PRÁVNE ROZPRAVY ON-SCREEN III. – Sekcia verejného práva
online vedecká konferencia – 7. máj 2021

ODHAĽOVANIE POČÍTAČOVEJ KRIMINALITY PRI VEREJNOM OBSTARÁVANÍ A OCHRANE HOSPODÁRSKEJ SÚŤAŽE
DETECTION OF CYBERCRIME IN PUBLIC PROCUREMENT AND PROTECTION OF COMPETITION

Daniel Blaško[1]

https://doi.org/10.24040/pros.07.05.2021.svp.108-121

Abstrakt

Termínom počítačová kriminalita sa označujú trestné činy zamerané proti počítačom ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužívanie elektronických informácií získaných prostredníctvom výpočtovej techniky. Príspevok sa zaoberá novými trendmi v oblasti počítačovej kriminality a taktiež odhaľovaním počítačovej kriminality pri verejnom obstarávaní a ochrane hospodárskej súťaže.

Kľúčové slová

Počítačová kriminalita, spôsoby páchania kriminality, verejné obstarávanie, ochrana hospodárskej súťaže

Abstract

The term cybercrime refers to crimes against computers as well as crimes committed using a computer. This is illegal, immoral and unauthorized conduct, which involves the misuse of electronic information obtained through computer technology. The paper deals with new trends in the field of cybercrime and also the detection of cybercrime in public procurement and protection of competition.

Key words

Computer crime, ways of committing crime, public procurement, protection of competition

Úvod

Počítačová kriminalita je relatívne novým druhom závažnej trestnej činnosti. Od klasickej kriminality sa odlišuje celým radom osobitných charakteristík a zvláštností. Trestný čin môže byť spáchaný v anonymite na diaľku, sprostredkovane a to všetko v priebehu niekoľkých sekúnd bez toho, aby poškodený zaregistroval spáchanie takéhoto trestného činu a niekedy sa o tom vôbec dozvedel. Internet, anonymita a nedostatočná legislatíva, robia

[1] Ing. Bc. Daniel Blaško, Právnická fakulta Univerzity Mateja Bela v Banskej Bystrici, dblasko@student.umb.sk

z počítačovej kriminality mocný nástroj na páchanie domácich a medzinárodných trestných činov veľakrát závažného charakteru s priamym dopadom na ekonomiku krajiny a jej bezpečnosť.

Počítačové systémy ponúkajú nové a vysoko sofistikované možnosti porušovania práva a predovšetkým potenciálu pre páchanie tradičných typov zločinov netradičnou cestou.

Počítačovým systémom sa podľa Dohovoru o kybernetickej kriminalite (Convention on Cybercrime; ďalej ako „Dohovor“) rozumie akékoľvek zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracovanie dát. Je to teda súbor technického a programového vybavenia (rozumej hardware a software), ktoré je určené ku spracovaniu dát bez priameho ľudského zásahu.[2]

Termínom počítačová kriminalita sa označujú trestné činy zamerané proti počítačom ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Počítače v podstate neumožňujú páchať nový typ trestnej činnosti, iba poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je sabotáž, krádež, zneužitie, neoprávnené užívanie cudzej veci, vydieranie alebo špionáž.[3]

Druhy počítačovej kriminality

Vzhľadom na široké pole nasadenia a používania výpočtovej techniky v rôznych oblastiach je ťažké reálne zmapovať a popísať všetky prejavy počítačovej kriminality.

Všeobecne sa jedná o tieto kategórie:

1. *Útok na počítač, program, údaje, komunikačné zariadenie:* fyzické útoky na zariadenie výpočtovej techniky, magnetické médiá, vedenie počítačovej siete alebo elektrického rozvodu a pod., vymazanie alebo pozmenenie dát, formátovanie pamäťových médií nesúcich dáta, pôsobenie počítačových infiltrácií, nelegálna tvorba a rozširovanie kópií programov, získanie kópie hospodárskych dát, databáz zákazníkov, v štátnych orgánoch únik informácií o občanoch a pod. Z hľadiska rozsahu najväčších škôd pravdepodobne

[2] Dohovor Rady Európy č. 185 z dňa 23.11.2001 o počítačovej kriminalite. [cit. 17. 4. 2021] Dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
[3] MATĚJKA, M.: Počítačová kriminalita. Praha: Computer Press, 2002, s. 11.

najväčší podiel patrí nelegálnej tvorbe a predaju autorsky chráneného programového vybavenia v počítačovom slangu označovaná ako Warez.

