ČASOPIS PRO PRÁVNÍ VĚDU A PRAXI
č. **3** | **2024** | roč. **XXXII** | 483–513
https://doi.org/10.5817/CPVP2024-3-5

Trestnoprávna zodpovednosť manažéra kybernetickej bezpečnosti v českom a slovenskom právnom poriadku*

Criminal Liability of a Cyber Security Manager in the Czech and Slovak Legal System

Jozef Čentéš[**], Michal Rampášek**[***]**

Abstrakt

V článku autori venujú pozornosť manažérovi kybernetickej bezpečnosť (ďalej „CISO" alebo „MKB"), zodpovednému za kybernetickú bezpečnosť v organizácii z hľadiska slovenského a českého právneho poriadku. V úvode článku sú charakterizované úlohy a zodpovednosť MKB pri riešení kybernetického bezpečnostného incidentu a vzťahu k štatutárnemu zástupcovi. V nasledujúcej časti článku sú analyzované vybrané prípady z USA, v ktorých bola voči manažérom právnických osôb (CISO, CEO) vyvodzovaná zodpovednosť pri riešení incidentu. V závere je analyzovaná trestnoprávna zodpovednosť MKB z pohľadu slovenského a českého právneho poriadku.

Klíčová slova

Manažér kybernetickej bezpečnosti; štatutárny orgán; právnická osoba; kybernetická bezpečnosť; zodpovednosť; trestný čin.

Abstract

In this paper, the authors focus to the cybersecurity manager (CISO), who is responsible for cybersecurity in the company's organization from the point of view of the Slovak and Czech legal system. In the introduction of the paper, the roles and responsibilities of the CISO in dealing with a cyber security incident and the relationship with the statutory representative (CEO) are characterized. The next part of the paper analyzes selected cases from the USA in which liability has been invoked against managers of legal entities (CISO, CEO) when dealing with an incident. Finally, the criminal liability of CISOs is analysed from the perspective of the Slovak and Czech legal system.

* Tento článok bol vypracovaný v rámci riešenia projektu APVV-19-0102 – Efektívnosť prípravného konania – skúmanie, hodnotenie, kritériá a vplyv legislatívnych zmien.

** Prof. JUDr. Jozef Čentéš, DrSc., Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta, Univerzita Komenského v Bratislave, Slovenská republika / Department of Criminal Law, Criminology and Criminalistics, Faculty of Law, Comenius University in Bratislava, Slovak Republic / E-mail: jozef.centes@flaw.uniba.sk / ORCID: 0000-0003-3397-746X / Scopus ID: 57205550015

*** JUDr. Michal Rampášek, doktorand, Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta, Univerzita Komenského v Bratislave, Slovenská republika; advokát / PhD. student, Department of Criminal Law, Criminology and Criminalistics, Faculty of Law, Comenius University in Bratislava, Slovak Republic / E-mail: rampasek1@uniba.sk / ORCID: 0009-0006-6997-0250

Keywords

Information Cybersecurity Manager; Ciso; Statutory Body; Legal Entity; Cybersecurity; Liability; Criminal Offense.

Úvod

Podstatným aspektom riadneho fungovania organizácie (typicky pôjde o právnickú osobu) je zabezpečenie ochrany jej informačných aktív v kybernetickom priestore. Nevyhnutným predpokladom tohto zabezpečenia je tiež prijatie adekvátnych bezpečnostných opatrení a určenie osoby zodpovednej za dodržiavanie kybernetickej bezpečnosti. Takouto osobou v zmysle slovenského zákona o kybernetickej bezpečnosti (ďalej „SZoKB“)[1] a vykonávacieho predpisu[2] k českému zákonu o kybernetickej bezpečnosti (ďalej „CZoKB“)[3] je manažér kybernetickej bezpečnosti,[4] označovaný tiež ako CISO *(Chief Information Security Officer)*[5] (ďalej „CISO“ alebo „MKB“). Rolu CISO je možno považovať za ekvivalent role MKB, ale tiež potrebné uviesť, že rola CISO vychádza z CxO systému označovania rolí v korporáciách. V praxi sa už začína zavádzať skratka MKB, ale na účely toho článku budeme ďalej požívať označenie CISO. CISO má byť v priamej línii podriadenosti štatutárneho zastúpenia umiestnený na úrovni B-1.[6] V praxi je manažér kybernetickej bezpečnosti akýmsi medzistupňom medzi vrcholovým vedením (strategickou úrovňou managementu) a operatívnou úrovňou.[7]

---

1 § 20 ods. 4 písm. a) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti v platnom znení (do 31. 12. 2024). Dňa 31. 5. 2024 bol zverejnený pod LP/2024/264 Zákon, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o zmene a doplnení niektorých zákonov, ktorý by mal byť v prípade schválenia účinný od 1. 1. 2025 (ďalej „Novela SZoKB“). Novela SZoKB nemení postavenie MKB avšak pridáva mu povinnosť vykonávať preverenie účinnosti prijatých opatrení podľa návrhu § 29 ods. 8, v rámci tzv. samohodnotenia. Dostupné z: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2024/264 [cit. 30. 5. 2024].

2 § 7 ods. 1 Vyhlášky č. 82/2018 Sb., rovnako bezpečnostní role NÚKIB. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf [cit. 30. 5. 2024]. Dňa 29. 5. 2024 bol zverejnený nový návrh zákona o kybernetické bezpečnosti s plánovanou účinnosťou od 18. 10. 2024 (ďalej „Nový CZoKB“) spolu s návrhom vykonávajúcich predpisov. Z návrhu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností vyplýva, že rola MKB bude povinne určená len pre poskytovateľov regulovanej služby v režime vyšších povinností. Dostupné z: https://www.odok.cz/portal/veklep/material/ALBSCSSFKU7S/ [cit. 30. 5. 2024].

3 Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

4 Najmä v komerčnom prostredí sa rola manažéra kybernetickej bezpečnosti zvyčajne uvádza pod skratkou CISO, ktorú používame v ďalšom texte. Pozri tiež MAKATURA, I. *Základy bezpečnostných opatrení. Príručka manažéra kybernetickej bezpečnosti*. Žilina: EUROKÓDEX, 2023, s. 22. DOI: https://doi.org/10.62874/afi.2023.1.06

5 Používa sa tiež označenie Chief security officer (CSO), porov. taktiež ibid.

6 Manažér úrovne B je manažér strednej úrovne v organizácii, ktorý pomáha realizovať politiky a iniciatívy vytvorené vedúcimi pracovníkmi organizácie na úrovni C (štatutárne vedenie).

7 Bezpečnostní role NÚKIB verzia 3.1 online. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf [cit. 21. 4. 2024].

Článok sa zameriava na oblasť posudzovania zraniteľností a riešenia kybernetického bezpečnostného incidentu (ďalej „incident“) z hľadiska zodpovednosti CISO a vymedzenia jeho zodpovednosti voči štatutárnemu zástupcovi. Na podklade analyzovaných súdnych konaní vedených voči CISO v USA a našich poznatkov formulujeme predpoklady vzniku trestnoprávnej zodpovednosti MKB v slovenskom a českom právnom poriadku pri riešení incidentu a súvisiacich okolností, ktoré predchádzajú jeho vzniku.

1 Postavenie a zodpovednosť MKB

1.1 Postavenie MKB

MKB riadi aplikáciu bezpečnostných opatrení,[8] tiež sa zaoberá riešením incidentu a má za úlohu riadenie všetkých postupov súvisiacich s oznamovaním, odhaľovaním, analýzou a reakciou na incident. Zároveň je spravidla aj kontaktnou osobou vo vzťahu k slovenskému Národnému bezpečnostnému úradu (ďalej „NBÚ“) resp. českému Národnímu úřadu pro kybernetickou a informační bezpečnost (ďalej „NÚKIB“), resp. národnej jednotke CSIRT (SK-CERT a CSIRT.CZ)[9], prípadne vládnej jednotke a akreditovanej jednotke CSIRT[10] (GovCERT.CZ a Vládna jednota CSIRT) (spoločne „CSIRT“). To osobitne platí pri subjektoch regulovaných právnymi predpismi v oblasti kybernetickej bezpečnosti, (v súčasnosti predovšetkým prevádzkovateľoch základnej služby a poskytovateľoch digitálnej služby). Po transpozícií smernice EÚ č. 2022/2555[11] (ďalej „smernica NIS2“) na ktorej základe dôjde k zmene kategorizácie, rozsahu a označenia regulovaných subjektov, pričom na Slovensku by sa mali označovať ako „prevádzkovateľ základnej služby“ a v Čechách „poskytovatel regulované služby“[12] (ďalej spoločne „regulované subjekty“).[13] Regulované subjekty sú povinné určiť osobu, ktorá bude vykonávať rolu manažéra kybernetickej bezpečnosti ako súčasť bezpečnostných opatrení.[14]

---

8 § 20 ods. 4 písm. a) SZoKB, ďalej tiež § 17d vyhlášky NBÚ č. 362/2018 Z.z. ako aj vyhláška NBÚ č. 492/2022 Z.z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

9 V SR plní úlohy národnej jednotky CSIRT, Národné centrum kybernetickej bezpečnosti SK-CERT ako súčasť Národného bezpečnostného úradu. V ČR národný CSIRT zaisťuje organizácia CZ.NIC.

