https://doi.org/10.5817/RPT2017-1-3

KYBERÚTOK AKO VNÚTORNÁ INFORMÁCIA ALEBO KEDY S PRAVDOU VON

TOMÁŠ ABELOVSKÝ[*]

ABSTRAKT

Nasledujúca úvaha sa snaží zodpovedať na otázku, kedy a či vôbec má tuzemský emitent finančného nástroja uverejniť informáciu o kyberútoku na jeho informačný systém. [1] *Sú analyzované otázky notifikačnej povinnosti o vnútornej informácii. Úvaha smeruje k záveru, že emitent má povinnosť bezodkladne informovať o prebiehajúcom alebo dokonanom kyberútoku relevantnú verejnosť, ak sú splnené niektoré podmienky kladené na kvalitu vnútornej informácie.*

KĽÚČOVÉ SLOVÁ

kyberútok, vnútorné informácie, oznamovacia povinnosť, emitent finančného nástroja

ABSTRACT

The following paper answers the question when and whether a domestic issuer of a financial instrument should disclose an information about a cyberattack against his system. The paper analyses a notification duty about insider information. The reasoning concludes that if certain requirements for the quality of insider information are met, the issuer has an obligation to inform the relevant public without delay about ongoing or completed cyberbattack.

[*] Mgr. Tomáš Abelovský je doktorand na Ústave práva a technológií, Právnickej fakulty Masarykovej Univerzity. Kontaktný e-mail je tomas@abelovsky.com.

[1] Úvaha je riešená vo svetle českej, ale aj slovenskej právnej úpravy vnútorných informácií.

KEYWORDS

Cyberattack, insider information, notification obligation, issuer of a financial instrument

1. ÚVODNÉ POZNÁMKY

V marci 2016 došlo ku masívnemu kyberútoku na viaceré americké advokátske kancelárie, ktoré zastupujú najväčšie verejne obchodovateľné korporácie (Cravath, Weil Gotshal).[2] Zaujímavosťou tohto útoku je, že na rozdiel od nedávneho prípadu odcudzenia množstva kreditných kariet a osobných údajov z banky JP Morgan Chase,[3] tento učebnicový hackerský útok smeroval k získaniu dôverných a vnútorných informácií klientov. Účelom bola ich analýza a následné zobchodovanie. Držanie vnútornej informácie a vyčkávanie na jej vhodné použitie má niekoľko následkov. Za prvé, táto taktika útočníkov sťažuje prácu orgánov činných v trestnom konaní. Za druhé, následok tohto činu je nekontrolovateľný, no najmä v prípade neochoty advokátskych kancelárií informovať o útoku svojich klientov alebo verejnosť. V USA tento prípad otvoril diskusiu o tom, či má právny zástupca verejne obchodovateľných spoločností informovať širokú verejnosť v prípade kyberútoku.[4] Takáto povinnosť sa už však dávno vzťahovala na subjekty regulované Americkou komisiou pre cenné papiere a burzu (SEC).[5] Nasledujúca krátka úvaha sa snaží zodpovedať na otázku, kedy a či vôbec

[2] HONG, N. a Sidel, R., Hackers Breach Law Firms, Including Cravath and Weil Gotshal. *The Wall Street Journal.* Marec 2016. Dostupné z: http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

[3] What lies behind the JPMorgan Chase cyber-attack. *The Economist.* November 2015. Dostupné z: http://www.economist.com/news/business-and-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itself-what-lies-behind

[4] 47 štátov má vlastnú legislatívu týkajúcu sa porušenia osobných údajov (*security breach notification laws*), ktorá ma pôvod v kalifornskej úprave. Viď Cal. Civ. Code 1798.82 and 1798.29. Dostupné z: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

[5] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance. 2011. Dostupné z: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

má tuzemský emitent finančného nástroja[6] povinnosť uverejniť informáciu o samotnom kyberútoku na jej informačný systém.[7]

2. POVINNÁ OSOBA

Zákon o podnikaní na kapitálovom trhu definuje širokú skupinu povinných osôb,[8] ktoré majú notifikačnú povinnosť, či už voči dozornému orgánu alebo verejnosti. Ako príklad môže poslúžiť akciová spoločnosť, ktorá je emitentom investičného nástroja obchodovaného na regulovanom trhu EÚ (napr. na Burze cenných papírů Praha). Táto obchodná korporácia má zákonnú povinnosť bezodkladne zverejňovať a oznamovať tie vnútorné informácie, ktoré sa jej priamo týkajú.[9] Je možné predpokladať, že emitent, ktorý má kapitálovú účasť širšej verejnosti, si nesie dôležitú povinnosť čo najskôr informovať akcionárov alebo investorov o vnútorných informáciách, ktoré môžu mať vplyv na cenu jej emitovaných finančných nástrojov (napr. akcií).

---

[6] Emitentom je právnická osoba, ktorá sa riadi súkromným alebo verejným právom a ktorá emituje finančné nástroje alebo navrhuje ich emisiu, pričom emitent je v prípade depozitných certifikátov zastupujúcich finančné nástroje emitentom zastupovaných finančných nástrojov.