2. *Neoprávnené užívanie počítača alebo komunikačného zariadenia:* využívanie počítačovej techniky, faxov, prostriedkov počítačových sietí, databáz a programov zamestnancami firiem a organizácií na vlastnú zárobkovú činnosť.
3. *Neoprávnený prístup k údajom, získanie utajovaných informácií (počítačová špionáž) alebo iných informácií o osobách, činnosti a pod.:* prenikanie do bankových systémov, systémov národnej obrany, do počítačových sietí dôležitých inštitúcií a pod. Niekedy táto činnosť spôsobuje priame škody veľkého rozsahu, napr. nelegálne bankové operácie, ako aj nepriame škody spôsobené únikom informácií. V súvislosti s týmto trestným činom môže byť aj súbežný trestný čin ako napr. vydieranie, nekalá súťaž, ohrozenie hospodárskeho tajomstva, vyzvedačstvo, ohrozenie štátneho tajomstva.
4. *Krádež počítača, programu, údajov, komunikačného zariadenia zmena v programoch a údajoch (okrajovo i v technickom zapojení počítača resp. komunikačného zariadenia):* zmena programov a údajov inými programami alebo priamymi zásahmi programátora, úprava v zapojení alebo inom atribúte technického vybavenia počítača.[4]
5. *Zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti:* manipulácia s údajmi ako napr. zostavy v skladoch, tržby, nemocenské poistenie, stavy pracovníkov, stav účtov a pod., patria sem aj krádeže motorových vozidiel, falšovanie technickej dokumentácie, priekupníctvo, daňové podvody, falšovanie a pozmeňovanie cenín, úradných listín a dokladov, dokonca aj peňazí.
6. *Podvody páchané v súvislosti s výpočtovou technikou:* využitie niečieho omylu vo svoj prospech (hry s vkladom finančnej čiastky a rozosielaním listov "následníkom" so sľubom zaručeného zisku). Tento druh trestnej činnosti možno vykonávať aj bez použitia výpočtovej techniky, ale s jej použitím je táto činnosť efektívnejšia.
7. *Šírenie poplašných správ:* vytvorenie poplašnej správy upozorňujúcej na fiktívne nebezpečenstvo. Najčastejším motívom páchateľov tejto trestnej činnosti je pobaviť sa na nevedomosti ostatných, no môže ísť i o správy spojené s páchaním inej trestnej činnosti. Tieto správy sú v počítačovom slangu označovaná ako Hoax.[5]

[4] ČERMÁK, J.: Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent a přihlédnutím k rozsudku ve věci The Pirate Bay. In: Právní rozhledy. 2008, č.8.
[5] BRVNIŠŤAN, M.: Bezpečnostné povedomie v kontexte boja proti novodobým bezpečnostným hrozbám. In: Zborník príspevkov z IX. medzinárodnej vedeckej konferencie v Banskej Bystrici 11. – 12. februára 2016. Banská Bystrica: Fakulta politických vied a medzinárodných vzťahov UMB, 2016, s. 520-530.

Spôsoby páchania počítačovej kriminality

Spôsoby páchania počítačovej kriminality môžeme rozdeliť do troch kategórií a to ako protiprávne konanie smerujúce k počítaču, protiprávne konanie páchané pomocou počítača a protiprávne konanie, pri ktorom vystupuje počítač ako vedľajší prvok.

Protiprávne konanie smerujúce k počítaču

Ide o protiprávne konanie špecificky zamerané na počítač ako objekt, proti ktorému je vedené takéto konanie. Takéto správanie možno rozdeliť do viacerých kategórií napríklad ako ilegálny prístup, nelegálne odchytávanie komunikácie, zasahovanie do dát, zasahovanie do systémov a zneužitie zariadení podľa definície Dohovoru rady EU o počítačovej kriminalite.

Niektoré z vyššie uvedených spôsobov konania sa dajú prirovnať k tradičným spôsobom protiprávneho konania zahŕňajúcim predmet ako fyzický objekt ako napríklad krádež, poškodzovanie cudzej veci alebo narúšanie práv na súkromie. Tieto nové spôsoby protiprávneho konania zastrešujú nehmotnú povahu dát a služieb na počítačoch. Možným motívom páchateľov týchto trestných činov býva vidina peňažného zisku, vandalizmus, vydieranie, odplata a ďalšie dôvody. Pri trestných činoch proti počítaču spáchaných pomocou internetu alebo pomocou iných technických prostriedkov sa vyžaduje aj určitá miera technickej znalosti páchateľa a nakoľko sú tieto trestné činy relatívne nové a existujú len tak dlho ako aj počítače samotné, táto skutočnosť aj vysvetľuje nepripravenosť ľudí a spoločnosti voči týmto trestným činom. Protiprávne konanie smerujúce proti počítaču, ale taktiež môže predstavovať tradičnejšie trestné činy ako krádež alebo poškodzovanie cudzej veci, v tomto prípade môže konanie smerovať aj proti softvéru ale aj hardvéru počítača. Ďalším cieľom takéhoto správania môžu byť telefonické alebo dátové prenosy a zariadenia, ktoré môžu byť ukradnuté alebo zneužité na iné účely.[6]

[6] IVOR, J. – POLÁK, P. – ZÁHORA, J. Trestné právo procesné I. Bratislava: Wolters Kluwer, 2017.

