Kapitola 12

POČÍTAČOVÁ KRIMINALITA

12.1 Úvod

Počítače sú súčasťou nášho každodenného života, ba niekedy až nevyhnutnosťou. Na jednej strane, sú komunikačným nástrojom spájajúcim celý svet neprekonateľnou rýchlosťou (napr. e-mail či Skype), neoceniteľným pomocníkom pri životných povinnostiach (napr. platenie výdavkov prostredníctvom internet bankingu), ideálnym prostriedkom na trávenie voľného času (napr. pozeranie filmov či fotografií) či v mnohých prípadoch štandardným pracovným nástrojom.

Na druhej strane, človek prišiel so „skvelým" nápadom – uškodiť inému prostredníctvom počítača (a internetu). Nemožno povedať, že človek začal konať trestnoprávne, ale až pri vybraných závažných konaniach spoločnosť usúdila, že je vhodné ich vymedziť ako trestné činy. Navyše, človek prišiel s ďalším „skvelým" nápadom – uľahčiť si už existujúcu trestnú činnosť, ktorá pomocou počítača (a internetu) je jednoduchšia, efektívnejšia a najmä anonymnejšia.

Počiatky počítačovej kriminality možno datovať do obdobia 60-tych a 70-tych rokov minulého storočia. Prirodzene, v tých časoch bola odlišná od dnešnej. Počítače boli úplne iné od dnešných. Ich cena predstavovala milióny amerických dolárov, zaberali celú miestnosť, vyžadovali si špeciálny klimatizačný systém a v neposlednom rade tím špecialistov, ktorí sa starali o ich chod. Vlastníkom počítačov boli spravidla len veľké spoločnosti, ako napríklad banky. Navyše, počítače neboli pripojené do sietí a v žiadnom prípade nemožno hovoriť o prítomnosti internetového pripojenia, ako ho poznáme dnes.

Počítačová kriminalita je v súčasnosti najrýchlejšie sa rozvíjajúca forma kriminality. V celosvetovom meradle je počet obetí počítačovej kriminality viac ako milión ľudí denne. Ide o výnosnejší druh kriminality ako celosvetový obchod s marihuanou, kokaínom a heroínom dohromady. Je mimoriadne široká, zahŕňa napríklad *hacking*, *cracking*, *warez*, *phishing*, *sniffing* či *skimming*. Ide o trestnú činnosť, ktorá bežnému človeku mnoho nevraví. V mnohých prípadoch je veľmi sofistikovaná a jej objasnenosť hraničí s nulou.

Pojem **počítačová kriminalita** má niekoľko alternatív v slovenskom jazyku – napríklad **kybernetická kriminalita** alebo **kyberkriminalita**. V anglickom jazyku nachádzame oveľa viac alternatív, napríklad *computer crime*, ktorý je časovo najstarším pojmom, alebo novšie alternatívy *cyber crime*, resp. *cybercrime* alebo *cyber-crime*, zriedkavo taktiež pojmy *high-tech crime*, *virtual crime* alebo výnimočne *e-crime*.

Za súčasného stavu poznania je definovanie počítačovej kriminality mimoriadne náročná úloha, ba priam nemožná. Praktickejšie je poukázať na **skupiny počítačových trestných činov**:

1. trestné činy, ktorých cieľom je počítač,
2. trestné činy, pri ktorých je počítač používaný ako nástroj na ich spáchanie,
3. trestné činy, pri ktorých má počítač len vedľajšiu príležitostnú úlohu pri ich páchaní.

Ad 1) V prvom prípade **je počítač cieľom či terčom útoku**. Konanie spočíva napríklad v prieniku do počítača za účelom „krádeže" dát, súborov či dokumentov, v neoprávnenom zásahu do informačných systémov alebo aj vo vydieraní založenom na hrozbách zo zverejnenia odcudzeného obsahu. V tomto prípade dochádza k neoprávanému prístupu k počítaču, t. j. k hackerstvu. Keďže počítač je majetkom/vlastníctvom, neoprávnený prístup k počítaču je podobný nepovolenému vkročeniu na cudzí pozemok. Avšak, kým neoprávnené vkročenie na cudzí pozemok či do obydlia sa týka reálneho sveta, neoprávnený prístup k cudziemu počítaču sa týka kyberpriestoru. V princípe túto skupinu trestných činov možno prirovnať k barbarstvu.

