Nikoliv, alespoň do okamžiku, než otevře trezor jiné osobě, nežli vlastníkovi, nebo prodá své sofistikované pomůcky kasaři.
Podobně tomu je i v případě ust. § 205, neboť je třeba si uvědomit, že nutnou podmínkou naplnění této skutkové podstaty je znak „neoprávněnosti“. Navíc v deliktu popsaném v písm. a) je jasně uvedeno, že se tak musí stát za účelem páchání zde vyjmenované trestné činnosti. Ano, v písm. b) není již uvedeno, že má být dosaženo neoprávněného přístupu k počítačovému systému – tady si myslím, že by bylo možné text vylepšit. Nikoliv ale z hlediska absolutní chyby, vedoucí k totálnímu ohrožení kryptologů trestním stíháním, ale z hlediska jednoduššího výkladu a chápání i běžnou veřejností.
Nicméně ani bez tohoto doplňku si nemusí kryptologové balit zavazadla k emigraci. Skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací (§ 204) a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 205) jsou zařazeny do návrhu trestního zákona na základě *Úmluvy Rady Evropy o počítačové kriminalitě*,[1] (Budapešť, 23. listopadu 2001), kdy bylo třeba zapracovat zejména články 2 až 11, které stanoví kriminalizaci nezákonného získání přístupu k počítačovému systému, nezákonného odposlechu počítačového systému technickými prostředky, neoprávněného poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat, která jako širší pojem zahrnují i počítačové informace, omezování funkčnosti počítačového systému pomocí manipulace s počítačovými daty, počítačového padělání, dále výrobu, prodej, opatření za účelem použití, držení, dovoz, distribuci a zpřístupňování zařízení, která jsou vytvořena

[1] Convention on Cybercrime (ETS no. 185), viz http://conventions.coe.int/

nebo uzpůsobena k páchání uvedených trestných činů podle článků 2 až 5 uvedené Úmluvy, nebo přístupových hesel, kódů a podobných počítačových dat, pokud má pachatel v úmyslu tato zařízení nebo kódy použít ke spáchání uvedených trestných činů podle článků 2 až 5 uvedené Úmluvy. Zde máme tedy výkladové vodítko, že postihován nemá být autor, ale pachatel, který těchto postupů využije.
Možná bychom nepřípustnost trestní odpovědnosti v případě výuky, výzkumu a vývoje mohli odvozovat nejednoduchou cestou přímo z ust. § 13, definující trestný čin jako čin protiprávní; vzhledem ke změně koncepce zákona na tzv. formální pojetí trestného činu, kde již nenajdeme pojmový znak „pro společnost nebezpečný čin“, jako tomu je ve stávajícím trestním zákoně, to nemusí být vůbec lehké či dokonce možné.
Nový zákon v ust. § 31 – Přípustné riziko – uvádí, že trestný čin nespáchá, kdo v souladu s dosaženým stavem poznání a informacemi, které měl v době svého rozhodování o dalším postupu, vykonává v rámci svého zaměstnání, povolání, postavení nebo funkce společensky prospěšnou činnost, kterou ohrozí nebo poruší zájem chráněný trestním zákonem, nelze-li společensky prospěšného výsledku dosáhnout jinak. Zde by ale asi nešlo toto ustanovení vztáhnout na kryptology – amatéry, natož hackery, ale pravděpodobně pro většinu případů, dr. Klímou uvedených, je možné je aplikovat.
Podle mého názoru nelze tedy podle daného ustanovení začít masově posílat kryptology do vězení. Čin musí být protiprávní a úmyslný – tzn. dle mého názoru se toto ustanovení nevztahuje na výrobu a šíření prostředků pro testování a zajišťování bezpečnosti IS/ICT. Nechápu ale, proč ani v zákoně, ale zejména ani v důvodové zprávě k němu, již nenajdeme další odstavec z *Úmluvy Rady Evropy o počítačové kriminalitě*, kde se říká: „This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.“
Výše uvedené připomínky by mohly být využity pro poslanecký pozměňovací návrh, což vzhledem ke stádiu projednávání nového trestního zákona je právě nyní možné. Je na české kryptologické obci, zda vyvine takovou iniciativu.
Prof. Ing. Vladimír Smejkal, CSc., rektor Vysoké školy finanční a správní v Praze, člen Legislativní rady vlády

---

Dodatek č. 3: Stanovisko Mgr. Zbyňka Loebla, LL.M. z CEAG
V e-mailové odpovědi se vyjádřil velmi jasně:
"Souhlasím s panem prof. Smejkalem, že je třeba navrhnout změnu navrženého ustanovení tak, aby nebylo v rozporu s mezinárodní úmluvou. Jinak hrozí až zneužití tohoto ustanovení, nejen spory o výklad."
Mgr. Zbyněk Loebl, LL.M., vedoucí konzultant CEAG (CENTRAL EUROPEAN ADVISORY GROUP), český zástupce v IT Law Group Europe, asociaci právních poradenských firem v Evropě, specializující se na informační technologie, telekomunikace a právní problémy týkající se nové ekonomiky.

-oOo-