10 Jednotka pre riešenie počítačových bezpečnostných incidentov, v angl. *Computer Security Incident Response Team* (CSIRT).

11 Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

12 Niektoré členské štáty EÚ sa rozhodli neprevziať označenie regulovaných subjektov používané v smernici NIS2, t.j. kľúčové subjekty a dôležité subjekty.

13 V ČR sú doposiaľ osobitne regulovanými aj správca a prevádzkovateľ informačného systému kritické informační infraštruktúry, správca a prevádzkovateľ komunikačného systému kritické informační infraštruktúry, správca a prevádzkovateľ významného informačného systému a ďalšie subjekty podľa § 3 CZoKB. V SR sa pod základnou službou rozumie aj prvok kritickej infraštruktúry a orgány verejnej moci, pričom v súvislosti s prevádzkou informačných technológií verejnej správy platí aj osobitná právna úprava zákonom č. 95/2019 Z.z. o informačných technológiách verejnej správy v platnom znení.

14 § 20 ods. 4 písm. a) SZoKB, a § 6 ods. 3 Vyhlášky č. 82/2018 Sb.

MKB má právnymi predpismi priamo ustanovené nasledovné požiadavky a povinnosti:[15]

1) *predkladá návrhy a oznamuje* informácie v oblasti informačnej a kybernetickej bezpečnosti *priamo štatutárnemu orgánu* prevádzkovateľa základnej služby,
2) *riadi aplikáciu bezpečnostných opatrení* v rámci systémov manažérstva,
3) je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií, a
4) spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti podľa osobitného predpisu.

Aplikáciou (alebo tiež *implementáciou)* bezpečnostných opatrení v systéme riadenia informačnej bezpečnosti sa rozumie najmä niekoľko základných úloh v cykle opatrení:

1) navrhovanie rozpočtu, súvisiaceho s bezpečnostnými opatreniami,
2) riadenie implementácií bezpečnostných opatrení (organizačných aj technických),
3) zaručenie bežnej prevádzky technických bezpečnostných opatrení,
4) zaručenie udržateľnosti organizačných opatrení vrátane bezpečnostných procesov.[16]

Právnymi predpismi je však určený iba základný rámec, resp. minimálne požiadavky, kladené na MKB. Vo všeobecnosti MKB zaisťuje ochranu informačných aktív organizácie implementáciou a riadením procesov informačnej a kybernetickej bezpečnosti. Organizuje výkon činností právnickej osoby, súvisiaci so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe, najmä vo vzťahu k zraniteľnostiam a incidentom:

- zabezpečuje implementáciu technických a organizačných bezpečnostných opatrení,
- implementuje a zabezpečuje riadny chod procesov manažmentu bezpečnostných rizík a ošetrovania bezpečnostných hrozieb,
- navrhuje zmeny a optimalizáciu bezpečnostných riešení,
- riadi proces hodnotenia technických zraniteľností systémov,
- riadi procesy detekcie, riešenia a prevencie incidentov.[17]

1.2 Zodpovednosť MKB

V oblasti riadenia kybernetickej bezpečnosti je štatutárna zodpovednosť za riadenie bezpečnosti *(SecurityGovernance)* oddelená od výkonnej zodpovednosti za riadenie bezpečnosti *(SecurityOperations)*.[18]

Riadiaca autorita reprezentuje štatutárnu zodpovednosť. Zodpovednosť štatutárneho orgánu (spravidla zároveň CEO) vyplýva priamo zo všeobecne záväzných právnych predpisov. Táto zodpovednosť sa neobmedzuje len na reguláciu v oblasti kybernetickej bezpečnosti, ale aj na zodpovednosť za dodržiavanie kybernetickej bezpečnosti, ktorá je súčasťou

15 § 17d Vyhlášky NBÚ č. 362/2018 Z.z. a § 7 ods. 1 Vyhlášky č. 82/2018 Sb.

16 Bezpečnostné opatrenia. *Kompetenčné a certifikačné centrum kybernetickej bezpečnosti* [online]. [cit. 21. 4. 2024]. Dostupné z: https://cybercompetence.sk/casto-kladene-otazky-opatrenia/

17 Riadenie KB. *Kompetenčné a certifikačné centrum kybernetickej bezpečnosti* [online]. [cit. 21. 4. 2024]. Dostupné z: https://cybercompetence.sk/casto-kladene-otazky-riadenie-kb/

18 MAKATURA, 2023, op. cit., s. 20.

širšej povinnosti vykonávať svoju pôsobnosť s odbornou starostlivosťou a v súlade so záujmami právnickej osoby a všetkých jej spoločníkov (akcionárov).[19] Zvýrazňujeme, že protiprávny čin člena štatutárneho orgánu právnickej osoby pri výkone jeho funkcie ako aj konanie inej osoby ako je štatutárny orgán alebo jeho člen, môže založiť jej trestnú zodpovednosť (pri splnení ďalších zákonných podmienok), pretože ide o trestný čin spáchaný právnickou osobou.[20] Trestná zodpovednosť môže byť vyvodená tak voči členovi štatutárneho orgánu (fyzickej osobe)[21] a súčasne voči právnickej osobe.[22] Trestnoprávnu zodpovednosť právnickej osoby nemôže založiť protiprávny čin člena jej štatutárneho orgánu, ktorý konal na jej úkor, proti jej záujmom, prípadne, ak by zneužil právnickú osobu k spáchaniu trestného činu.[23]

MKB na **výkonnej úrovni** zodpovedá za každodenné operatívne činnosti v oblasti informačnej a kybernetickej bezpečnosti (Security Operations). Z pohľadu skúmania v tomto článku osobitne nerozlišujeme, či sú úlohy MKB vykonávané internými kapacitami alebo dodávateľsky (čo je bežná prax najmä v prípade menších právnických osôb). Trestná zodpovednosť môže byť vyvodená voči nemu v prípade, ak naplní zákonné znaky trestného činu. Jeho protiprávny čin tiež môže založiť trestnú zodpovednosť právnickej osoby.[24]

Zvýrazňujeme, že v článku sa zameriavame najmä na zodpovednosť a povinnosti štatutárneho orgánu, generálneho riaditeľa (CEO) a MKB. Avšak, konanie a zodpovednosť, ktoré sú podrobne rozobrané v tomto článku, sa môžu týkať aj ďalších osôb. Okrem vyššie uvedených môže ísť aj o vlastníkov aktív, ktorí sú zodpovedný za aktívum v ich správe. Ďalej sa môžu dotýkať aj iných zamestnancov, ktorí majú vplyv na správu a ochranu firemných

19 V slovenskom právnom poriadku pozri najmä § 135a ods. 1, 194 ods. 5 Obchodného zákonníka. V prípade iných osôb pozri § 66 ods. 7 Obchodného zákonníka. V českom právnom poriadku všeobecne pozri najmä § 159 ods. 1, § 163, 164 ods. 1, § 454, § 1411 Občanského zákoníka a § 49 a § 51 až § 53 zákona č. 90/2012 Sb. o obchodních společnostech a družstvech (zákon o obchodních korporacích). Podrobnejšie pozri PÚRY, F. Možnosti postihu porušení povinnosti péče řádného hospodáře o cizí majetek. *Právní rozhledy*. 2010, č. 5, s. 541–553. GŘIVNA, T. Porušení péče řádného hospodáře z pohledu trestního práva ČR. In: HAVEL, B., ŽITŇANSKÁ, L. (eds.). *Fiduciární povinnosti orgánů společnosti na pomezí korporačního, insolvenčního a trestního práva*. Wolters Kluwer ČR, Praha 2020, s. 43. ČENTÉŠ, J., BELEŠ, A., ŠANTA, J. Porušovanie povinnosti pri správe cudzieho majetku – rozhodovacia činnosť súdov. In: FRYŠTÁK, M., BRUCKNEROVÁ, E. (eds.). *Nové jevy v ekonomické kriminalitě: sborník příspěvků z mezinárodní konference*. 1. vyd. Brno: Masarykova univerzita, 2020, 240 s., s. 30 a nasl. SZABOVÁ, E. Vybrané otázky trestnoprávnej zodpovednosti členov kolektívnych orgánov obchodných spoločností s dôrazom na proces dokazovania. In: FRYŠTÁK, M., BRUCKNEROVÁ, E. (eds.). *Nové jevy v ekonomické kriminalitě: sborník příspěvků z mezinárodní konference*. 1. vyd. Brno: Masarykova univerzita, 2020, 240 s., s. 60.