Ad 2) V prípade trestných činov, pri ktorých **počítač je používaný ako nástroj**, počítač slúži ako pomocník na uľahčenie trestnej činnosti. Ide napríklad o falšovanie peňazí, falšovanie úradných listín, výroba a distribúcia detskej pornografie na internete, porušovanie autorských práv výrobou nelegálnych kópií hudobných CD nosičov, filmových nosičov v najrôznejších podobách – DVD disk, HD DVD disk, Blu-ray disk alebo v neposlednom rade ide o výrobu nelegálnych kópií počítačových programov.

Ad 3) V poslednom prípade, keď **počítač má len vedľajšiu príležitostnú úlohu pri páchaní trestných činov**, počítač zohráva malú úlohu a nie je potrebný na spáchanie trestného činu. Príkladom je napísanie vydieračského alebo výhražného listu, ktorý je napísaný na počítači, ale mohol byť napísaný aj na písacom stroji alebo rukou, taktiež ohováranie prostredníctvom internetu,

ekonomická kriminalita či ilegálny predaj drog prostredníctvom internetu. Táto skupina počítačových trestných činov nepredstavuje počítačovú kriminalitu v pravom slova zmysle.

12.2 Právna úprava

Práva úprava EÚ v oblasti počítačovej kriminality sa týka štyroch oblastí, a to a) podvody a falšovanie bezhotovostných platobných prostriedkov, b) útoky na informačné systémy, c) detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia a d) porušovanie právnej ochrany počítačových programov. Podvody a falšovanie bezhotovostných platobných prostriedkov sú upravené v samostatnej kapitole ako samostatný európsky trestný čin (bližšie pozri kapitolu 11). Detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia sú upravené taktiež v samostatnej kapitole (bližšie pozri kapitolu 7). Právna úprava porušovania právnej ochrany počítačových programov (smernica 2009/24/ES o právnej ochrane počítačových programov) neobsahuje sama osebe trestnoprávne prvky. V dôsledku toho sa nasledujúci text tejto kapitoly zameriava len na útoky na informačné systémy.

Vedúcim právnym predpisom EÚ ochrany proti útokom na informačné systémy je **smernica 2013/40/EÚ o útokoch na informačné systémy**. Táto smernica vymedzuje trestné činy a sankciie v oblasti útokov na informačné systémy. Jej cieľom je tiež uľahčiť predchádzanie takýmto trestným činom a zlepšiť spoluprácu medzi justičnými a inými príslušnými orgánmi.

Smernica chráni **informačný systém**. Na účely smernice sa ním rozumie zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje podľa programu, ako aj počítačové údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby [čl. 2 písm. a) smernice 2013/40/EÚ]. Príkladom môže byť internetové bankovníctvo banky alebo univerzitný informačný systém, ktorý slúži na internú potrebu zamestnancov, ale aj študentov danej inštitúcie. Aj napriek tomu, že ich účelom je zjednodušenie a zefektívnenie komunikácie, nie všetci ich vnímajú rovnako. Na jednej strane, väčšina ľudí ich používa spôsobom, ktorý je im prínosný a zároveň pre iných nezávadný. Na druhej strane, možno sa stretnúť aj so škodlivými útokmi na informačné systémy. Úmyselne

škodlivé útoky môžu mať mnoho podôb, napríklad neoprávnený prístup, t. j. hackerstvo, alebo šírenie škodlivého kódu (vírusov).