[7] Právny problém bude analyzovaný vo svetle platnej právnej úpravy ČR (zákon č. 256/2004 Sb. o podnikání na kapitálovém trhu), SR (Zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov, zákon č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov.) a najmä nariadenia Európskeho parlamentu a rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (nariadenie o zneužívaní trhu) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES. Český zákon používa pojem „vnitřní informace“ (§ 124), slovenský „dôverná informácia“ (§ 132b) a nariadenie „inside information“ (Article 7). Pre potreby tejto práce bude používaný promiscue pojem „dôverná informácia“ aj keď jeho význam v obchodnoprávnych vzťahoch je odlišný. Viď. KOTÁSEK, Josef. *Ochrana vnitřních informací.* Brno: Tribun EU, 2008. 255 s. ISBN 978-80-7399-355-9. Str. 77 an.

[8] Napr. obchodník s cennými papiermi a inštitucionálny investor, organizátor regulovaného trhu, emitent cenných papierov, osoba podieľajúca sa na rozhodovaní emitenta a osoby jej blízke, akcionár v špecifickej situácii, zamestnanci alebo iné osoby pri výkone svojho zamestnania, povolania alebo funkcie, alebo osoby v súvislosti s plnením svojich povinností na obchodoch s investičnými nástrojmi.

[9] § 132b odst. 1 zákona č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov, § 125 odst. 1 zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu alebo článok 17 odst.1 nariadenia EÚ č. 596/2014 o zneužívaní trhu.

Filozofia tejto úpravy spočíva v tom, že ide jednak o prevenčný boj s *insider tradingom*, ale rovnako aj záväzok kapitálovej spoločnosti voči svojím akcionárom, ale aj potencionálnym investorom. Spoločnosť môže svoje financovanie hľadať na kapitálových trhoch – burzách, čo však nie je zvykom pre kontinentálne burzy na rozdiel od USA. Napokon aj prísna verejná regulácia emitenta (napr. akciovej spoločnosti) je znakom toho, že štát má záujem o transparentnosť obchodných transakcií takejto spoločnosti. Vyššie uvedená povinnosť trvá aj z dôvodu, že spoločnosť si potrebuje sústavne budovať vlastnú dôveru u svojich akcionárov, potencionálnych investorov, partnerov, zákazníkov a v neposlednom rade celého trhu ako takého.

Americká teória pri zákaze *insider tradingu* hovorí o *fiduciárnej* povinnosti voči investorom (akcionárom), resp. o rovnom a férovom prístupe k obchodovateľným nástrojom (*equal access*), ale aj o predchádzaní zneužitia takejto informácie (prípady *Chiarella* and *Dirks*).[10] Je zrejmé, že táto teória ovplyvnila aj európsku reguláciu. Tá akcentuje zákaz transakcií zasvätených osôb (s výnimkami pre určité osoby a určité transakcie, v režime *safe harbour*), s určitými prvkami transparentnej evidencie (vedenie zoznamov zasvätených osôb, oznamovanie transakcií).[11]

3. KYBERÚTOK AKO VNÚTORNÁ INFORMÁCIA

Kyberútok je možné definovať ako čin s použitím počítača alebo súvisiacich technológií, siete alebo systémov, smerujúci k narušeniu, odcudzeniu alebo zničeniu informačného systému (resp. tam uložených dát) a majetku. Pre potreby tejto práce bude používaný zjednodušený pojem kyberútok.[12]

---

[10] SCHEPPELE, Kim Lane. *"It's Just Not Right": The Ethics of Insider Trading.* Law and Contemporary Problems, Vol. 56, No. 3, Modern Equity, Summer, 1993. Str.124 an. alebo Ibid. KOTÁSEK, Str. 41 an.

[11] Ibid. KOTÁSEK, Str. 51 an.

[12] Český zákon o kybernetickej bezpečnosti rozoznáva kybernetickú bezpečnostnú udalosť a incident. „Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události." Viď. § 7 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Kyberútok voči súkromnej spoločnosti je väčšinou motivovaný nedovoleným obohatením na úkor napadnutej osoby. Trestný zákon definuje trestný čin neoprávneného prístupu k počítačovému systému alebo nosiču informácií pomocou prekonania bezpečnostného opatrenia a tým neoprávnené získanie prístupu k počítačovému systému alebo k jeho časti.[13]

Predmetom tohto činu v prípade akciovej spoločnosti môže byť široká paleta vnútorných informácií alebo osobných údajov, ktoré spravujú zasvätené osoby:[14] napr. vnútorná databáza partnerov a ich platby, nezverejnené účtovníctvo a súvisiace správy, pripravované podnikateľské zámery a projekty, pripravovaný odpredaj podniku atď. Je zrejmé, že každá z týchto informácií má potenciál ohroziť úplnú a riadnu transparentnosť trhu. Najmä v prípade, ak by sa dostala do rúk len niektorých účastníkov trhu (zneužívanie trhu).[15] Základným motívom je zvyčajne obchodovanie s využitím týchto vnútorných informácií. Útočníkom môže byť externá osoba, ale aj zamestnanec, resp. zasvätená osoba emitenta. Zainteresované subjekty (napr. kupujúci vnútornej informácie) tak získavajú nespravodlivú výhodu na úkor poškodenej osoby na základe vnútornej informácie, o ktorej pred útokom nevedeli, a v dôsledku toho narušujú integritu finančných trhov a dôveru investorov.[16] Otázkou zostáva, či odhalený kyberútok na akciovú spoločnosť je sám o sebe dôvernou informáciou, ktorú má táto spoločnosť zverejniť, resp. sprístupniť.