20 V slovenskom právnom poriadku pozri najmä § 4 ods. 1, ods. 2 zákona o trestnej zodpovednosti právnických osôb. V českom právnom poriadku pozri najmä § 8 ods. 1 písm. a) až d), ods. 2 písm. b), § 9 ods. 3 zákona o trestní odpovědnosti právnických osob.

21 Pozri § 128 ods. 8 slovenského Trestného zákona a § 114 ods. ods. 1, ods. 2 trestného zákoníku. Pozri tiež Rč 47/2001, Rč 36/2020.

22 V slovenskom právnom poriadku pozri najmä § 4 zákona o trestnej zodpovednosti právnických osôb. V českom právnom poriadku pozri najmä § 8 ods. 1 a § 9 ods. 3 zákona o trestní odpovědnosti právnických osob. Pozri tiež Rč 18/2006-II a nadväzujúci Rč 41/2010 a Rč 131/2017.

23 Rč 29/2017. Pozri tiež § 8 ods. 5 zákona o trestní odpovědnosti právnických osob a R č 50/2020.

24 V slovenskom právnom poriadku pozri najmä § 4 ods. 3 zákona o trestnej zodpovednosti právnických osôb. V českom právnom poriadku pozri najmä § 8 ods. 1 písm. d), odst. 2 písm. b) zákona o trestní odpovědnosti právnických osob. Pozri tiež Rč 17/2022.

údajov a systémov. Taktiež je dôležité zohľadniť rolu zamestnancov a poradcov, ktorí môžu mať priamu alebo nepriamu zodpovednosť vo vzťahu k riadeniu incidentov. Zároveň uvádzame, že konaním štatutárneho orgánu, či MKB môže vzniknúť trestnoprávna zodpovednosť aj podľa zákona o trestní odpovědnosti právnických osob/zákona o trestnej zodpovednosti právnických osôb.

1.3 MKB a samohodnotenie regulovaného subjektu

V dôsledku novelizovania právnej úpravy v oblasti kybernetickej bezpečnosti, najmä transpozície smernice NIS2 očakávame, že počet regulovaných subjektov výrazne stúpne. Podľa odhadov NBÚ[25] tak len v Slovenskej republike môže byť priamo regulovaných takmer 700 právnických osôb, ktoré sú veľkým podnikom.[26] Je preto zrejmé, že dostupné kapacity certifikovaných auditov kybernetickej bezpečnosti nebudú postačovať na vykonávanie auditov všetkých regulovaných subjektov. Pre väčšiu časť slovenských regulovaných subjektov (t.j. prevádzkovateľov základnej služby, ktorí neposkytujú kritickú základnú službu) bude „opätovne" zavedená možnosť zjednodušeného spôsobu overenia miery implementácie bezpečnostných opatrení, tzv. samohodnotenie.[27]

Medzi rokmi 2021 až 2023 SZoKB ustanovoval možnosť zjednodušeného spôsobu overenia miery implementácie požiadaviek na kybernetickú bezpečnosť. Mieru implementácie požiadaviek tohto zákona bolo možné overiť aj prostredníctvom tzv. samohodnotenia. Samohodnotenie pritom nahrádzalo potrebu auditu kybernetickej bezpečnosti, ktoré mohlo byť použité iba prevádzkovateľmi základných služieb, ktorí nemali identifikovanú III. kategóriu informačných systémov. V praxi sa teda samohodnotenie týkalo len subjektov, ktorí nemali kritické informačné aktíva.

Podstatou samohodnotenia je posúdiť účinnosť prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených SZoKB manažérom kybernetickej bezpečnosti.[28] Regulovaný subjekt, resp. v jeho mene MKB musia vedieť preukázať pravdivosť odpovedí uvádzaných v samohodnotení. Súčasťou samohodnotenia je aj plán implementácie opatrení kybernetickej bezpečnosti na nasledujúce obdobie. Pravdivosť informácií zaznamenaných

---

25 Odhadovaný počet regulovaných subjektov prezentovaný na stretnutí „Cyber breakfast", ktoré sa uskutočnilo 17. 1. 2024 v Bratislave.

26 I keď nemožno vylúčiť že regulovaným subjektom môže byť aj fyzická osoba / podnikateľ, vo väčšine prípadov pôjde o právnickú osobu. Podľa odporúčania Európskej komisie č. 2003/361/EC sa stredným podnikom rozumie podnik, ktorý zamestnáva aspoň 50 osôb a jeho ročný obrat a/alebo celková ročná bilančná hodnota presahuje 10 miliónov Eur. Veľkým podnikom sa rozumie podniky, ktoré zamestnávajú aspoň 250 osôb a u ktorých ročný obrat presahuje 50 miliónov € a/alebo celková ročná bilancia nepresahuje 43 miliónov €.

27 Podľa navrhovaného ustanovenia § 29 ods. 8 Novely SZoKB, prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite určenej osobitným predpisom zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom (pozn. teda samohodnotením, tento pojem je priamo použitý v návrhu § 32 ods. 1 písm. e) Novely SZoKB). Takýto prevádzkovateľ základnej služby je však povinný podrobiť sa auditu kybernetickej bezpečnosti do šiestich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity určenej osobitným predpisom.

28 Rovnako, § 29 ods. 8 Novely SZoKB explicitne určuje, že samohodnotenie vykonáva MKB.

do samohodnotenia sa overuje a skúma na základe aktuálneho stavu v prostredí regulovaného subjektu v konkrétnom čase. Na preukázanie svojich zistení si MKB má povinnosť zadovážiť od regulovaného subjektu potrebné dokumenty, na základe ktorých vie zodpovedať na otázky uvedené v predmetnom formulári.[29]

V Českej republike ani súčasná úprava CZoKB ani Nový CZoKB neupravuje inštitút samohodnotenia a to vzhľadom odlišný prístup českého zákonodarcu k povahe preverovania opatrení kybernetickej bezpečnosti. Preverovanie zavedených bezpečnostných opatrení sa vykonáva prostredníctvom (interného) audítora kybernetickej bezpečnosti[30], ktorý je bezpečnostnou rolou u poskytovateľa regulovanej služby a kontrol zo strany NÚKIB.

2 Riadenie zraniteľností a riešenie incidentov

Incident je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov alebo tiež vysoká pravdepodobnosť kompromitácie činností služby alebo ohrozenie bezpečnosti informácií.[31] Zjednodušene povedané incident je nielen už realizovaná aktuálna hrozba pre bezpečnosť informácií[32] ale aj už hrozba, ktorá môže viesť k závažnému incidentu.[33] Kľúčovú úlohu v riadení vyšetrovania a nápravy následkov incidentov zohráva práve MKB.

Základný rámec postupu pri incidente v režime SZoKB je postavený na 5 pilieroch.[34]

1) riešiť incident,
2) bezodkladne hlásiť incident[35] na jednotku CSIRT (popri dobrovoľnom hlásení akéhokoľvek incidentu),
3) spolupracovať s jednotkou CSIRT pri riešení hláseného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie incidentu,

[29] Porovnaj Metodické usmernenie NBÚ: Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti. *NBÚ* [online]. [cit. 21. 4. 2024]. Dostupné z: https://www.nbu.gov.sk/samohodnotenie-v-zmysle-zakona-o-kybernetickej-bezpecnosti/

[30] V Slovenskej republike môže audit kybernetickej bezpečnosti vykonať len certifikovaný audítor kybernetickej bezpečnosti, ktorý nie je v žiadnom vzťahu k regulovanému subjektu.

[31] Porovnaj článok 6 bod 6 smernice NIS2, § 3 písm. k) SZoKB.

[32] NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Praha: WoltersKluwer ČR, 2022, s. 8.

[33] MAKATURA, 2023, op. cit., s. 113.

[34] Primerane aj § 19 ods. 6 SZoKB.