Protiprávne konanie s využitím počítača

Ide o protiprávne konanie, kde počítač vystupuje ako nástroj pomocou ktorého je páchaná trestná činnosť. Toto protiprávne konanie je väčšinou smerované voči konkrétnemu jednotlivcovi. V takýchto prípadoch sa väčšinou nevyžaduje väčšie technické vzdelanie na páchanie takejto činnosti, nakoľko ide o konanie, ktoré existovalo už dlho predtým ako prišiel internet a počítače. Ide hlavne o podvody a krádeže kde sa využíva ľudská neskúsenosť. Tí istí kriminálnici takto získali nové nástroje na páchanie trestnej činnosti, pomocou ktorých sa zvýšil ich dosah na obete a sťažila sa možnosť ich dostihnutia.[7]

Protiprávne konanie, pri ktorom vystupuje počítač ako vedľajší prvok

Pri takomto spôsobe konania počítač nevystupuje ako cieľ alebo prostriedok na páchanie trestnej činnosti ale iba ako pomôcka pri páchaní inej trestnej činnosti, napríklad na uchovávanie dát a údajov, fotografií a podobne. Môže ísť o počítače, mobilné telefóny a ďalšiu technológiu, ktorú u seba mali páchatelia alebo obete trestných činov.[8]

Súčasné trendy v oblasti počítačovej kriminality

Rýchly vývoj informačných technológií, počítačový vek svetovej spoločnosti spolu s pozitívnymi trendmi, dávajú priestor na vývin a zlepšenia v kriminálnej sfére, kriminalizuje spoločenské právne vzťahy. Počítačovo orientovaná kriminalita sa presadzuje čoraz viac. Oblasť IT neposkytuje možnosti len na tradičné druhy kriminality ako sú krádeže a podvody, sprenevery, pranie peňazí , falšovanie dokumentov vrátane šekov, ale vytvára i druhy nové, ako sú neoprávnené používanie cudzích informácií, počítačové falzifikáty, počítačové podvody, atď. Pojmy ako počítačová informácia, počítačová kriminalita, kyber terorizmus a informačné zbrane sú počuť čoraz častejšie. Počítače sa stali súčasťou našich domovov, niektorí z nás si bez nich už nevieme ani predstaviť svoj každodenný život.[9]

[7] KRÁL, M.: Bezpečnost domácího počítače. Praha: Grada, 2006, s. 34.
[8] KURILOVSKÝ, R. Vyšetrovanie počítačovej kriminality. In: Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie. Bratislava: APZ, 2018, s. 162-171.
[9] KURILOVSKÝ, R. Vyšetrovanie počítačovej kriminality. In: Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie. Bratislava: APZ, 2018, s. 162-171.

Počítačoví zločinci dneška už nie sú iba nadšencami, ktorí potrebujú niekomu niečo dokazovať. Dnes sa už organizujú do skupín za účelom obohatenia sa na úkor iných a to spôsobom, ktorí nie je nikde v civilizovanom svete našťastie akceptovaný.[10]

Legislatívny rámec verejného obstarávania v SR

Oblasť verejného obstarávania je pre svoj význam veľmi často dávaná do centra pozornosti. Požiadavka existencie funkčného systému verejného obstarávania bola jednou z prioritných oblastí v procese približovania sa Slovenska k Európskej únii.

Zákon o verejnom obstarávaní bol na Slovensku, ako v prvej postkomunistickej krajine vypracovaný v jednoduchej forme na základe odporúčaného Model Law UNESCO v roku 1993. V roku 1999 bol prepracovaný s prihliadnutím na osnovu a terminológiu smerníc Európskej Únie o verejnom obstarávaní.