---

[13] § 230 zákona č. 40/2009 Sb. trestní zákoník. V SR ide o viac skutkov: (§ 247) Neoprávnený prístup do počítačového systému, (§ 247a) Neoprávnený zásah do počítačového systému, (§ 247b) Neoprávnený zásah do počítačového údaja, (§ 247c) Neoprávnené zachytávanie počítačových údajov, (§ 247d) Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov, Zákon č. 300/2005 Z. z. Trestný zákon.

[14] Zasvätenou osobou môže byť právnická osoba alebo fyzická osoba, ktorá získala dôvernú informáciu. Viď. § 131 (8) zákona č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov, § 124 (3) zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu.

[15] Zneužívanie trhu je pojem, ktorý zahŕňa neoprávnené konanie na finančných trhoch a na účely tohto nariadenia by sa mal chápať tak, že pozostáva z obchodovania s využitím dôverných informácií, neoprávneného zverejňovania dôverných informácií a manipulácie s trhom. Takéto konanie bráni úplnej a riadnej transparentnosti trhu, ktorá je predpokladom pre obchodovanie všetkých hospodárskych subjektov na integrovaných finančných trhoch. Viď. Nariadenie EÚ č. 596/2014 o zneužívaní trhu, rec. 7.

[16] Nariadenie EÚ č. 596/2014 o zneužívaní trhu, rec. 23.

Aby informácia o kyberútoku bola vnútornou informáciou, musí vykazovať nasledujúce znaky, ktoré musia byť splnené súčasne:[17]

a) týka sa skutočnosti významnej pre vývoj kurzu či inej ceny finančného nástroja alebo jeho výnosu a mohla by po tom, čo by sa stala verejne známou, významne ovplyvniť kurz, inú cenu alebo výnos finančného nástroja alebo iného nástroja, ktorého hodnota sa odvodzuje od tohto finančného nástroja;
b) nie je verejne známa;
c) je presná.

3.1 KYBERÚTOK AKO KURZOTVORNÁ INFORMÁCIA

Z pohľadu možných následkov, kyberútok nie je odlišný od iného protiprávneho konania smerujúceho k poškodeniu majetku napadnutej osoby.[18] Ide o virtualizovaný útok na virtualizované záujmy obete, ktorého následok sa vždy aktualizuje do úbytku aktuálnych hodnôt. Odlišnosť je možné vidieť v povahe následkov, nakoľko samotný kyberútok nemusí byť odhalený vôbec. Medzi najčastejšie následky patrí priama a vyčísliteľná škoda (napr. odcudzenie hodnotných vnútorných údajov), ušlý zisk (napr. zmarená transakcia), zvýšené náklady na kybernetickú ochranu, náklady na konzultačnú činnosť expertov a právnikov, súdne poplatky a v neposlednom rade nemajetková škoda na povesti. Štatistický sa uvádza, že útok je zistený v priemere až po 205 dňoch.[19] Tým, že vo virtualizovanom móde je každá informácia *potenciálne ubiquitná*, jej odcudzenie vo fyzickom zmysle slova nehrozí. Avšak jej zneužitie je ďaleko škodlivejšie. Pri odhaľovaní kyberútokov sa bezpečnostní analytici sústredia na kontamináciu alebo narušenie

[17] Úřední sdělení České národní banky ze dne 18. prosince 2009 o ochraně proti zneužívání trhu a transparenci. Věstník ČNB částka 21/2009 ze dne 23. prosince 2009.

[18] Metodika ČNB uvádza ako príklad kurzotvornej informácie informáciu „o zahájení nebo ukončení soudních, správních nebo rozhodčích řízení, které mají nebo by mohly mít významný vliv na finanční situaci nebo ziskovost emitenta finančního nástroje, např. uložení významné pokuty nebo povinnosti k náhradě škody významného rozsahu, včetně řízení svýznamným dopadem na reputaci emitenta finančního nástroje apod.“ pod ktorú je možné následky kyberútoku podradiť.