[35] Rôzne právne predpisy môžu stanoviť povinnosť hlásenia len určitej kategórie (typicky závažnejších, resp. s podstatným vplyvom) incidentov, ako je tomu aj v súčasnom znení § 19 ods. 6 a § 22 ods. 3 ZoKB. Rovnako tak smernica NIS2 upravuje postup hlásenia „významného" incidentu. Na druhej strane regulované subjekty vo verejnom sektore, oznamujú povinne každý incident, porov. § 23 ods. 3 písm. a) zákona č. 95/2019 Z.z. o ITVS. Preto považujeme za vhodnejšie neuvádzať kategóriu incidentu, resp. používať spoločne len označenie „incident" bez ohľadu na jeho závažnosť.

4) v čase incidentu zabezpečiť stopy (dôkaz alebo dôkazný prostriedok) tak, aby mohol byť použitý v trestnom konaní,[36]
5) oznámiť orgánu činnému v trestnom konaní skutočnosti, že bol spáchaný trestný čin, ktorého sa incident týka, ak sa o ňom hodnoverným spôsobom dozvie.[37]

Riešením incidentu sa rozumejú všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na incident a s obmedzením jeho následkov.[38] Kľúčovou súčasťou procesu riešenia incidentu je posúdenie zhromaždených informácií o bezpečnostnej udalosti, rozhodnutie či táto udalosť je incidentom. Nasleduje klasifikácia incidentu a rozhoduje o prioritizácii incidentu, teda klasifikácii incidentu podľa dopadu či náročnosti na riešenie.[39] Tieto povinnosti sú podľa nášho názoru natoľko kľúčové, že nie sú len zákonnou povinnosťou pre regulované subjekty. Pre neregulované subjekty ich možno posúdiť prinajmenšom ako dobrú prax a tiež ako povinnosti vyplývajúce z iných všeobecne záväzných právnych predpisov (predovšetkým pôjde o povinnosť štatutárnych orgánov konať s odbornou starostlivosťou; všeobecnú povinnosť právnických osôb bez meškania oznámiť skutočnosti nasvedčujúce spáchaniu trestného činu[40]) alebo z technických noriem, ktoré sa subjekt zaviazal dobrovoľne dodržiavať, typicky normami rady ISO/IEC 27000 (povinnosti riešiť incident, zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní).[41]

Zvýrazňujeme, že povinnosti pri riešení incidentu ako aj oznamovaciu povinnosť pritom odvodzujeme zo všeobecnej prevenčnej povinnosti podľa súkromného práva (§ 415 Občianskeho zákonníka), a to aj pre subjekty v neregulovanom prostredí.[42] Preto hoci v ďalšom texte uvádzame predovšetkým odkazy na reguláciu v oblasti kybernetickej bezpečnosti, základný rámec postupu pri riešení incidentu sa dotýka aj v subjektov, na ktoré nedopadá špecifická regulácia kybernetickej bezpečnosti.

Oznamovaciu (notifikačnú) povinnosť tiež vnímame v širšom zmysle aj z pohľadu zahrnutých subjektov, teda nie je len voči notifikovanému subjektu[43], ale aj ako povinnosť oznámiť incident dotknutým osobám[44], klientom, dodávateľom a odberateľom. Oznamovacia

36 Obdobná povinnosť pre české regulované subjekty z CZoKB ani Nového CZoKB nevyplýva. K elektronickým dôkazom pozri POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. s. 225–226.

37 Obdobná povinnosť pre české regulované subjekty z CZoKB ani Nového CZoKB nevyplýva.

38 Porovnaj § 3 písm. p) SZoKB. Obdobne § 14 Vyhlášky č. 82/2018 Sb.

39 NONNEMANN, ČERVENÝ, VÍTEK, op. cit., s. 143.

40 Porovnaj § 3 ods. 2 Trestného poriadku. KURILOVSKÁ, L. § 3 Súčinnosť štátnych orgánov, právnických osôb a fyzických osôb. In: ČENTÉŠ, J., KURILOVSKÁ, L., ŠIMOVČEK, I., BURDA, E. a kol. *Trestný poriadok I*. 1. vyd. Bratislava: C. H. Beck, 2021, s. 54, marg. č. 2.

41 Porovnaj opatrenia 5.26 až 5.28 (Príloha A) podľa normy STN ISO/IEC 27001:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2022).

42 Rovnako porov. NONNEMANN, ČERVENÝ, VÍTEK, op. cit., s. 175.

43 Ibid.

44 Podľa článku 23 ods. 1 Smernice NIS2 sú regulované subjekty povinné bez zbytočného odkladu oznámiť príjemcom svojich služieb významné incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb.

povinnosť by sa naviac onedlho nemala vzťahovať len na incident, resp. hrozbu, ale aj na (i) významnú kybernetickú hrozbu, o ktorej sa dozvie, (ii) udalosť odvrátenú na poslednú chvíľu, ktorá mohla spôsobiť závažný incident a (iii) zraniteľnosť prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika.[45]

V českom trestnom práve neplatí pre trestné činy súvisiace s kybernetickými útokmi oznamovacia povinnosť (vzhľadom na formuláciu skutkovej podstaty trestného činu neoznámenie trestného činu podľa § 368 trestního zákoníka, bližšie k tomu pozri ďalší text). Napriek tomu oznámenie incidentu orgánom činným v trestnom konaní, môže byť najmä pri závažnejších incidentoch alebo incidentoch so zjavným zapojením tretej strany, útočníka, podľa okolností vnímané aj ako povinnosť napadnutej právnickej osobe a jej vedenia, ktoré je povinné konať so starostlivosťou riadneho hospodára.[46]

2.1 Prípad Uber

V prípadoch zavineného porušenia povinností, môže aj MKB niesť (trestnoprávnu) zodpovednosť za (ne)riešenie incidentov, ako aj za neošetrenie známej zraniteľnosti; tým nie je vylúčená zodpovednosť aj iných osôb napr. vlastníkov (garantov) aktív [uvedené však presahuje predmet tohto článku a preto sa mu ďalej nevenujeme – pozn. aut.].

Uvedené tvrdenie o zodpovednosti MKB podporujeme aj prípadom *Spojené štáty proti Sullivanovi*. Pán Sullivan, v čase spáchania skutku CISO v spoločnosti Uber Technologies, Inc. (ďalej „Uber"), bol uznaný vinným z trestných činov marenia konania vedeného Federálnou obchodnou komisiou *(United States Federal Trade Commission*, ďalej „FTC") a neoznámenia trestného činu v súvislosti s jeho pokusom o utajovanie incidentu v spoločnosti Uber z roku 2016. Za to mu bol okresným súdom Severného dištriktu štátu Kalifornia ako súdom prvého stupňa v roku 2023 uložený podmienečný trest odňatia slobody na tri roky odňatia slobody, trest verejnoprospešných prác 200 hodín a pokuta 50 000 dolárov.[47] Uloženiu trestu predchádzal verdikt poroty.[48] Súd zamietol návrh obvineného na nové

45 Porov. § 24 ods. 5 novely SZoKB.

46 NONNEMANN, ČERVENÝ, VÍTEK, op. cit., s. 171.

47 Trestný spis je dostupný z: https://urtlistener.com/docket/18414184/united-states-v-sullivan/?page=2 [cit. 21. 4. 2024].

48 Verdikt poroty zo dňa 5. 10. 2022. In: *CourtListener.com* [online]. [cit. 21. 4. 2024]. Dostupné z: https://storage.courtlistener.com/recap/gov.uscourts.cand.365508/gov.uscourts.cand.365508.224.0.pdf

konanie pred súdom.[49] Trestné konanie pána Sullivana ako prvé[50] odsúdenie CISO vyvolalo značný ohlas v odbornej verejnosti.[51]

V tomto prípade podľa dostupných informácií FTC v čase incidentu (november 2016) vyhodnocovala program a postupy ochrany bezpečnosti údajov Uberu v reakcii na predchádzajúci incident ešte z roku 2014. FTC vypočula Sullivana, ktorý opísal postupy Uberu v oblasti bezpečnosti údajov vrátane ukladania prístupových kľúčov, používania služieb Amazon Web Services a možných zraniteľností. Desať dní po výsluchu Sullivan dostal e-mail od „neznámeho aktéra", ktorý odhalil, že hackeri sa dostali k údajom Uberu. Sullivan sa mal dozvedieť, že Uber bol opätovne napadnutý v dôsledku rovnakých nedostatočných bezpečnostných postupov, ktoré viedli k incidentu v roku 2014, čo malo za následok stratu ešte väčšieho množstva údajov o zákazníkoch a vodičoch, ako počas incidentu v roku 2014. Toto druhé napadnutie odhalilo, že predchádzajúce vyhlásenia Uberu pre FTC o šifrovacích postupoch a rozsahu prístupu zamestnancov Uberu k takýmto údajom – vrátane tých, ktoré Sullivan opísal vo svojom výsluchu malo byť nepravdivé.

