# Nový trestní zákon - kampaň za změnu k § 205 - pozměňovací návrh s vysvětlením

## Pozměňovací návrh k § 205 návrhu trestního zákoníku, , sněmovní tisk č. 744 pro druhé čtení tisku na 48. schůzi PS

### I. Text stávajícího návrhu:

§ 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.*

### II. Návrh pozměňovacího návrhu pro 2. čtení tisku na 48.schůzi PS:

Na konec návětí odstavce 1 doplnit slova „v úmyslu spáchat trestný čin 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)“.
a
Opravit gramatické překlepy.

### Text navrhovaného ust. § 205 (úpravy jsou vyznačeny tučným písmem):

§ 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 **v úmyslu spáchat trestný čin 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)**
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořen**é** nebo přizpůsoben**é** 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 počítačové**mu** 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.

**III. Odůvodnění:**

Mezi odborníky na informační technologie je běžné, že se informace o zranitelnosti (chybách) v počítačových systémech zveřejňují (tzv. princip full disclosure), o problémech se otevřeně diskutuje a **různé demonstrační a testovací nástroje jsou volně dostupné.** Pro různé nástroje (tzv. exploity) existuje dvojí využití – mohou být zneužity, ale zrovna tak je může používat odborník k testování bezpečnosti systému, demonstraci zranitelnosti, studiu apod. Různé nebezpečné nástroje vytváří jak hackeři, tak odborníci na bezpečnost, kteří tímto právě často nástroj analyzují, navrhují protiopatření, diskutují nad možnostmi, nástroj lze i zveřejnit, aby se podle toho mohl každý bezpečnostní odborník zařídit. Toto ustanovení by omezilo veřejnou diskusi o chybách v systémech poskytující i demonstrační software (exploit). **Pokud by takto vázla diskuse v odborných kruzích, je zde zřejmé riziko stagnace celého průmyslu (zatímco tradičně konspirační aktivity hackerů by zákon omezoval podstatně méně).**

Současná **dikce ustanovení § 205 je v rozporu se zněním čl. 6 odst. 2 Úmluvy Rady Evropy o počítačové kriminalitě, (Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185, viz http://conventions.coe.int/),**

**která speciálně v odstavci 2 článku 6 zdůrazňuje, že podmínkou trestnosti je, že pachatel musí sledovat protiprávní cíl.**

Rozdíl mezi hackerem a přednášejícím kryptoanalýzu na Univerzitě Karlově v Praze je pouze v tomto cíli. Oba dva mohou přechovávat, vytvářet a jinak pracovat se stejnými prostředky. Kryptoanalytik vyvíjí a používá tyto prostředky k odhalování slabin systémů s cílem navrhnout protiopatření a zodolňovat je, hacker s cílem spáchat trestný čin. Protože rozdíl mezi nimi je jedině a pouze v úmyslu, Úmluva výslovně požaduje, aby podmínkou trestnosti byl protiprávní cíl (viz výše).

Dalším příkladem je administrátor počítačové sítě. Když podle nějaké nové kryptoanalytické metody vytvoří nebo použije program, který odhaluje slabá přihlašovací hesla, metodou práce se nijak neliší od hackera. Jeho úmyslem je zjistit, zda uživatelé nepoužívají slabá hesla a zabránit tomu, aby se systém nemohl stát předmětem útoku hackerů. Úmyslem hackera je slabá hesla využít a do systému proniknout. Oba dva opět používají stejné prostředky a metody a liší se jedině a pouze úmyslem.

Navržená varianta je**v souladu s Úmluvy Rady Evropy o počítačové kriminalitě; není v rozporu z žádnými jinými mezinárodními závazky ČR.**

Změna **nepřinese dopady na státní rozpočet, nemá rovněž vliv na rovnost mužů a žen, sociální dopady ani dopady v oblasti životního prostředí.**

Změna **významně napomůže rozvoji informatizace společnosti,** a to umožněním zvyšování bezpečnosti dat a nejrůznější elektronické komunikace v celé řadě sektorů ekonomiky. Jako taková má **jednoznačně pozitivní dopad na hospodářský život;** lze říci, že je podmínkou kontinuálního vývoje základní podmínky informatizace, její bezpečnosti.

RNDr. Vlastimil Klíma,
JUDr. Ing. Helena Svatošová,
materiál Iudicium remedium pro meziresortní připomínkové řízení, 2003