Platný zákon o verejnom obstarávaní – zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej len zákon o verejnom obstarávaní), je od vzniku Slovenskej republiky v poradí už piatou právnou úpravou tohto inštitútu. Pravidlá verejného obstarávania boli v našich podmienkach prvý krát uplatňované roku 1994, kedy nadobudol účinnosť zákon č. 263/1993 Z. z. o verejnom obstarávaní tovarov, služieb a verejných prác. Vzhľadom na to, že išlo o prvú právnu úpravu tohto inštitútu, bola zvolená čo najjednoduchšia forma zákona s dôrazom na základné princípy verejného obstarávania, ako napríklad transparentnosť a nediskriminácia. Zároveň bol v roku 1996 prijatý zákon NR SR č. 119/1996 Z. z. o koncesnom obstarávaní. Nasledovala právna úprava v podobe zákona č. 263/1999 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, ktorá predstavovala významný posun v uplatňovaní pravidiel verejného obstarávania v súlade so smernicami Európskych spoločenstiev pre túto oblasť. V poradí tretím zákonom venujúcim sa verejnému obstarávaniu od vzniku Slovenskej republiky bol zákon č. 523/2003 Z. z. o verejnom obstarávaní a o zmene zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, ktorý nadobudol účinnosť 1. januára 2004. Táto právna úprava bola plne aproximovaná s vtedy platnými smernicami ES upravujúcimi túto oblasť.

[10] GŘIVNA, T.: Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – iuridica 4, 2008, s. 21-34.

Nové smernice, ktoré boli prijaté Európskym parlamentom dňa 31. marca 2004, boli dôvodom na prijatie aktuálneho zákona o verejnom obstarávaní. Boli to smernice:

- smernice 2004/17/ES o koordinácii postupov obstarávania subjektov pôsobiacich v odvetviach vodného hospodárstva, energetiky, dopravy a poštových služieb a
- smernice 2004/18/ES o koordinácii postupov pri zadávaní verejných zákaziek na práce , verejných zákaziek na dodávku tovaru a verejných zákaziek na služby.

Tým že boli prijaté nové smernice, musela Slovenská republika prebrať ich právnu úpravu do legislatívy o verejnom obstarávaní. Tým, že by bola prijatá novela pôvodného zákona o verejnom obstarávaní, by sa sťažila aplikácia tohto zákona. Práve preto sa riešenie našlo v úplne novej právnej úprave zákona 25/2006 Z. z., ktorý upravil postupy pre obstarávanie ako aj tzv. klasického sektora, tak aj postupy obstarávania vo vybraných odvetviach (vodne hospodárstvo, energetika a pod.). 18. novembra 2015 bol prijatý zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej len zákon o verejnom obstarávaní). Tento zákon upravuje zadávanie zákaziek na dodanie tovaru, zákaziek na uskutočnenie stavebných prác, zákaziek na poskytnutie služieb, súťaž návrhov, zadávanie koncesií na stavebné práce, zadávanie koncesií na služby a správu vo verejnom obstarávaní.

V Slovenskej republike je Úrad pre verejné obstarávanie príslušným štátnym orgánom vykonávajúcim dohľad nad verejným obstarávaním v súlade so zákonom o verejnom obstarávaní a zákonom o koncesnom obstarávaní. Rozhodnutia Úradu pre verejné obstarávanie sú preskúmateľné súdom. Podľa zákona o verejnom obstarávaní má Úrad pre verejné obstarávanie právo:

- preskúmavať sťažnosti a námietky účastníkov verejného obstarávania podané proti postupom a rozhodnutiam obstarávateľa;
  zrušiť alebo pozastaviť proces verejného obstarávania v prípade podania námietok voči činnosti obstarávateľa pri verejnom obstarávaní;
- napadnúť platnosť zmluvy, ktorú obstarávateľ uzavrel v rozpore s ustanoveniami zákona o verejnom obstarávaní pred príslušnými súdmi do jedného roka od uzavretia takejto zmluvy.

Kontrolný orgán vykonáva Najvyšší kontrolný úrad ale vystupuje tu aj faktor, ktorý si nie každý uvedomuje.

Európska únia má vytvorený svoj právny aj súdny systém. Pre každého člena únie sú záväzné direktívy, upravujúce verejné obstarávanie nad stanovenými finančnými limitmi. Nová smernica nastavila tieto limity relatívne nízko, a to najmä pre tovary a služby, kde je potrebné postupovať podľa nadnárodných pravidiel už od sumy 154-tisíc eur.

Únia predpisy nielen vydáva, ale ich nedodržiavanie aj trestá. Konanie pred Európskym súdnym dvorom v Haagu sa nevedú voči subjektom, ktoré priamo problém spôsobili, ale voči krajine. Slovensko už zaplatilo pomerne veľa prostriedkov za prieťahy v súdnom konaní. Tieto sumy sú ale maličkosťou oproti rizikám, ktoré vyplývajú z potenciálnych žalôb v oblasti verejného obstarávania.[11]

Kolúzia a indície protisúťažného správania z pohľadu podnikateľov pri verejnom obstarávaní

Elektronické trhovisko je zriadené na základe zákona č. 25/2006 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 25/2006 o verejnom obstarávaní"). V zmysle § 13 ods. 1 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“) ide o informačný systém verejnej správy, ktorý slúži na zabezpečenie ponuky a nákupu tovarov, stavebných prác alebo služieb, bežne dostupných na trhu, a to aukčným postupom, ako aj na zabezpečenie s tým súvisiacich činností. Elektronické trhovisko bolo zriadené 1. júla 2014, pričom prvý obchod sa na ňom uskutočnil 30. septembra 2014.

