POČITAČOVÁ KRIMINALITA-NEBEZPEČÍ PRO VAŠI PRÁCI

D. Brechlerová
Katedra Informatiky PEF, Vysoká škola zemědělská
165 21 Praha 6 Suchdol, tel.(02) 338 2356, fax.(02) 39 37 08

Anotace:
Referát podává základní informace o počítačové kriminalitě, o zákonných normách týkajících se této oblasti a o možnostech ochrany proti tomuto druhu kriminality.

Summary:
This paper gives basic information about computer crime, about legal regulations dealing with this topic and about possible approaches how to secure data from this kind of crime.

Klíčová slova:
Počítačová kriminalita, bezpečnostní opatření, počítačové viry

Key words:
Computer Crime, Safety Measures, Computer Viruses

Během několika poslednich let se aplikace výpočetní techniky (dále VT), zejména díky PC, rozšířily i do oblastí, kde dříve VT nebyla využívána. Společnost se stává na výpočetní technice stále více závislou, proto musí více dbát na bezpečnost informací. Ale v souvislosti s rozšířením VT a především s nárustem významu informací touto technikou zpracovávaných se objevuje nový druh kriminality-počítačová kriminalita.

Pod pojmem počítačová kriminalita se skrývá široký okruh činností, které zde nyní vyjmenuji včetně jejich stručné charakteristiky.

1.Útok na počítač, program, komunikační zařízení; krádež téhož.

Sem patří odcizení nebo poškození počítače, útok na informace v něm obsažené. Musíme si uvědomit, že při odcizení počítače např. s datovými soubory, mohou tyto soubory mnohonásobně převyšovat hodnotu počítače a mohou být případně i nenahraditelné. Odcizení či poškození souborů může mít i další následky, například odcizení adresáře zákazníků může firmu zničit. Do této kategorie nutno dále zařadit zavirování.

2.Neoprávněné užívání počítače či komunikačních zařízení.

Pod tuto kategorii řadíme tzv. krádež strojového času tj. užívání počítače (či komunikačního zařízení) včetně softwaru, které patří někomu jinému, obvykle zaměstnavateli. Zde navíc hrozí zavirování počítače, příp. při neodborné manipulaci se systémem i zhroucení systému, poškození datových souborů atd.

3.Neoprávněný přístup k datům, špionáž, získávání utajených informací o osobách.

Patří sem nahlížení do databází, změny v databázích, neoprávněné kopírování dat pro komerční účely. Pouhé nahlédnutí do databáze u nás ale není trestné, musí být prokázán úmysl způsobit škodu (např.změnami v databázích). Dále je trestné neoprávněné užití databáze. Dalšimi doprovodnými jevy může být vydírání, nekalá soutěž, ohrožení hospodářského tajemství atd.

4.Změny v programech, datech, technickém zapojení počítače, v komunikačních zařízeních.

Zde můžeme hovořit jak o změnách způsobených viry, tak o změnách způsobených záměrně (např.nepatrné změny v programu způsobující defraudaci atd.)

5.Zneužití počítače k další trestné činnosti.

Typickým příkladem z této kategorie je manipulace s daty ve vlastní prospěch (data týkající se např. tržeb, skladů, platů, vkladních knížek aj). V tomto případě pachatel často zneužívá skutečnosti, že lidé ochotně věří výpočetní technice a např. výpisy z tiskárny považují již předem za pravdivé. Pachatel trestné činnosti zde může např. měnit data, a to jak při vstupu dat, tak během chodu programu i při výstupu dat.

6.Podvody páchané pomocí výpočetní techniky

Do této skupiny můžeme zařadit finanční hry tzv. řízené počítačem (typu pyramida), kdy všichni hráči nemají stejné šance a předpoklady k výhře. V současnosti je provozování těchto her dle § 250a trestné.

7.Porušení autorského (softwarového) práva.

Jedná se pravděpodobně o nejčastější jev počítačévé kriminality, do kterého patří: nelegální provozování počítačových programů, plagiátorství (tj. malá změna programu a jeho neoprávněný prodej), neoprávněná tvorba a šíření české verze, šíření pirátských rozmnoženin, nelegální šíření programů.