Smernica zohľadňuje nové metódy páchania počítačových trestných činov, najmä použitie botnetov. Tie sú v poslednom období pravdepodobne najväčšou hrozbou, ktorej čelí internet, ako aj jeho bezpečnosť. Pojem „botnet" je pomenovaním siete „robotov-počítačov", ktoré boli infikované škodlivým počítačovým vírusom. Vírus sa za účelom preniknutia dostane do počítača veľmi jednoducho, ak počítač nie je zabezpečený ochrannými mechanizmami (napr. antivírusový systém alebo „FireWall"). Pojem „botnet" pramení v anglickom jazyku. Je spojením slov *bot* a *net* ako skrátený tvar spojenia *robot network* alebo *network of robots*. Slovo *bot* je skrátený tvar slova robot, čo v slovenskom jazyku znamená rovnomenné pomenovanie robot a *net* je skrátený tvar slova *network*, čo v slovenskom jazyku znamená sieť. Infikovaný počítač je pomenovaný ako *bot* alebo v nedávnej minulosti *zombie*. Takéto siete sú riadené a kontrolované iným počítačom, často aj bez vedomia ich užívateľov. Osoba, ktorá ho riadi a kontroluje, je pomenovaná ako *bot herder* alebo *bot master*.

Sieť botnet môže byť aktivovaná na vykonávanie špecifických činností. Každý počítač siete môže pracovať samostatne, napríklad za účelom krádeže osobných údajov z počítača ako sú e-mailové adresy, heslá, údaje týkajúce sa licencií k počítačovým programom počítača, údaje k elektronickému bankovníctvu a pod. Počítače môžu pracovať taktiež spolu, napríklad zasielaním záplav správ alebo dát za účelom „odmietnutia služby", čím sa sleduje ohrozenie internetovej stránky. Ohrozenie spočíva v tom, že napadnutá stránka je nefunkčná alebo nedostupná pre užívateľov internetu. Iným účelom je odosielanie spamu prostredníctvom e-mailu. Takmer všetok spam pramení práve z činnosti botnetov. Omnoho závažnejšou činnosťou sú podvody s kreditnými kartami či útoky na informačné systémy.

Je ťažké definovať takéto siete čo do veľkosti, avšak boli spozorované siete s odhadom 40 000 až 100 000 infikovaných počítačov za 24 hodín (počet pripojení za 24 hodín je bežne používaná meracia jednotka na odhad veľkosti botnetov). Možno teda konštatovať, že útoky sú rázne. Osoby, ktoré riadia a kontrolujú botnety, majú byť považované za páchateľov trestného činu.

Smernica dopĺňa už pred ňou existujúce medzinárodné nástroje. Smernica nadväzuje na Dohovor o počítačovej kriminalite z roku 2001, prijatý Radu Európy. Tento dohovor je na medzinárodnej úrovni považovaný za najúplnejšiu

súčasnú medzinárodnú normu v oblasti boja proti počítačovej kriminalite. Poskytuje komplexný a ucelený rámec zahŕňajúci viaceré aspekty počítačovej kriminality v medzinárodnom európskom kontexte.

12.3 Vymedzenie trestných činov

Smernica 2013/40/EÚ o útokoch na informačné systémy predstavila konkrétne **trestné činy týkajúce sa informačných systémov**, a to:

- protiprávny prístup do informačných systémov,
- protiprávny zásah do systému,
- protiprávny zásah do údajov a
- protiprávne zachytávanie údajov.

Na druhej strane, je vhodné vopred poukázať, že smernica neukladá trestnoprávnu zodpovednosť v prípadoch, keď trestné činy v nej vymedzené sú spáchané, ale boli spáchané bez úmyslu. Príkladom je, ak osoba nevie o neoprávnenosti prístupu alebo v prípade povereného testovania alebo ochrany informačných systémov, napríklad ak osobu poverí spoločnosť alebo predajca, aby otestovala silu jej bezpečnostného systému.