V reakcii na incidenty tím Uberu mal pracovať na ich zvládnutí, komunikoval s hackermi, aby potvrdili, že incident nebol podvod, a potom určili jeho rozsah. Uber zdokumentoval svoj postup spolu s nevyriešenými problémami. Tento dokument obsahoval tiež komentáre porovnávajúce povahu incidentu z roku 2016 so Sullivanovým svedectvom pred FTC o postupoch spoločnosti Uber v oblasti bezpečnosti údajov. Súčasťou dokumentu bol komentár od Sullivana, že „toto môže tiež skončiť veľmi zle na základe predchádzajúcich tvrdení" a že to odkazuje na „tvrdenia FTC" týkajúce sa prístupu k údajom a šifrovania a zdôraznil potrebu utajenia zistených skutočností. Sullivanov priamy nadriadený Flynn vypovedal, že Sullivan mu pri diskusii o incidente povedal: „Toto sa nemôže dostať von". Flynn ďalej vypovedal, že Sullivan sa mu zmienil: „Len nedávno som vypovedal pred FTC" a povedal, že „niečo na týchto dvoch problémoch" – vrátane únikov údajov v rokoch 2014 a 2016 – „bolo podobné". Tímu Uberu pre reakciu na incidenty tiež povedal, že „toto musíme mať pod prísnou kontrolou" a že „komunikuje priamo s A tímom", čo je prezývka pre vrcholových manažérov Uberu, ktorí sú priamo podriadení jeho výkonnému riaditeľovi (CEO).

---

49 Rozhodnutie súdu o odmietnutí návrhu na oslobodenie a na nové súdne konanie. Dostupné z: https://storage.courtlistener.com/recap/gov.uscourts.cand.365508/gov.uscourts.cand.365508.250.0.pdf [cit. 21. 4. 2024]. K uvedenému je zaujímavé aj stanovisko obžaloby. Dostupné z: https://storage.courtlistener.com/recap/gov.uscourts.cand.365508/gov.uscourts.cand.365508.254.0.pdf [cit. 21. 4. 2024].

50 K dňu 5. 6. 2024 však nie ešte právoplatné.

51 SACK, J. S., HURLEY, Ch. M. Cybersecurity and Individual Liability: 'U.S. v. Sullivan' and the Criminalization of a Cyber Attack Response. In: *New York Law Journal*. [online]. 6. 5. 2022 [cit. 21. 4. 2024]. Dostupné z: https://www.maglaw.com/media/publications/articles/2022-05-09-cybersecurity-and-individual-liability-united-states-v-sullivan-and-the-criminalization-of-a-cyber-attack-response/_res/id=Attachments/index=0/NYLJ5052022549925Morvillo.pdf. Tiež VIJAYAN, J. Judge Spares Former Uber CISO Jail Time Over 2016 Data Breach Charges. *DARKREADING* [online]. 5. 5. 2023 [cit. 21. 4. 2024]. Dostupné z: https://www.darkreading.com/cyberattacks-data-breaches/judge-spares-former-uber-ciso-jail-time-over-2016-data-breach-charges a BEAUBURN, G. a kol. Ex-Uber CSO Joseph Sullivan Sentenced to Probation: The Do's and Don'ts of Responding to Data Breaches. *Arnold & Porter* [online]. 9. 5. 2023 [cit. 21. 4. 2024].. Dostupné z: https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2023/05/ex-uber-cso-sentenced-to-probation

Po tom, čo sa tím dozvedel, že hackeri získali čísla vodičských preukazov, Sullivan sa opýtal Clarka: *„Ako to môžeme zaradiť pod bug bounty* [program][52]*?"*, čo tento pochopil ako pokyn na nájdenie spôsobu, ako dosiahnuť, že incident z roku 2016 bude zaradený v rámci programu Uber pre odmeňovanie za nahlásenie zraniteľnosti treťou stranou *(bug bounty program)*. Podľa Clarka mu Sullivan neskôr povedal, že *„budeme to považovať za odmenu za nahlásenie zraniteľnosti."* Jeden z hackerov vypovedal, že vyjednával s jedným zo zamestnancov Uberu o platbe v sume 100 000 USD, ktorá výrazne prevyšuje maximálnu výšku odmeny za oznámenie zraniteľností od Uberu (10 000 USD) ako výmenu za to, že podpísali dohodu o mlčanlivosti (ďalej „NDA"). V NDA sa uvádzalo, že Uber zaplatí hackerom 100 000 USD, ak sa zaviažu, že *„nevezmú ani neuložia žiadne údaje počas alebo prostredníctvom* [ich] *výskumu"* a *„doručili* [spoločnosti Uber] *alebo forenzne zničili všetky informácie o a/alebo analýzy zraniteľností."* NDA tiež požadovala, aby sa hackeri zaviazali, že *„neprezradili a neprezradia čokoľvek o zraniteľnostiach alebo* [ich] *dialógu s* [Uberom] *komukoľvek pre akýkoľvek účel bez písomného súhlasu* [Uberu]*."* Výmenou za to, sa Uber v NDA zaviazal, že *„si neuplatní nároky podľa civilného alebo trestného práva"* proti hackerom za ich *„aktivitu a výskum"*, pokiaľ neporušia niektorý zo svojich vlastných záväzkov. V konaní boli predložené dôkazy, ktoré preukazovali úpravy vykonané v NDA, ktoré mal vykonať priamo Sullivan.

V konaní Sullivan namietal, že neboli naplnené všetky znaky skutkových podstát trestných činov uvedených v obžalobe. Tvrdil napríklad, že v súvislosti s trestným činom marenia konania pred FTC, dôkazy nie sú dostatočné na to, aby bola preukázaná príčinná súvislosť medzi jeho konaním a konaním pred FTC.

Pre naplnenie skutkovej podstaty trestného činu marenia konania pred ministerstvami, agentúrami a výbormi (18 U.S. Code § 1505)[53] sa vyžaduje preukázanie: (1) že došlo ku konaniu pred agentúrou; (2) že páchateľ o tomto konaní vedel; a (3) že páchateľ sa *úmyselne snažil hrubo ovplyvniť, mariť alebo brániť prebiehajúcemu konaniu*.

Podľa súdu naplnenie obligatórnych znakov posudzovaného trestného činu nevyžaduje preukázanie príčinnej súvislosti medzi konaním páchateľa a konaním pred vládnou agentúrou. Odsúdenie môže byť založené aj na opomenutí páchateľa, na rozdiel od jeho aktívneho konania. Prvostupňový súd poukázal na to, že pojem „hrubo" (corruptly) zahŕňa nepravdivé alebo zavádzajúce vyhlásenia alebo zadržania, zatajenia, pozmenenia alebo zničenia dokumentu alebo inej informácie. Zadržanie a zatajenie informácie je naplnené aj bez odkazu na povinnosť nahlásiť incident.

52 Bug bounty program je iniciatíva, v rámci ktorej organizácia odmeňuje jednotlivcov alebo skupiny za objavenie a hlásenie softvérových chýb (bugov) alebo zraniteľností, ktoré môžu ohroziť bezpečnosť alebo správne fungovanie systému.

53 Text skutkovej podstaty trestného činu je dostupný z: https://www.law.cornell.edu/uscode/text/18/1505 [cit. 21. 4. 2024]. V slovenskej právnej praxi je snáď najbližšie tomuto trestnému činu, trestný čin marenia spravodlivosti podľa § 344 Trestného zákona, najmä ak niekto úmyselne v trestnom konaní predloží dôkaz, o ktorom vie, že je sfalšovaný alebo pozmenený, na účel použiť ho ako pravý, prípadne falšuje, pozmení alebo marí dôkaz, alebo bráni v získaní dôkazu. Trestné činy, ktorým venujeme pozornosť z hľadiska slovenského Trestného zákona neboli zásadne zmenené v schválenom zákone č. 40/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon (…).

Trestného činu *neoznámenia trestného činu (18 U.S. Code § 4)*[54] sa dopustí páchateľ, ktorý vie o skutočnom spáchaní trestného činu (zločinu, *felony)*, ktorý môže byť prejednaný súdom Spojených štátov amerických, zatají a čo najskôr ho neoznámi sudcovi alebo inej osobe, ktorá má civilnú alebo vojenskú právomoc v rámci Spojených štátov amerických.