[19] BITGLASS. “Where’s your data?” experiment. Dostupné z: http://pages.bitglass.com/rs/bitglass/images/BR-Bitglass_Wheres_Your_Data.pdf

systému podozrivými inštrukciami alebo na chovanie operačného systému a analyzujú sieťovú prevádzku. Takýto bezpečnostný incident však ešte nemusí spôsobiť priamu škodu. Je preto odlišný od prípadu, kedy sa do archívu spoločnosti vláme zlodej a odcudzí doklady pripravovanej fúzie. Identifikácia chýbajúceho dokladu je jasná a navyše je zrejmé, s akou sumou informácií sa mohol zlodej oboznámiť v danom čase a na danom mieste. Kyberútoky sú častokrát koncipované vo vrstvách. Každá vrstva odhaľuje ďalšiu vrstvu iného útoku na iné záujmy v napadnutom informačnom systéme. Avšak nie vždy sa podarí vypátrať všetky vrstvy.

Aby kyberútok mal význam pre notifikačnú povinnosť, informácia o ňom musí predstavovať kurzotvornú informáciu. Kurzotvorná informácia je taká informácia, ktorá sa priamo dotýka emitenta finančného nástroja, jeho hospodárskej situácie a vyhliadok do budúcnosti, prípadne ktoré sa týkajú práv plynúcich z finančného nástroja. Podľa usmernenia ČNB „okrem toho ide o značné množstvo informácií, ktoré sa emitenta finančného nástroja, kurzu a pod. týkajú nepriamo - napr. o rastúcej cene ropy, zmene úrokových sadzieb, uzavretie dohody regulovaného trhu s tvorcom trhu o zabezpečenie likvidity k akciám emitenta finančného nástroja a podobne. […] Na rozdiel od priamych vnútorných informácií nie je však emitent finančného nástroja povinný nepriame informácie uverejniť.“[20] Preto informácia o kyberútoku[21] musí splniť nasledujúce podmienky:

- kyberútok je cielený na informačný systém v kompetencii emitenta (priamo alebo nepriamo spojený s emitentom); a
- následok zverejnenia informácie emitentom o prebiehajúcom kyberútoku má sám o sebe potenciál ovplyvniť cenu finančného nástroja (hovoríme o teste cenovej citlivosti na možnú škodu alebo iný následok vyvolaný kyberútokom).

Vyššie uvedený potenciál v zmysle nariadenia EÚ o zneužívaní trhu je definovaný tak, že následok (ne)zverejnenia má pravdepodobný vplyv na

[20] Ibid. Úřední sdělení ČNB o ochraně proti zneužívání trhu a transparenci, str. 2.

[21] § 116 zákona č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov, § 124 (3) zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu.

cenu finančného nástroja.[22] Je zrejmé, že táto pravdepodobnosť nebude hraničiť s istotou, avšak musí vyznieť dostatočne presvedčivo. Bude posudzovaná individuálne od prípadu k prípadu. Je možné zhrnúť, že ak emitent vie o kyberútoku, ktorý prebehol alebo prebieha v takom rozsahu, že každý riadny hospodár, resp. uvážlivý investor by nadobudol presvedčenie o tom, že takýto útok ovplyvní hodnotu jeho podniku z pohľadu jeho majetku, bezpečnosti, ušlého zisku, prípadných sporov alebo povesti, má tento útok pravdepodobný vplyv na cenu.

3.2 DOSTUPNOSŤ INFORMÁCIE O KYBERÚTOKU

Informácia o kyberútoku sa stáva verejnou informáciou v čase, keď bola sprístupnená tej časti investorov, ktorí sa zhromažďovaním informácií tohto typu a ich hodnotením aktívne zaoberajú (napr. sledujú odvetvie, v ktorom pôsobí emitent).[23] Všeobecne sa považuje informácia za verejne známu, ak je zverejnená voči širokému publiku investorov neurčitého počtu. Ďalej je verejne známa aj taká informácia, ktorá je dostupná súčasným i potenciálnym investorom, aj keď nebola zverejnená emitentom včas a riadne. Navyše nie je podstatné, či informáciu uverejnil emitent finančného nástroja alebo či sa stala známou z iných zdrojov.[24]

Môže sa stať, že kyberútok je vykonaný v tichosti a samotná informácia o ňom nemá dôvod preniknúť na verejnosť. Avšak motívy útočníkov sú rôznorodé. Niektorí predbehnú v informovaní o útoku svoje obete, iní využijú strach zo straty reputácie a pokračujú v tichom vydieraní. Najčastejšie motívy sú vždy kriminálne s úmyslom sa obohatiť, čo dokresľuje nasledovná štatistika pre rok 2016:[25]

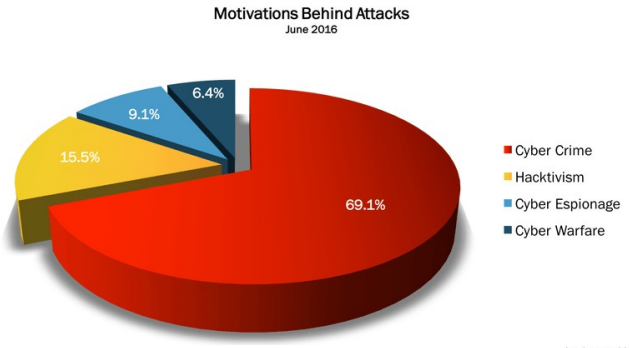
Príkladom medzinárodnej špionáže spolu s kriminálnou činnosťou bol masívny kyberútok na spoločnosť Sony v roku 2014. Informácia o kyberútoku prenikla na verejnosť v novembri 2014, keď hackerská skupina Guardians of Peace začala zverejňovať skopírované dáta. Samotná spoločnosť

[22] Článok 7 (1) Nariadenia EÚ č. 596/2014 o zneužívaní trhu.