Jak je vidno z předcházejícího výčtu, počítačová kriminalita v sobě zahrnuje velké množství různorodých činností. Stejně rychlým vývojem, kterým prochází VT, prochází i počítačová kriminalita. Na to ovšem musí reagovat i zákonodárství. Vzhledem k tomu, že v posledních 3 letech i u nás došlo v této oblasti k několika významným změnám, považuji za nutné se krátce zmínit o příslušných zákonech.

V r. 1990 byl novelizován autorský zákon (247/90 Sb.), který nyní uvádí ve výčtu autorských děl také počítačové programy.

S účinností od 29.4.1992 byl přijat zákon 256/92 Sb. o ochraně osobních údajů v informačních systémech, který upravuje zejména povinnosti související s ochranou informací.

V roce 1991 bylo přijato ustanovení (novelizace trestního zákona 557/91 Sb. $257a), které se zabývá poškozením a zneužitím záznamu na nosiči informací.

Ačkoliv ke všem výše uvedeným právním úpravám mají jak právníci, tak uživatelé VT mnoho připomínek, jistě se jedná alespoň o první potřebné kroky v dané oblasti.

Ochrana proti počítačové kriminalitě musí především spočívat v prevenci, a to u každého uživatele VT. Je nutno se chránit proti všem druhům této trestné činnosti.Protože se jedná o velmi závažnou oblast, vyspělé státy vyvíjejí normy pro hardwarovou i softwarovou ochranu. V USA je to tzv. Oranžová kniha, ve Francii Modro-bílo-červená, společná kriteria dnes rozvíjí i Evropské Společenství. V řadě zemí pracují specializované instituce, které se zabývají ochranou dat a VT, pořádají školení atd. U nás bohužel se zatím, až na vyjímky, jedná o postupy nepříliš koordinované.

Proto musí každý uživatel VT zhodnotit všechny možnosti svého ohrožení a poté promyslet (případně za pomoci specializované firmy) preventivní opatření. Mezi ta by měla patřit organizační opatření ,systém zálohování souborů,jasně vypracované dodatky k pracovním smlouvám, které každému pracovníkovi vymezují rozsah oprávnění při práci s počítačem (které soubory smí používat, zákaz her na pracovišti, zákaz užívání soukromých disket atd.) Dále je nutno při nákupu softwaru (pouze od solidních firem) trvat na přesném sepsaní uživatelských smluv a dobře prostudovat licenční ujednání. S autory softwaru, ať již jsou zaměstnanci firmy či organizace nebo jsou externisté, by měla být sepsána smlouva, která poté zabrání sporům při prodeji softwaru. Používání kvalitních protivirových programů by mělo být samozřejmostí. Na našem trhu se již objevují ochranné programy, chránící data, části disku, zamezující nežádoucím operacím na souborech atd.

Při všech těchto preventivních opatřeních je dále nutno počítat s tím, že VT stále více užívají pracovníci v této oblasti zcela nekvalifikovaní.Proto je lépe zavést taková opatření, která pracují nezávisle na obsluze VT.

V tomto referátu jsem chtěla naznačit ,s jakým nebezpečím by každý uživatel VT měl počítat při své práci. Je jasné, že se jedná o téma nesmírně široké, a já jsem v tak krátké době pouze mohla probudit váš zájem o tuto problematiku.

Literatura:

M.Šipovič: Softwarové pirátství v ČSFR, sborník přednášek ze semináře Právní prostředky proti soft.pirátství v ČSFR,1992

Vladimír Smejkal,Tomáš Sokol: Počítačová kriminalita a její trestněprávní aspekty , sborník přednášek ze sem. Ochrana dat a právní úprava v ČR, 1993
Alena Bímová: Bezpečnost počítačového zpracování informací a její normy,tamtéž
Václav Zápotocký: Právní ochrana software,SEKURKON Praha,1993
Kriminalistická společnost(časopis čs. společnosti pro kriminalistiku) 1/1992,2/1992, 5/1992