Pre naplnenie skutkovej podstaty uvedeného trestného činu sa vyžaduje preukázanie: *„(1) že hlavný páchateľ* […] *spáchal a dokonal uvedený zločin; (2) že páchateľ o tejto skutočnosti plne vedel; (3) že to neoznámil orgánom; a (4) že podnikol kroky na utajenie trestného činu hlavného páchateľa."*

Súd dospel k zisteniu, že platba 100 000 USD hackerom a NDA to podporujú, pričom poukázal na konkrétne ustanovenie, v ktorom sa hackeri zaviazali, že „nezverejnili a nezverejnia nič o zraniteľnostiach" alebo o svojich rozhovoroch so spoločnosťou Uber bez písomného povolenia. Súd konštatoval Sullivanovu vedomosť o konaní FTC vo vzťahu k incidentu z roku 2016, jeho poznámky o potrebe utajenia a snaha o zaradenie incidentu do programu odmeňovania *(bug bounty)* spoločnosti Uber a jeho účasť na vytvorení NDA zmluvy. Vykonaným dokazovaním bolo preukázané, že hackeri odcudzili obrovské množstvo osobných údajov a dostali 100 000 USD, keď boli ešte anonymní, pod podmienkou, že nikomu inému nepovedia, čo urobili.

V súhrne bolo podľa rozsudku v konaní preukázané, že:

1) pred FTC prebiehalo konanie,
2) Sullivan o tomto konaní vedel,
3) úmyselne sa snažil konanie významne ovplyvniť, mariť a brániť v zisteniu relevantných skutočností,
4) dôkazy boli dostatočné na odsúdenie za marenie konania.

Rovnako podľa rozsudku boli dôkazy dostatočné na odsúdenie Sullivana za neoznámenie trestného činu, pretože boli splnené nasledovné podmienky:

1) spáchanie federálneho trestného činu (v tomto prípade „úmyselný prístup k počítaču bez oprávnenia a tým získanie informácií z chráneného počítača alebo sprisahanie s cieľom vylákať peniaze prostredníctvom hrozby narušenia dôvernosti informácií získaných z chráneného počítača bez oprávnenia"), vedel o spáchaní tohto zločinu,
2) vedel, že toto konanie je federálnym zločinom,
3) neoznámil uvedené okolnosti federálnym orgánom,
4) vykonal činnosť s cieľom utajiť trestný čin.

V súčasnosti prebieha odvolacie konanie, nakoľko Sullivan podal odvolanie voči odsudzujúcemu rozsudku.

54 Text skutkovej podstaty trestného činu je dostupný z: https://www.law.cornell.edu/uscode/text/18/4 [cit. 21. 4. 2024]. V slovenskej právnej praxi je tento trestný čin podobný trestnému činu neoznámenia trestného činu podľa § 340 Trestného zákona.

2.2 Prípad SolarWinds

Snaha o vyvodenie individuálnej zodpovednosti CISO vyvrcholila v októbri 2023, keď americká Komisia pre cenné papiere a burzu *(Securities and Exchange Commission*, ďalej „SEC") podala civilnú žalobu na spoločnosť SolarWinds Corp. (ďalej „SolarWinds")[55] a fyzickú osobu Browna za jeho úlohu v tom, čo SEC nazýva úmyselné dezinformácie o bezpečnostných zraniteľnostiach spoločnosti.[56] Ide pritom o prvú žalobu SEC takéhoto druhu a naviac aj voči fyzickej osobe, CISO.

SEC v obžalobe tvrdí, že najneskôr od októbra 2018 do minimálne 12. januára 2021 spoločnosť SolarWinds a Brown podvádzali investorov a zákazníkov SolarWinds prostredníctvom nesprávnych vyhlásení, opomenutí a schém, ktoré zakrývali nesprávne a nedostatočné opatrenia kybernetickej bezpečnosti v spoločnosti a jej zvýšené a zvyšujúce sa bezpečnostné riziká. Útok (ktorý sa stal známy pod označením SUNBURST), kompromitoval softvérovú platformu Orion, ktorú spoločnosť SolarWinds považovala za najcennejšie aktívum *(crownjewel)* a ktorý predstavoval 45 % jej príjmov v roku 2020. SolarWinds a/alebo Brown mali urobiť podstatne nepravdivé a zavádzajúce vyhlásenia a opomenutia súvisiace s rizikami a postupmi spoločnosti SolarWinds v oblasti kybernetickej bezpečnosti v najmenej troch typoch oznámení.[57] V dôsledku tohto konania mali byť identifikované nedostatočné opatrenia kybernetickej bezpečnosti, ktoré zahŕňali

1) zlyhanie spoločnosti SolarWinds pri dôslednom udržiavaní bezpečného životného cyklu vývoja softvéru (SDLC), ktorý vyvinula a poskytla (tisíckam) zákazníkov,
2) zlyhanie pri presadzovaní používania silných hesiel na všetkých systémoch a
3) zlyhanie v riešení problémov s kontrolou prístupu, ktoré pretrvávali roky.

V roku 2018 zraniteľnosť spoločnosti SolarWinds mala umožňovať prístup k virtuálnej súkromnej sieti (VPN) spoločnosti prostredníctvom nespravovaných zariadení, ako sú mobilné telefóny a notebooky, ktoré spoločnosť nevlastnila ani neprevádzkovala. V januári 2019 pristupovali aktéri hrozieb k systémom SolarWinds prostredníctvom VPN pomocou nespravovaného zariadenia. Aktéri potom mali široký, nezistený prístup k systémom SolarWinds (je možné, že aktéri hrozieb prvýkrát pristupovali k systémom SolarWinds skôr a inými prostriedkami, ale najskôr potvrdený prístup bol cez zraniteľnosť VPN). Pomocou svojho prístupu vložili aktéri hrozieb škodlivý kód do troch softvérových verzií pre produkty Orion spoločnosti SolarWinds. SolarWinds potom dodala tieto napadnuté produkty viac ako 18 000 zákazníkom po celom svete. Škodlivý kód poskytol aktérom hrozby možnosť

[55] Spoločnosť SolarWinds poskytuje softvér na správu infraštruktúry informačných technológií, napríklad sledovanie aktivity na sieťových serveroch.

[56] Žaloba SEC voči SolarWinds a pánovi Brownovi, podaná na okresný súd Južného dištriktu štátu New York zo dňa 30. 10. 2023, sp. zn. 23-cv-9518. Dostupné z: https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf [cit. 21. 4. 2024].

[57] Vyhlásenia, ktoré mali za cieľ opísať postupy a zásady kybernetickej bezpečnosti spoločnosti, vrátane „Vyhlásenia o bezpečnosti" uverejneného na webovej stránke spoločnosti. Tiež formulár S-1 a S-8 pre vyhlásenia a pravidelné správy podané na SEC a formulár 8-K podaný SEC dňa 14. decembra 2020 týkajúci sa rozsiahleho incidentu kybernetickej bezpečnosti SUNBURST, ktorý ovplyvnil softvérovú platformu Orion.

prístupu k systémom týchto napadnutých zákazníkov, za predpokladu splnenia určitých ďalších podmienok, a stal sa známym ako útok SUNBURST.

Dňa 14. decembra 2020 spoločnosť SolarWinds podala formulár 8-K SEC, v ktorom oznámila, že jej softvér na monitorovanie siete Orion obsahuje škodlivý kód, ktorý vložili aktéri hrozieb v rámci útoku na dodávateľský reťazec. Formulár 8-K bol vytvorený skupinou vedúcich pracovníkov vrátane Browna a podpísaný CEO spoločnosti SolarWinds. Tento formulár 8-K bol podstatne zavádzajúci v niekoľkých ohľadoch, vrátane toho, že nezverejnil, že predmetná zraniteľnosť bola aktívne zneužitá proti zákazníkom spoločnosti SolarWinds niekoľkokrát počas najmenej šiestich mesiacov.