[23] Ibid. Úřední sdělení ČNB o ochraně proti zneužívání trhu a transparenci, str. 3.

[24] Ibid. Úřední sdělení ČNB o ochraně proti zneužívání trhu a transparenci, str. 3.

[25] PASSERI, Paolo. July 2016 Cyber Attacks Statistics. Dostupné z: http://www.hackmageddon.com/2016/08/18/july-2016-cyber-attacks-statistics/



v tomto čase už o útoku vedela, ale zvolila vyčkávaciu taktiku (resp. bola ním zaskočená do takej miery, že nevedela čo robiť).[26]

Je zrejmé, že útočník má často v rukách rozhodnutie o tom, či informácia o kyberútoku zostane vnútorná alebo verejná. Sám je viazaný povinnosťou mlčanlivosti. Spáchaním trestného činu, t.j. kyberútoku, sa dostal do rovnakého postavenia ako emitent, t.j. do postavenia zasvätenej osoby.[27] Bolo by však naivné sa domnievať, že útočník po spáchaní kyberútoku dodrží povinnosť mlčanlivosti.[28] To má však už aj trestnoprávny rozmer v naplnení niektorých ďalších trestných činov a poškodený musí predvídať takéto konanie.[29]

3.3 PRESNOSŤ INFORMÁCIE O KYBERÚTOKU

Presnosť informácie je žiadúca najmä z dôvodu, aby sa predišlo nedorozumeniu o tom, či ide o exaktnú informáciu alebo o špekulácie a fámy. Navyše táto presnosť je naviazaná na potenciál informácie ovplyvniť trh

[26] SEAL, Mark. An Exclusive Look at Sony's Hacking Saga. *Vanity Fair.* Retrieved February 4, 2015. Dostupné z: http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

[27] Porovnaj § 124(3) ZPK alebo § 131(8)d CPIS.

[28] *Insider trading* sa vyznačuje tým, že zasvätená osoba poruší nejakú z nasledujúcich povinnosti: nesmie využiť vnútornú informáciu k svojmu alebo cudziemu prospechu, nesmie ju oznámiť alebo sprístupniť inej osobe a nesmie dávať odporúčania inej osobe na základe znalosti vnútornej informácie. Porovnaj § 124(4) ZPK alebo § § 131(9) CPIS.

[29] V ČR môže ísť o trestný čin neoprávněné nakládání s osobními údaji (§ 180 TZ), poškození cizích práv (§ 181 TZ), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ), porušení předpisů o pravidlech hospodářské soutěže (porušování obchodního tajemství, § 248(1)h TZ), na SR to bude zrkadlovo najmä ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva (§ 264 TZ).

s finančnými nástrojmi. Smernica hovorí, že „právna istota pre účastníkov trhu by sa mala zvýšiť prostredníctvom užšieho vymedzenia dvoch z prvkov nevyhnutných pre vymedzenie dôvernej informácie, a to presnosti tejto informácie a významnosti jej možného účinku na ceny finančných nástrojov, súvisiacich spotových zmlúv týkajúcich sa komodít alebo dražených produktov založených na emisných kvótach.“[30] Kotásek uvádza, že „do istej miery možno dostatočnú záruku presnosti informácií vidieť [aj] v tom, že sú vnímané ako informácie, ktorých obsahom sú "skutočnosti", t.j. preukázateľné a dôkazom prístupné udalosti a stavy vonkajšieho sveta.“[31] Žiaľ z právnej úpravy nemôžeme dovodiť to, že by informácia mala byť úplne exaktná. Môžeme sa pýtať, ako veľmi presná má byť informácia o kyberútoku na to, aby išlo o vnútornú informáciu, ktorá bude mať vplyv na kurz alebo cenu príslušného nástroja.

Odpoveď je možné nájsť v prípade *Lafont,* kde Súdny dvor Európskej únie dovodil, že podmienka presnej informácie nevyžaduje, aby z nej bolo zrejmé, v akom smere bude mať táto informácia vplyv na kurz alebo cenu príslušného nástroja (či bude klesať alebo stúpať). Súd uviedol, že informácia o pláne spoločnosti kúpiť významný podiel v inej spoločnosti „môže byť totiž uvážlivým investorom použitá ako súčasť základne jeho investičných rozhodnutí.“[32] Tento prístup prekonal doteraz platný názor Európskeho orgánu pre trhy cenných papierov (ESMA), podľa ktorého „informácia samotná nemusela síce indikovať, v akom rozsahu bude mať vplyv na kurz finančného nástroja, aby však bola presná, musela z nej byť zrejmá aspoň indikácie možného smeru vývoja tohto kurzu.“[33] Toto rozhodnutie je v súlade s názorom Kotáska, „či je vôbec nutné klásť na vnútorné informácie požiadavku "presnosti" (keď presné informácie bude [sám] trh schopný vyhodnotiť ako informácie s kurzotvornou relevanciou).“[34]

Pootvorenie dverí pre širší výklad nároku na presnosť umožňuje vidieť informáciu o kyberútoku ako vnútornú informáciu poškodeného emitenta.