12.3.1 Protiprávny prístup do informačných systémov

Protiprávny prístup do informačných systémov je *hacking* resp. hackerstvo. *Hacking* je najstarším spôsobom páchania počítačovej kriminality. Ide o neoprávnené preniknutie do cudzieho systému (napr. počítačového, informačného, riadiaceho) inou ako štandardnou cestou, a to prostredníctvom prelomenia alebo obídenia jeho bezpečnostnej ochrany. Pre jeho páchateľov – hackerov – často nie je ničím iným ako intelektuálnou výzvou. Obeťami hackingu boli napríklad Pentagon, NASA, Yahoo či Google. V Slovenskej republike bolo najznámejšou kauzou hackerstva preniknutie do systému Národného bezpečnostného úradu Slovenskej republiky, teda ostro výsmešná kauza prelomenia hesla „nbusr123".

V zmysle smernice za trestný čin je považované úmyselné získanie prístupu do celého informačného systému alebo akejkoľvek jeho časti bez oprávnenia, ak bolo spáchané porušením bezpečnostného opatrenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

Konaním bez oprávnenia sa na účely smernice rozumie konanie vrátane prístupu, zásahu alebo zachytávania údajov, ktoré nie je povolené zo strany vlastníka či iného držiteľa práv systému alebo jeho časti alebo ktoré nie je povolené vnútroštátnym právom.

Za menej závažný prípad sa má považovať, keď došlo k protiprávnemu prístupu menšieho významu alebo keď porušenie dôverného charakteru informačného systému je menšieho stupňa. Ide o možnosť uplatnenia materiálneho korektívu.

12.3.2 Protiprávny zásahu do systému

V prípade protiprávneho zásahu do systému, ktorého zmyslom je ochrana celistvosti informačných systémov, za trestný čin je považované úmyselné závažné bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania vložením počítačových údajov, prenosom, poškodením, vymazaním, zhoršením, pozmenením alebo potlačením takýchto údajov alebo ich zneprístupnením bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

Za menej závažný prípad sa má považovať, keď samotný zásah do systému má menší význam alebo keď sa do celistvosti informačného systému zasiahlo len v menšej miere. Aj tu ide o možnosť uplatnenia materiálneho korektívu.

12.3.3 Protiprávny zásah do údajov

V prípade protiprávneho zásahu do údajov je za trestný čin považované úmyselné vymazanie, poškodenie, zhoršenie, pozmenenie, potlačenie počítačových údajov v informačnom systéme alebo zneprístupnenie takýchto údajov bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

12.3.4 Protiprávne zachytávanie údajov

V neposlednom rade, za trestný čin je považované taktiež úmyselné zachytávanie údajov prostredníctvom technických prostriedkov, neverejného prenosu počítačových údajov do informačného systému, z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému

nesúceho takéto počítačové údaje, ak je spáchané bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 6 smernice 2013/40/EÚ].

Zachytávanie zahŕňa získavanie obsahu údajov buď priamo, a to prostredníctvom prístupu a využívania informačného systému, alebo nepriamo, a to prostredníctvom využívania elektronického odpočúvania alebo odpočúvacieho zariadenia technickými prostriedkami.

Kapitola 13

ORGANIZOVANÁ TRESTNÁ ČINNOSŤ (ORGANIZOVANÁ KRIMINALITA)

13.1 Úvod

Páchatelia trestných činov sa neraz zoskupujú do organizovaných skupín, čím vytvárajú organizovanú trestnú činnosť, ktorá v porovnaní so „sólo páchateľom" je omnoho efektívnejšia.

Najzávažnejšie organizované skupiny pochádzajú napríklad z Ruska, Talianska, Spojených štátov amerických, Číny, Japonska, Mexika, Izraela či Kolumbie. Ako najznámejšie organizované skupiny možno uviesť napríklad talianskú skupinu Cosa Nostra, japonskú Yakuzu, čínske Triády alebo „ruskú mafiu". Niektoré organizácie majú dlhú tradíciu – napríklad história Yakuzy siaha až do 17. storočia. V extrémnom prípade, počet členov organizácií presahuje aj stotisíc členov. Neobmedzujú sa len na jednu krajinu, ale ich aktivity sa prejavujú aj v medzinárodnom rozmere. Napríklad talianska Cosa Nostra pôsobí aj v Spojených štátoch amerických, čínske Triády v Európe alebo „ruská mafia" pôsobí v desiatkach krajín celého sveta.