Pri verejnom obstarávaní sa podnikatelia opakovane stretávajú, čo im umožňuje dohodnúť si striedanie víťazstiev v tendroch. Proces je transparentný, čo na jednej strane umožňuje verejnú kontrolu, ale na druhej strane kartelistom uľahčuje sledovanie, či sa dohodnuté kartelové schémy dodržiavajú. Existencia protisúťažnej dohody sa dá ľahko utajiť a podnikatelia môžu vytvoriť zdanie, že existujú konkurenčné ponuky. Obstarávatelia nerozhodujú o vlastných peniazoch, preto nie sú prirodzene motivovaní a tlačení k získaniu najlepšieho výsledku pri obstarávaní a môžu byť menej senzitívni aj na odhaľovanie kartelových dohôd. Tieto faktory spôsobujú, že verejné obstarávanie je náchylné na kolúziu.

Kolúzia vo verejnom obstarávaní je dohoda medzi uchádzačmi v tendri, na základe ktorého je vopred dohodnutý víťaz. Pri protisúťažných dohodách ide o dohody medzi priamymi

[11] KLIMEK, L.: Základy trestného práva Európskej únie. Bratislava: Wolters Kluwer, 2017.

konkurentmi. Sú to najškodlivejšie protisúťažné praktiky, kedy vlastne verejné obstarávanie stráca svoj význam. Negatívne efekty takýchto dohôd majú za následok:

- umelý rast cien – čím sa podľa štúdií môže zvýšiť cena tovaru prác a služieb o viac ako 30 %,
- neefektívne využívanie verejných prostriedkov – ktoré mohli byť využité na iné projekty,
- negatívny dopad na podnikateľské prostredie – ktoré sa deformuje pri dlhodobej kartelizácii tendrov.

Každá kolúzia v sebe obsahuje systém rozdelenia dodatočných výnosov získaných ako výsledok vyššej ceny dosiahnutej koordináciou medzi uchádzačmi. Napr. uchádzači, ktorí súhlasili, že nepredložia svoje ponuky alebo predložia len krycie ponuky, môžu dostať subdodávky na danú zákazku alebo akúkoľvek inú dodávku pre úspešného uchádzača, aby si tak rozdelili nelegálne zisky. Bežne sa používajú aj priame platby od úspešného uchádzača pre neúspešných, tzv. kompenzačné platby. Tie sa vyplácajú na základe falošných subdodávateľských prác, čiže žiadne práce sa nevykonajú a faktúry za ne sú len fiktívne dohodnuté na základe podvodných konzultačných zmlúv a podobne. Avšak pri dlhotrvajúcich a rozsiahlejších dohodách môžu byť použité oveľa viac prepracovanejšie metódy rozdelenia ziskov. Tieto metódy môžu byť dlhodobo rozpracované na obdobie mesiacov alebo rokov.[12]

Tovary a služby, ktoré sú dodávané podnikateľmi sú určené jednak k všeobecnému používaniu (veľkoobchod a maloobchod), pričom v prípade obchodovania podlimitných zákaziek realizovaných s využitím elektronického trhoviska sú tieto tovary a služby určené pre konkrétne subjekty (predovšetkým nemocnice a iné zdravotnícke zariadenia, zariadenia sociálnych služieb, zariadenia vojenskej, colnej, väzenskej správy) a z uvedeného dôvodu sú tieto tovary a služby *„šité na mieru“* podľa požiadaviek a potrieb objednávateľa, ktorým môže byť zákazník tak z verejného, ako aj súkromného sektora.

Analýzou podlimitných zákaziek realizovaných s využitím elektronického trhoviska Protimonopolný úrad opakovanie a veľakrát v minulosti zistil, že medzi podnikateľmi mohlo dôjsť k uzatvoreniu dohody obmedzujúcej súťaž a/alebo k zosúladenému postupu, ktorý spočíval v koordinácii ich postupu v podlimitných zákazkách realizovaných s využitím