[30] Rec. 18 nariadenia EÚ č. 596/2014 o zneužívaní trhu.

[31] Ibid. KOTÁSEK, str. 107.

[32] Rozsudok SDEÚ vo veci C-628/13 zo dňa 11.3.2015, Jean-Bernard Lafonta proti Autorité des marchés financiers, odst. 33.

Aj keď ten v čase útoku nevie zhodnotiť skutočnú škodu a ušlý zisk spôsobený týmto útokom, musí sa riadiť tým, že daná informácia môže byť uvážlivým investorom použitá ako súčasť základne jeho investičných rozhodnutí. Napríklad informácia o kyberútoku na spoločnosť Sony spôsobila prepad jej akcii na japonskom trhu o 10 %.[35] K podobnému názoru dospeli Arcuri, Brogi a Gandolfi, ktorí skúmali verejne dostupné dáta o kyberútokoch medzi rokmi 1995 až 2012.[36] Tu však treba spomenúť aj opačný názor, ktorý poukazuje na to, že kyberútok ma tendenciu byť zamlčaný, resp. komunikovaný s dlhým časovým odstupom, a preto nemá žiaden kurzotvorný potenciál ako taký.[37] Osobne zastávam názor prvej skupiny. Je len otázkou času a technologického pokroku, kedy investori dokážu jednoduchým spôsobom zmerať rozsah a výšku škody kyberútoku a bezprostredne na to reagovať. Navyše, nič nie je horšie pre investora technologickej spoločnosti, ak sa až s odstupom času dozvie, že bola terčom kyberútoku. Preto sa ďalšie odborné výskumy odohrávajú aj v oblasti zaisťovníctva a poisťovacích služieb, ktoré udávajú smer poistnej matematiky a hľadajú spôsob ako kvantifikovať kybernetické riziká.[38]

4. NOTIFIKAČNÁ POVINNOSŤ

V prípade kyberútoku je možné uvažovať o dvoch existujúcich notifikačných povinnostiach: oznam o porušení ochrany osobných údajov[39] a oznámenie trestného činu. Podnikanie na kapitálovom trhu priamo takýto

[33] ŠOVAR, Ján. Soudní dvůr Evropské unie k insider tradingu: Jak moc nepřesná informace je ještě přesná? Dostupné z: https://www.patria.cz/pravo/2949748/soudni-dvur-evropske-unie-k-insider-tradingu-jak-moc-nepresna-informace-je-jeste-presna.html

[34] Ibid. Kotásek, str. 80.

[35] Paul, Monica. Sony hack sends stock down 10 % in past week. Dostupné z: http://money.cnn.com/2014/12/15/investing/sony-stock-hack/

[36] Arcuri, Brogi a Gandolfi. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? Dostupné z: http://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2014Rome/papers/EFMA2014_'0408_fullpaper.pdf

[37] Kvochko, Elena. Why Data Breaches Don't Hurt Stock Prices. Harvard Business Review. Dostupné z: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

[38] Swiss Re Corporate Solutions joins forces with IBM to offer cyber risk protection. Dostupné z: http://www.swissre.com/corporate_solutions/Swiss_Re_Corporate_Solutions_joins_forces_with_IBM_to_offer_cyber_risk_protection.html

oznam nepozná, avšak úprava rozlišuje dva druhy notifikácií emitentov: pravidelné notifikačné povinnosti a priebežné (náhodilé) notifikačné povinnosti emitenta. Pravidelne zverejňované informácie (napr. výročné správy) sa v dnešnom digitálnom svete veľmi rýchlo stávajú obsolentnými. Stávajú sa z nich skôr formálne potvrdenia o predvídanej skutočnosti. Je zrejmé, že investori by neboli schopní urobiť svoje rozhodnutia len na základe týchto správ. Priebežne zverejňované informácie sú práve korektívom toho, čo sa stalo medzi pravidelnými hláseniami a zároveň šikovným nástroj na „zneškodnenie" vnútorných informácií.