Organizovaná trestná činnosť sa prejavuje najmä v oblastiach, ktoré sú finančne výnosné. Ide spravidla o výrobu a obchodovanie s drogami, obchodovanie s ľuďmi, sexuálne vykorisťovanie žien na účely prostitúcie, obchodovanie so zbraňami a muníciou, obchodovanie s kradnutými autami, obchodovanie s diamantmi a drahými kovmi, pašovanie cigariet, falšovanie peňazí, vydieranie/výpalníctvo či podvody najrôznejšieho charakteru. V neposlednom rade ide aj o pranie špinavých peňazí, ktorým organizované skupiny legalizujú svoje nelegálne príjmy, napríklad v reštauračných zariadeniach, disco podnikoch alebo v hoteloch, ktoré vykazujú neexistujúce tržby, resp. faktúry za neexistujúce služby.

Ak organizovaná trestná činnosť nadobúda cezhraničný rozmer, môže byť prirovnávaná k **medzinárodnému podnikaniu**. Spoločným im je cieľ – dosahovanie zisku bez obmedzenia aktivít len v jednej krajine. Avšak zásadným rozdielom medzi nimi je spôsob k jeho dosiahnutiu – organizované skupiny nie sú

vždy viazané zákonnými spôsobmi výkonu ich činností. Navyše, berúc do úvahy nemožnosť obmedzení monopolov či zdanenia ich ziskov, sú v značnej výhode.

Do polovice 80-tych rokov minulého storočia bola organizovaná trestná činnosť považovaná za problém, ktorý sa týkal len obmedzeného počtu krajín – predovšetkým Spojených štátov amerických a Talianska, s eventuálnym pridaním Japonska, Číny a Kolumbie. O dvadsať rokov neskôr sa obraz organizovanej trestnej činnosti dramaticky zmenil.

Zmeny sa prejavili aj v Európe. V rámci EÚ malo vplyv na rozmach organizovanej trestnej činnosti dokončenie vnútorného trhu a zrušenie kontrol na vnútorných hraniciach. Tým bol organizovaným skupinám uľahčený pohyb v rámci celej EÚ a taktiež došlo k otvoreniu priestoru pre ich nelegálne aktivity. Okrem toho, po páde železnej opony v roku 1989 sa otvorili územia ďalších krajín, najmä v strednej Európe vrátane Slovenskej republiky.

V súčasnosti na európskom území vykonávajú svoje aktivity rôzne organizácie – napríklad v Holandsku skupiny zaoberajúce sa drogami, v Nemecku skupiny zaoberajúce sa nelegálnym prisťahovalectvom, v Poľsku skupiny zaoberajúce sa prepravou kradnutých áut z Nemecka do Ruska alebo v Litve skupiny pašujúce cigarety z Ukrajiny do baltických a nordických krajín. Možno hovoriť aj o organizáciách z neeurópskych krajín, ktoré v Európe pôsobia – napríklad čínske Triády alebo ruská mafia.

Boj proti organizovanej trestnej činnosti nie je jednoduchý. Dosiaľ si vyžiadal nemálo ľudských obetí. Známymi príkladmi sú talianski sudcovia Giovanni Falcone a Paolo Borsellino, aktívne bojujúci proti Cose Nostre, ktorí boli v roku 1992 obeťami bombových atentátov.

V rámci legislatívnej činnosti EÚ boli prijaté legislatívne akty za účelom boja proti organizovanej trestnej činnosti. Možno hovoriť napríklad o obchodovaní s ľuďmi, obchodovaní s drogami alebo o praní špinavých peňazí. Tieto oblasti spadajú do oblasti európskych trestných činov a sú spracované v samostatných kapitolách tejto učebnice. Avšak ako samostatný trestný čin je považovaná už len samotná účasť v zločineckej organizácii.

13.2 Právna úprava

Vedúcim právnym predpisom EÚ v boji proti organizovaným zločineckým skupinám je **rámcové rozhodnutie 2008/841/SVV o organizovanom zločine**.