Podľa SEC sa obaja žalovaní mali dopustiť porušenia viacerých ustanovení zákona o obchode s cennými papiermi *(Exchange Act)*. Porušenia zákona sa mali dopustiť najmä tým, že

1) vedome používali zariadenia, schémy alebo úskoky na podvod,
2) vedome získali peniaze alebo majetok nepravdivými vyhláseniami o podstatnej skutočnosti alebo opomenutím uviesť podstatnú skutočnosť potrebnú na to, aby mohli urobiť vyhlásenia, vzhľadom na okolnosti, za ktorých boli vyrobené, nie zavádzajúce a
3) vedome sa zapojili do transakcií, praktík, ktoré fungovali alebo by fungovali ako podvod alebo klamstvo voči kupujúcim akcií spoločnosti SolarWinds.[58]

Ďalšie porušenia mali spočívať v uvedení zavádzajúcich informácií vo formulárových podaniach pre SEC.[59] Rovnako tak porušením malo byť aj to, že spoločnosť SolarWinds nedokázala navrhnúť a udržiavať systém interných kontrol, ktorý by dával primerané záruky, že prístup k aktívam je povolený iba oprávneným osobám. Osobitne Brownovi SEC vytýka, že prostredníctvom svojich nepravdivých vyhlásení, nepravdivých osvedčení a iných prostriedkov, vedome poskytol významnú pomoc, a tým napomáhal a navádzal na porušovanie predpisov o cenných papieroch spoločnosťou SolarWinds.

Pozoruhodné je, že vo februári 2024 podala skupina CISO, odborníkov na kybernetickú bezpečnosť a organizácií zaoberajúcich sa kybernetickou bezpečnosťou podanie amicus curie na podporu návrhu žalovaných na zamietnutie žaloby. V tomto podaní tvrdia, že argumenty v žalobe o vzniku zodpovednosti sú kontraproduktívne vzhľadom na reálne požiadavky kybernetickej bezpečnosti, a hrozia škodlivé dôsledky vrátane zvýšenia frekvencie a škodlivosti kybernetických útokov, zabránenia internému úsiliu o posilnenie kybernetickej bezpečnosti, zhoršenia krízy v oblasti prijímania a udržania osôb na pozícii CISO a odradenia CISO od spolupráce so štátom.[60] Združenie BSA Softvérová aliancia, rovnako

58 V slovenskej právnej praxi by mohlo byť takéto konanie posúdené z hľadiska naplnenia znakov trestného činu podvodu podľa § 221 Trestného zákona, trestného činu kapitálového podvodu podľa § 224 Trestného zákona, či dokonca trestného činu poškodzovania spotrebiteľa podľa § 269 Trestného zákona.

59 V slovenskej právnej praxi by mohlo byť takéto konanie posúdené z hľadiska naplnenia znakov trestného činu skresľovania údajov hospodárskej a obchodnej evidencie podľa § 259 alebo § 260 Trestného zákona.

60 Podanie amicus curie *Motion of chief information security officers and cybersecurity organizations for leave to file brief as amicus curiae in support of defendants' motion to dismiss the complaint* zo dňa 2. 2. 2024. Dostupné z: https://www.cooley.com/-/media/cooley/alerts/2024-2-2-amicus-brief-of-cisos--cybersecurity-orgs.pdf [cit. 21. 4. 2024].

predložila podanie amicus curie, v ktorom uviedla podobné argumenty z pohľadu softvérových spoločností.[61]

Aj v nadväznosti na vyššie uvedené podania, doručil SEC súdu doplnenie žaloby obsahujúce podrobnejšie skutkové tvrdenia proti pánovi Brownovi. Predovšetkým SEC uvádza, že v tomto prípade nejde o jediné zlyhanie opatrenia alebo niekoľko izolovaných zlyhaní opatrení. Podstatné bolo skôr rozsiahle a pretrvávajúce nedodržiavanie každej z politík (dodržiavanie rámca kybernetickej bezpečnosti NIST, používanie SDLC, monitorovanie siete, správa hesiel a kontroly prístupu). K osobe Browna SEC doplnil, že Brown bol tvorcom vyššie uvedených vyhlásení a jeho vedomosť, ľahkomyseľnosť a/alebo nedbanlivosť sa pripisuje spoločnosti aj na základe jeho úlohy ako riadiaceho pracovníka spoločnosti SolarWinds, vedúceho jej skupiny InfoSec, hlavného hovorcu pre otázky kybernetickej bezpečnosti a doslova «tváre» kybernetickej bezpečnosti v spoločnosti.[62]

V júly 2024 súd nepripustil väčšinu zo žalobných návrhov SEC, avšak konanie stále pokračuje vo zvyšku žaloby aj voči pánovi Brownovi.[63] Doposiaľ o žalobe právoplatne rozhodnuté nebolo.

2.3 Prípad Drizly (zodpovednosť CEO v prípade absencie osoby CISO)

V roku 2022 FTC podnikla kroky proti spoločnosti Drizly, online predajcovi s alkoholom a jej CEO (pánovi Rellasovi) v súvislosti so zisteniami, že malo prísť k zlyhaniu spoločnosti v oblasti kybernetickej bezpečnosti, ktoré viedli k narušeniu bezpečnosti údajov, v dôsledku čoho unikli osobné údaje približne 2,5 milióna spotrebiteľov. Spoločnosť Drizly nemala ustanoveného CISO a jeho úlohy vykonával jej CEO. Spoločnosť Drizly v rámci svojej obchodnej činnosti zhromažďovala a ukladala osobné údaje zákazníkov v cloudovej službe Amazon Web Services (AWS), napr. e-mailové adresy, heslá, informácie o geografickej polohe a poštové adresy zákazníkov. Na uľahčenie spolupráce vývojárov spoločnosť Drizly údajne používala aj softvérovú platformu GitHub, ako nezabezpečené „úložisko", v ktorom spoločnosť Drizly ukladala nielen projekty spoločnosti, ale aj prístupové údaje k AWS, ktoré umožňujú prístup k heslám jej zákazníkov.[64]

V roku 2018 spoločnosť Drizly zaznamenala narušenie bezpečnosti po tom, čo údajne umožnila prístup k úložisku GitHub vedúcemu pracovníkovi spoločnosti Drizly a nezrušila prístup tohto vedúceho pracovníka. Útočník, ktorému sa podarilo preniknúť do úložiska GitHub spoločnosti Drizly pomocou hesiel vedúceho pracovníka, našiel v úložisku

61 Podanie amicus curie *Brief of BSA | the Software alliance as amicus curiae supporting defendants'motion to dismiss*. 2. 2. 2024. Dostupné z: https://fingfx.thomsonreuters.com/gfx/legaldocs/xmpjrngbapr/frankel-secvsolarwinds--bsaamicus.pdf [cit. 21. 4. 2024].

62 Doplnenie žaloby SEC sp. zn. 23-cv-9518-PAE zo dňa 16. februára 2024. Dostupné z: https://www.law360.com/articles/1804498/attachments/0 [cit. 21. 4. 2024].

63 STEMPHEL, J. SolarWinds beats most of US SEC lawsuit over Russia-linked cyberattack. *Reuters* [online]. 18. 7. 2024 [cit. 13. 8. 2024]. Dostupné na: https://www.reuters.com/legal/us-judge-dismisses-most-sec-lawsuit-against-solarwinds-concerning-cyberattack-2024-07-18/

64 Sťažnosť FTC proti Drizly a Rellas. *Federal Trade Commission* [online]. [cit. 21. 4. 2024]. Dostupné z: https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf

prihlasovacie údaje k AWS. V roku 2020 malo prísť k opätovnému narušeniu, keď útočník podobne získal prístup k prihlasovacím údajom AWS prostredníctvom nezabezpečeného úložiska GitHub, nabúral sa do databázy spoločnosti a potom odcudzil informácie o zákazníkoch.

FTC uvádza, že incident bol zhoršený nasledujúcimi bezpečnostnými chybami spoločnosti Drizly a jej CEO, ktoré mali spočívať v tom, že:[65]

1) napriek vyhláseniam spoločnosti Drizly, v ktorých sa uvádza, že spoločnosť používa vhodné bezpečnostné postupy na ochranu údajov spotrebiteľov, spoločnosť a ani jej CEO nezaviedli primerané bezpečnostné opatrenia na zabezpečenie zhromaždených a uložených osobných údajov. Nevyžadovali od zamestnancov, aby používali dvojfaktorovú autentifikáciu pre GitHub, neobmedzila prístup zamestnancov k osobným údajom, nevypracovala primerané písomné bezpečnostné zásady ani neškolila zamestnancov o týchto postupoch.
2) ukladali kritické informácie z databázy na nezabezpečenej platforme: spoločnosť Drizly uchovávala prihlasovacie údaje na platforme GitHub v rozpore s vlastnými usmerneniami platformy a dobre medializovanými bezpečnostnými incidentmi týkajúcimi sa GitHubu.
3) zanedbali monitorovanie siete z hľadiska bezpečnostných hrozieb: spoločnosť Drizly nemala stanoveného CISO, ani nemonitorovala svoju sieť z hľadiska neoprávnených pokusov o prístup k osobným údajom alebo ich odstránenie.[66]

Nápravné opatrenia FTC sa týkali predovšetkým CEO[67] (Rellasa), ktoré sa budú vo vzťahu k nemu uplatňovať aj v prípade, že opustí spoločnosť Drizly. Konkrétne sa od CEO bude vyžadovať, aby počas 10 rokov v budúcich spoločnostiach zaviedol program informačnej bezpečnosti, ak prejde do spoločnosti, ktorá zhromažďuje informácie o viac ako 25 000 osobách a v ktorej je väčšinovým vlastníkom, generálnym riaditeľom alebo vedúcim pracovníkom zodpovedným za informačnú bezpečnosť.