[12] LÁTAL, I.: Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*, 1998, č.3, příloha s. VIII. [cit. 16. 4. 2021] Dostupné z: http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html

elektronického trhoviska. V rámci spracovania analýzy Protimonopolný úrad a aj Úrad pre verejné obstarávanie zistili, že ponuky podnikateľov, ako aj spôsob ich predkladania, vykazuje také znaky podobnosti, ktoré vedú k pochybnosti o tom, či boli ponuky vypracované jednotlivými podnikateľmi nezávisle a bez vzájomnej koordinácie, komunikácie či konzultácie, a to predovšetkým pokiaľ ide o určenie cien obstarávaných tovarov a služieb, určenie účasti, resp. neúčasti podnikateľov v tendri, určenie víťaza tej ktorej podlimitnej zákazky a či nedochádzalo k následným kompenzáciám prostredníctvom subdodávok, či iným dohodnutým spôsobom, resp. či boli ponuky vyššie uvedených podnikateľov vypracované jednotlivými podnikateľmi bez inej koordinácie a komunikácie realizovanej či už priamo podnikateľmi alebo nepriamo prostredníctvom tretej osoby. Indície protisúťažného správania podnikateľov pri verejnom obstarávaní:

- prítomnosť „prieskumníka“ – systém určitej analýzy podnikateľskými subjektmi s cieľom zistiť, kde je hranica ceny pre postup do EA,
- blízke časy predkladania ponúk v prvom kole – zväčša ide o rozsah 3 až 10 sekúnd,
- blízke ceny/minimálne cenové rozdiel:
  - s ohľadom na výšku zákaziek a s ohľadom na čas, v ktorom predkladali uchádzači svoje ponuky sú ponuky uchádzačov, a účastníkov kartelovej dohody, a cenové rozdiely medzi nimi minimálne,
  - niektoré rozdiely predstavujú násobky (t.j. rozdiel medzi 1. a 2. je 0,50 a medzi 2. a 3. je 1), iné sa zvyšujú o rovnakú čiastku napr. 1),
  - vo väčšine prípadov však rozdiely nie sú násobkami či rovnakými navýšeniami ale sú veľmi blízke (napr. rozdiel 0,70 a 0,80, alebo rozdiel 0,35 a 0,70, atď.),
- často postupujú do druhého kola tí istí uchádzači a súčasne v druhom kole už uchádzači medzi sebou nesúťažia,
- ďalšou indíciou je rovnaká IP adresa súťažiacich.

V tejto súvislosti platí, že čím je zákazka viac nadhodnotená v porovnaní s reálnou trhovou cenou, tým atraktivita uzatvárania a realizovania kartelových dohôd stúpa, keďže členovia kartelovej dohody si rozdeľujú väčšiu sumu. V prípade kartelových dohôd totiž členovia kartelovej dohody vždy zvažujú potenciálne zisky z kartelovej dohody vo vzťahu k riziku možného odhalenia.

Organizácia pre hospodársku spoluprácu a rozvoj (OECD), ako aj Protimonopolný úrad už v minulosti upozorňovali na to, že predpokladaná cena zákazky by mala byť založená na

dôkladnom prieskume trhu a malo by ísť o skutočne konkurenčnú cenu. Iba ak je cena nastavená „agresívne“, môže obmedziť nelegálne zisky z kolúzie, a tým obmedzovať priestor pre kolúziu. Naopak, ak je nastavená „mäkko“, takýto priestor sa môže vytvoriť. Tieto pravidlá by sa mali aplikovať aj na určenie „maximálnej výšky zdrojov“, nakoľko stanovenie tejto veličiny má výrazný vplyv na zadanie vstupnej ceny uchádzačov a v konečnom dôsledku môže ovplyvniť aj vysúťaženú (zazmluvnenú) cenu zákazky. V tejto súvislosti nemožno opomenúť ani skutočnosť, že porovnanie viacerých súm uvedených ako „maximálna výška zdrojov“ a v niektorých prípadoch dokonca aj vysúťažených (zazmluvnených) cien demonštruje, že „maximálna výška zdrojov“, či dokonca vysúťažená (zmluvná) cena získaná v rámci verejného obstarávania s využitím elektronického trhoviska je skutočne v niektorých prípadoch vyššia, resp. výrazne vyššia ako trhová cena. Aj správca elektronického trhoviska v časti „Najčastejšie chyby objednávateľov“ upozorňuje, že neuvedenie „maximálnej výšky zdrojov“ môže mať za následok predloženie neprimerane vysokej cenovej ponuky, ktorá nebude znížená ani v elektronickej aukcii, avšak nezavádza žiadne opatrenia na eliminovanie takýchto situácií. Je zrejmé, že ak dodávatelia identifikujú, že stanovená „maximálna výška zdrojov“ prevyšuje trhovú cenu, ich záujem koordinovať svoje správanie vo verejnom obstarávaní stúpa.