Podľa súčasného znenia nariadenia EÚ o zneužívaní trhu emitent čo najskôr informuje verejnosť o vnútorných informáciách, ktoré sa ho priamo týkajú. Emitent zabezpečí tiež sprístupnenie vnútorných informácií verejnosti, ktoré umožní rýchly prístup a úplné, správne a včasné posúdenie informácií zo strany verejnosti. Emitent nesmie spájať sprístupnenie vnútorných informácií verejnosti s trhovým zviditeľňovaním svojich činností. Navyše, emitent má povinnosť uverejniť a uchovať na svojej webovej stránke najmenej päť rokov všetky vnútorné informácie, ktoré je povinný sprístupniť verejnosti. Vnútorné informácie uverejňované emitentom by sa mali šíriť tak, aby k nim bol zaistený neuprednostňujúci, ľahký a bezodplatný prístup. To znamená, že rovnaká informácia by mala byť zároveň zaslaná (v elektronickej podobe) Českej Národnej Banke, príp. organizátorom regulovaných trhov, na ktorých sú finančné nástroje emitenta prijaté na obchodovanie, a zároveň uverejnená v obvyklom formáte, t.j. tak, aby všetkým investorom boli poskytnuté informácie obsahovo zhodné a v rovnakom čase. Nesplnenie notifikačnej povinnosti je prísne sankcionované dozorným orgánom.[40]

Americká SEC už v roku 2011 prijala (nezáväzné) odporúčanie o tom, ako by mal postupovať emitent v prípade informácie o kybernetickom

[39] Článok 33 (Oznámenie porušenia ochrany osobných údajov dozornému orgánu) a článok 34 (Oznámenie porušenia ochrany osobných údajov dotknutej osobe) nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

[40] Viď článok 30 nariadenie EÚ č. 596/2014 o zneužívaní trhu.

útoku.[41] Kyberútok už dávno nie je len záležitosťou IT oddelenia, ale stal sa vecou záujmu akcionárov, investorov a širšej verejnosti. Zaujímavosťou je, že notifikačná povinnosť v USA sa nevzťahuje len na samostatný útok, ale pokrýva aj hrozbu útoku a vytvára rámec pre *cybersecurity governance*:[42]

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky […] In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents.

Emitent (*registrant*) v USA musí pred zverejnením informácie o kyberútoku posúdiť pravdepodobnosť takého incidentu. Musí zohľadniť kvantitatívne a kvalitatívne hľadisko hroziaceho rizika, ďalšie potencionálne náklady na jeho odstránenie a iné aspekty súvisiace so zneužitím vnútorných informácií. Tieto povinnosti logicky tlačia povinné osoby k tomu, aby prijali najvyššie možné preventívne opatrenia voči kyberútokom. Emitent má taktiež povinnosť identifikovať, ktoré jej oblasti podnikania sú rizikové z pohľadu možného kyberútoku. Adekvátne opatrenia sú posudzované samotným SECom. Už len zanedbanie prijatia takéhoto opatrenia môže podliehať enormným sankciám. V čase ohrozenia alebo odhalenia nestačí nahlásiť kyberútok, ale emitent musí preukázať taktiež všetky reaktívne kroky.

Na záver sa je možné spýtať, čo v prípade, že by bol kyberútok odvrátený. Má emitent rovnakú informačnú povinnosť? Tu sa je možno inšpirovať znením všeobecného nariadenia o ochrane údajov v prípade notifikačnej povinnosti o porušení osobných údajov, kde sa oznámenie nevyžaduje, ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia.[43] V prípade kyberútoku by malo ísť o také následné opatrenia,

---

[41] Ibid. SEC, CF Disclosure Guidance.

[42] Podobne ako tomu je pri inštitúte *e-discovery hold* v prípade hroziaceho súdneho sporu, kedy strana, ktorá môže byť zažalovaná, má povinnosť uchovávať všetky elektronické informácie pre budúci spor.

[43] Článok 34 nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 (všeobecné nariadenie o ochrane údajov).

ktorými sa zabezpečí, že riziko zneužitia informácie o kyberútoku pravdepodobne už nebude mať vplyv na kurz, cenu alebo výnos finančného nástroja.

5. ČASOVÝ ASPEKT

Česká a slovenská úprava hovorí o povinnosti „bezodkladného" uverejnenia. Ide o primeraný časový úsek, v ktorom je emitent finančného nástroja schopný uverejniť vnútornú informáciu za daných okolností a pri svojom bežnom chode.[44] Za nezverejnenie zodpovedá priamo emitent. Domnievam sa, že emitent musí informovať o kyberútoku okamžite po tom, čo sa dozvedel o jeho technických znakoch, ktoré sú dostatočne zrozumiteľné pre uvážlivého investora a súčasne boli splnené všetky kritéria vnútornej informácie.

Uverejnenie informácie možno odložiť v prípade závažných dôvodov na strane emitenta.[45] Avšak musí byť splnená podmienka, že nesprístupnením informácie nebude verejnosť klamaná (pravdepodobne nebude zavádzaná) a emitent je schopný zabezpečiť dôvernosť týchto informácií. Zabezpečenie dôvernosti informácie o kyberútoku na strane emitenta je len zdanlivé riešenie. Ako bolo spomenuté vyššie, útočník, hoci v postavení zasvätenej osoby, je nekontrolovateľným elementom v šírení informácie, a preto túto povinnosť emitent nemôže takmer nikdy objektívne splniť. Domnievam sa, že odloženie informácie o zistenom kyberútoku je možné len v prípade, ak by došlo k zadržaniu všetkých útočníkov orgánmi činnými v trestnom konaní, súčasne by nedošlo ešte k rozšíreniu tejto informácie v relevantnom okruhu investorov a emitent bol o tejto skutočnosti riadne informovaný.

[44] Ibid. Úřední sdělení ČNB o ochraně proti zneužívání trhu a transparenci, str.8, porovnaj nález Ústavného súdu ČR sp. zn. IV. ÚS 314/05 zo dňa 15. augusta 2005 a rozsudok Najvyššieho správneho súdu ČR sp. zn. 3 As 2/2008 – 152 zo dňa 2. apríla 2008.

[45] O odložení musí emitent informovať dozorný orgán, t.j. ČNB alebo NBS, a to vrátane uvedenia dôvodov pre odloženie a obsahu odkladané informácie. Článok 17(3) Nariadenia EÚ č. 596/2014 o zneužívaní trhu.

6. ZÁVER

Na základe vyššie uvedeného je možné dospieť k záveru, že emitent má povinnosť bezodkladne informovať o prebiehajúcom alebo dokonanom kyberútoku relevantnú verejnosť, ak sú splnené podmienky kladené na kvalitu vnútornej informácie. Takéto oznámenie by malo obsahovať jasne a jednoducho formulovaný opis povahy narušenia informačného systému emitenta a základné informácie o prijatých opatreniach.[46] Vzhľadom na to, že v súčasnosti právna úprava v tejto oblasti absentuje a konkrétne odporúčania alebo usmernenia neexistujú, posúdenie tejto informačnej povinnosti emitenta bude v kompetencii jeho dozorných orgánov a bude v konečnom dôsledku závisieť od rozhodovacej činnosti súdu.

7. POUŽITÁ LITERATÚRA

7.1 LITERATURA

[1] HONG, N. a Sidel, R., Hackers Breach Law Firms, Including Cravath and Weil Gotshal. The Wall Street Journal. Marec 2016. Dostupné z: http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

[2] What lies behind the JPMorgan Chase cyber-attack. The Economist. November 2015. Dostupné z: http://www.economist.com/news/business-and-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itself-what-lies-behind

[3] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance. 2011. Dostupné z: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[4] KOTÁSEK, Josef. Ochrana vnitřních informací. Brno: Tribun EU, 2008. 255 s. ISBN 978-80-7399-355-9.

[5] SCHEPPELE, Kim Lane. "It's Just Not Right": The Ethics of Insider Trading. Law and Contemporary Problems, Vol. 56, No. 3, Modern Equity, Summer, 1993.

[6] BITGLASS. “Where’s your data?” experiment. Dostupné z: http://pages.bitglass.com/rs/bitglass/images/BR-Bitglass_Wheres_Your_Data.pdf

[7] PASSERI, Paolo. July 2016 Cyber Attacks Statistics. Dostupné z: http://www.hackmageddon.com/2016/08/18/july-2016-cyber-attacks-statistics/

[46] Inšpiráciu tu môže byť použitie slovníka „Common Vulnerabilities and Exposures (CVE®)“. Viď. https://cve.mitre.org/about/

[8] SEAL, Mark. An Exclusive Look at Sony's Hacking Saga. Vanity Fair. Retrieved February 4, 2015. Dostupné z: http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

[9] Paul, Monica. Sony hack sends stock down 10 % in past week. Dostupné z: http://money.cnn.com/2014/12/15/investing/sony-stock-hack/

[10] Arcuri, Brogi a Gandolfi. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? Dostupné z: http://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2014-Rome/papers/EFMA2014_0408_fullpaper.pdf

[11] Kvochko, Elena. Why Data Breaches Don't Hurt Stock Prices. Harvard Business Review. Dostupné z: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

[12] Swiss Re Corporate Solutions joins forces with IBM to offer cyber risk protection. Dostupné z: http://www.swissre.com/corporate_solutions/Swiss_Re_Corporate_Solutions_joins_forces_with_IBM_to_offer_cyber_risk_protection.html

7.2 POUŽITÉ PRÁVNE PREDPISY A SÚDNE ROZHODNUTIA:

[13] Cal. Civ. Code 1798.82 and 1798.29. Dostupné z: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

[14] Rozsudok SDEÚ vo veci C-628/13 zo dňa 11.3.2015, Jean-Bernard Lafonta proti Autorité des marchés financiers,

[15] Úřední sdělení České Národní Banky ze dne 18. prosince 2009 o ochraně proti zneužívání trhu a transparenci. Věstník ČNB částka 21/2009 ze dne 23. prosince 2009.

[16] Zákon č. 256/2004 Sb. o podnikání na kapitálovém trhu.

[17] Zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov.

[18] Zákon č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov.

[19] Nariadenia Európskeho parlamentu a rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (nariadenie o zneužívaní trhu) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES.

[20] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.

[21] Zákon č. 40/2009 Sb. Trestní zákoník.

[22] Zákon č. 300/2005 Z. z. Trestný zákon.