Možnosť získať zákazku s vyšším ziskom môže niektorých podnikateľov motivovať do takej miery, že prospech z kartelového správania preváži nad možným rizikom z jeho odhalenia. Preto v záujme systému elektronického trhoviska a rovnako vo verejnom záujme je nutné, aby bolo obchodovanie na elektronickom trhovisku nastavené tak, aby prispievalo k zníženiu rizika uzatvárania kartelových dohôd na elektronickom trhovisku.

Záver

Počítačová kriminalita je relatívne nový druh kriminality vstupujúci do popredia hlavne v posledných desaťročiach, pričom každým rokom môžeme sledovať jej nárast a hlavne posuny v postupoch a formách jej páchania. Rýchlosť rozvoja informačných technológií a počítačových systémov je tak dynamický, že zasa na opačnej strane znemožňuje zákonodarcovi pružne na ňu reagovať a zároveň orgánom činným v trestnom konaní tento jav potierať. Tieto dva aspekty robia z počítačovej kriminality fenomén hodný pozornosti a hlbšieho spracovania.

Masová dostupnosť počítačov a iných podobných zariadení, ich klesajúca cena a pomerne sa zvyšujúci výkon umožňujú čím ďalej tým väčšej skupine obyvateľstva prísť do

styku s týmto druhom kriminality a to ako na strane páchateľa tak aj na strane obete. Preto je nutné aktivizovať prevenčné opatrenia a výchovne pôsobiť na obe strany, a tak aspoň čiastkovo prispievať k redukcii protiprávnych jednaní v kyberpriestore. Rolu, ktorú v týchto vzťahoch hrá Internet tiež nemožno opomenúť. Ten v podstate búra hranice štátov a prakticky zoskupuje celý svet na jednom mieste. Preto je aktívny boj proti počítačovej kriminalite otázkou viac medzinárodnou ako národnou, čo dokladajú aj silnejúce snahy po regulácií prostredníctvom medzinárodných dohôd. Úplný konsenzus je však len ťažko dosiahnuteľný a to s ohľadom na rôznorodé postoje jednotlivých štátov k potrebe kriminalizácie a trestnoprávneho postihu jednotlivých jednaní. To je najviac viditeľné práve v prípade problému pôsobnosti trestného práva v kyberpriestore, ktorý tvorí závažnú prekážku v činnosti orgánov činných v trestnom konaní pri vyšetrovaní a postihovaní páchateľov.

Proces verejného obstarávania je nastavený tak, že simuluje podmienky súťaže v klasickom trhovom prostredí. Podnikatelia v tendri teda podávajú súťažné ponuky s cieľom vyhrať. Za účelom dosiahnutia lepšej hodnoty za peniaze je však nevyhnutné, aby uchádzači súťažili reálne. Verejné obstarávania (nielen na elektronickom trhovisku, ale všeobecne) by mali byť navrhované tak, aby maximalizovali účasť skutočne si konkurujúcich uchádzačov. Prax ukazuje, že vo viacerých prípadoch sa verejných obstarávaní zúčastňujú majetkovo alebo personálne prepojené osoby. Ide napríklad o situácie, keď majetkové alebo personálne prepojenia medzi podnikateľmi umožňujú niektorému z nich vykonávať rozhodujúci vplyv nad činnosťou iného podnikateľa. V takomto prípade vytvárajú subjekty jednu ekonomickú skupinu a vzťah vzájomnej závislosti môže mať vplyv na ich správanie v rámci príslušného verejného obstarávania. Účasť personálne alebo majetkovo prepojených subjektov na procese verejného obstarávania pritom môže oslabovať alebo úplne eliminovať intenzitu súťaže medzi uchádzačmi. Predkladanie ponúk zo strany personálne alebo majetkovo prepojených subjektov tak v niektorých prípadoch vyvoláva iba zdanie súťaže vo verejnom obstarávaní, no jednotliví uchádzači nepodávajú také ponuky, ktoré by boli nezávislé od iných uchádzačov, ale práve naopak, ponuky uchádzačov sú výsledkom dohody, konzultácie alebo komunikácie s inými uchádzačmi.

V dôsledku takéhoto podávania súťažných ponúk sa verejní obstarávatelia iba domnievajú, že si môžu vybrať zo súťažných ponúk, ktoré sú výsledkom hospodárskej súťaže, pričom v skutočnosti dotknutí podnikatelia vedome nahradili hospodársku súťaž praktickou

spoluprácou medzi sebou. De facto sa tak stráca podstata a zmysel tendra, cieľom ktorého je výber najvýhodnejšej ponuky.

Predkladanie ponúk zo strany takto prepojených subjektov môže vzbudzovať falošné zdanie riadnej súťaže, čo je priamo v rozpore s princípom súťaženia vo verejnom obstarávaní, a preto, podľa môjho názoru je nevyhnutná právna regulácia, ktorá rieši túto situáciu. Ďalším problémom, ktorý pri verejných obstarávaniach s využitím elektronického trhoviska je možné badať, je podávanie ponúk zo strany takých subjektov, ktorí zjavne ani nie sú spôsobilé dodať obstarávaný tovar, stavebné práce alebo služby. Dôvodom účasti týchto subjektov na procese verejného obstarávania nie je zvíťaziť v tendri, ale iba vytvoriť zdanie súťaže podaním „krycej ponuky“ a často aj zakrytie umelo vysokej ceny. V tejto súvislosti z dôvodu zabezpečenia „krycej účasti“ vo verejnom obstarávaní realizovanom s využitím elektronického trhoviska dochádza k vzniku nových podnikateľských subjektov, ktorých jediným cieľom je uľahčiť koordináciu postupu vo verejnom obstarávaní. Ide o subjekty, ktoré môžu, ale nemusia byť personálne alebo majetkovo prepojené s víťazom tendra a ktorých úlohou je zabezpečiť plynulý prechod vopred určených podnikateľov do druhého kola (do elektronickej aukcie) tým, že koordinovaným postupom vylúčia skutočných konkurentov z druhého kola. Takíto dodávatelia vo väčšine prípadov nikdy nezvíťazia v elektronickej aukcii, resp. v prípade ich víťazstva buď odstúpia od zmluvy alebo obstaraný tovar realizujú cez subdodávky s reálnym dodávateľom. Pre takýchto dodávateľov pritom represívne nepôsobí ani vystavenie kvalifikovanej negatívnej referencie a zaradenie na „Black list“ (zoznam nežiaducich dodávateľov), či prípadné vylúčenie z účasti na zadávaní zákazky. Pokiaľ ide o subdodávky medzi víťazom tendra a iným neúspešným uchádzačom, ide o veľmi frekventovanú schému kolúzneho správania, pri ktorom úspešný uchádzač poskytne neúspešnému uchádzačovi (resp. viacerým uchádzačom) subdodávky v získanej zákazke, resp. v inej zákazke prostredníctvom počítača ako prostriedku na páchanie takejto činnosti.

Považujem za dôležité upozorniť rovnako na fakt, že bez patričného technicky relevantného vzdelávania orgánov činných v trestnom konaní, či už útvarov polície alebo sudcov, bude boj s počítačovou kriminalitou neúčinný. Verejný sektor musí byť v tomto ohľade konkurencieschopný a teda technologicky napredovať aspoň tak rýchlo ako svet počítačových hackerov, inak bude takmer nemožné dostať tento typ kriminality pod kontrolu. Fakt, že kybernetická kriminalita väčšinou nie je spájaná s hrubými formami delikvencie a teda nie je

charakterizovaná ako násilná len prižívuje ľahkomyseľné nazeranie verejnosti na tento problém.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BRVNIŠŤAN, M.: Bezpečnostné povedomie v kontexte boja proti novodobým bezpečnostným hrozbám. In: Zborník príspevkov z IX. medzinárodnej vedeckej konferencie v Banskej Bystrici 11. – 12. februára 2016. Banská Bystrica: Fakulta politických vied a medzinárodných vzťahov UMB, 2016, str. 520-530. ISBN 978-80-557-1093-8.

ČERMÁK, J.: Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent a přihlédnutím k rozsudku ve věci The Pirate Bay. Právní rozhledy. 2008, č.8.

GŘIVNA, T.: Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. Acta universitatis carolinae – iuridica 4, 2008, str. 21-34.

IVOR, J. – POLÁK, P. – ZÁHORA, J.: Trestné právo procesné I. Bratislava: Wolters Kluwer, 2017. ISBN 978-80-8168-593-4.

KLIMEK, L.: Základy trestného práva Európskej únie. Bratislava: Wolters Kluwer, 2017, ISBN-978-80-8168-601-6

KRÁL, M.: Bezpečnost domácího počítače. Praha: Grada, 2006. 336 s. ISBN 80-247-1408-6.

KURILOVSKÝ, R.: Vyšetrovanie počítačovej kriminality. In: Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie. Bratislava: APZ, 2018, s. 162-171. ISBN 978-80-8054-751-6.

LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. In: Policista, 1998, č. 3, příloha s. VIII. [cit. 16. 4. 2021] Dostupné z: http://aplikace.mvcr.cz/archiv2008/casopisy/policista/prilohy/pc_krimi.html

MATĚJKA, M.: Počítačová kriminalita. Praha: Computer Press, 2002, 106 s. ISBN 80-7226-419-2.

Dohovor Rady Európy č. 185 z dňa 23.11.2001 o počítačovej kriminalite.