Domnievame sa, že takéto opatrenie sa v budúcnosti môžu aplikovať nielen na štatutárneho zástupcu príp. CEO, ktorí prevezmú povinnosti v oblasti kybernetickej bezpečnosti. Osoba bez ohľadu na jej pozíciu, ktorá je zodpovedná za porušenie ochrany údajov, bude s veľkou pravdepodobnosťou čeliť podobnému opatreniu. A keď sa presunie do inej spoločnosti, bude to znamenať, že FTC sa môže obrátiť aj na túto spoločnosť.

65 Tlačová správa FTC: FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumer. *Federal Trade Commission* [online]. 24. 10. 2022 [online]. [cit. 21. 4. 2024]. Dostupné z: https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million

66 V slovenskej právnej praxi by mohlo byť takéto konanie posúdené z hľadiska naplnenia znakov trestného činu porušovania povinností pri správe cudzieho majetku podľa § 237 a 238 Trestného zákona, či trestného činu poškodzovanie spotrebiteľa podľa § 269 Trestného zákona.

67 Rozhodnutie a opatrenie FTC. *Federal Trade Commission* [online]. [cit. 21. 4. 2024]. Dostupné z: https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf

3 Trestnoprávna zodpovednosť MKB v českom a slovenskom práve

Rešpektovanie povinností právnickou osobou v oblasti kybernetickej bezpečnosti je výzvou pre každú právnickú osobu, jej štatutárny orgán a MKB. Pri incidente prichádza tiež k zhromažďovaniu faktov spravidla pod časovým tlakom, k úsiliu o limitovanie vzniku škôd na majetku právnickej osoby, a to pri snahe dodržať povinnosti ustanovené právnymi predpismi. V tomto kontexte môže otázka vyvodenia trestnoprávnej zodpovednosti nadobudnúť väčší význam.

Prípady SolarWinds a Uber sú síce odlišné, ale oba zahŕňajú možné trestnoprávne aspekty porušenia povinností MKB, v súvislosti s reakciou na incidenty a komunikovaním stavu kybernetickej bezpečnosti digitálnych produktov a služieb. Prípad Drizly ukazuje, že ak zodpovednosť za kybernetickú bezpečnosť nie je v spoločnosti delegovaná na CISO, môže niesť zodpovednosť aj priamo CEO, resp. štatutárny orgán spoločnosti.

Nie je našou ambíciou hodnotiť konanie zodpovedných subjektov v uvedených prípadoch podľa právnych predpisov USA, ale skôr skúmať konanie týchto subjektov všeobecne (a nielen pri incidentoch), toto konanie vymedziť a posúdiť v podmienkach českej a slovenskej právnej úpravy, so zameraním sa na to aké implikácie by mohli vzniknúť v oblasti trestnoprávnej zodpovednosti. Naše skúmanie sa nezužuje len na konanie CISO v regulovaných subjektoch, ale aj vzhľadom na to čo sme už uviedli vyššie aj na neregulované subjekty, na ktoré nedopadajú špecifické povinnosti podľa právnych predpisov v oblasti kybernetickej bezpečnosti. Na druhej strane je zrejmé, že práve regulované subjekty budú pod väčším drobnohľadom a postup voči nim a ich vedeniu aj vzhľadom na závažnosť možného dopadu bude prísnejší.

V súvislosti s konaním zodpovedných subjektov považujeme za primárne rešpektovanie povinností uložených zákonmi alebo na ich základe. Uplatnenie trestnoprávnej zodpovednosti by malo predstavovať prostriedok poslednej inštancie (ultima ratio), keď predchádzajúce (mimo-trestné) prostriedky zlyhali. Nami preferovaný postup v takýchto prípadoch uprednostňuje prevenciu pred represiou. Dôležitým predpokladom k naplneniu tohto zámeru nesporne predstavujú dostatočné vedomosti MKB o tom, ako má postupovať pri plnení svojich povinností, interné predpisy právnickej osoby upravujúce postup zodpovedných subjektov a ich vzdelávanie v oblasti kybernetickej bezpečnosti.

Vzhľadom na zameranie tohto článku venujeme pozornosť v ďalšej časti tohto článku podmienkam vyvodenia trestnoprávnej zodpovednosti voči MKB a ďalším zodpovedným subjektom.

3.1 Nepravdivo vyplnené samohodnotenie

V podmienkach Slovenskej republiky bude podstatnou povinnosťou MKB vypracovanie samohodnotenia, v ktorom sa overuje miera implementácie bezpečnostných opatrení na ochranu majetku právnickej osoby. Tento majetok zahŕňa okrem hmotných statkov aj nehmotné statky a práva, v digitálnej sfére súhrnne nazývané *informačne aktíva*, ktorými rozumieme tiež každú informáciu, systém, aplikáciu alebo hardvér v majetku právnickej osoby, ktorý sa používa pri prevádzkových činnostiach.

Vyvodenie trestnoprávnej zodpovednosti voči MKB (v prípade regulovaného subjektu) prichádza do úvahy, keď vyhotoví výkaz či evidenciu o stave a hodnote jej informačných aktív (v rámci samohodnotenia právnickej osoby), ktoré obsahujú predovšetkým vedome nepravdivé alebo chybné údaje, prípadne keď zatají relevantné údaje.

Trestný zákon chráni záujem na riadnom vedení hospodárskej a obchodnej evidencie pred jej skresľovaním, prostredníctvom trestného činu (prečinu) skresľovania údajov hospodárskej a obchodnej evidencie podľa § 259 ods. 1 písm. g) Trestného zákona (zahŕňa úmyselné konanie) alebo podľa § 260 Trestného zákona (zahŕňa nedbanlivostné konanie).

Podstata tohto trestného činu spočíva v uvedení nepravdivých alebo hrubo skresľujúcich údajov alebo zatajení povinných údajov o závažných skutočnostiach vo výkaze, v hlásení, vo vstupných údajoch vkladaných do počítača alebo v iných podkladoch slúžiacich na zápis do registra podľa osobitného predpisu. Registrom podľa osobitného predpisu v tomto prípade rozumieme tiež príslušný register regulovaných subjektov (najmä prevádzkovateľov základných služieb) vedený NBÚ.

V zmysle odbornej literatúry *nepravdivé údaje* predstavujú údaje celkom odporujúce skutočnosti. *Hrubo skresľujúcimi údajmi* sa rozumejú informácie sčasti chybné, neúplné, a preto nepravdivé. Rozdiel oproti skutočnosti musí byť podstatný a takáto čiastočne nepravdivá informácia musí mať i podstatný význam pre objektívne zistenie z hľadiska účelu, na ktorý má slúžiť. *Zatajenie údajov* môže spočívať tak v predstieraní ich neexistencie, ako aj v nepravdivom predstieraní nepravých údajov ako pravých.[68]

Vo vzťahu k trestnému činu (prečinu) skresľovania údajov hospodárskej a obchodnej evidencie podľa § 259 ods. 1 písm. g) Trestného zákona je potrebné pri posudzovaní závažnosti činu hodnotiť rozsah porušenia právnych predpisov právnickou osobou (regulovaným subjektom) z hľadiska § 10 ods. 2 Trestného zákona[69]; v prípade tohto trestného činu (prečinu) podľa § 260 Trestného zákona navyše to, že ide o nedbanlivostné konanie.

Z hľadiska trestního zákoníka je možné takéto konanie právne kvalifikovať ako trestný čin zkreslování údajů o stavu hospodaření a jmění (§ 254 ods. 1 trestního zákoníku), ktorého sa dopustí ten, kto *nevede účetní knihy, zápisy nebo jiné doklady sloužící k přehledu o stavu hospodaření a majetku nebo k jejich kontrole, ač je k tomu podle zákona povinen, kdo v takových účetních knihách, zápisech nebo jiných dokladech uvede nepravdivé nebo hrubě zkreslené údaje, nebo kdo takové účetní knihy, zápisy nebo jiné doklady změní, zničí, poškodí, učiní neupotřebitelnými nebo zatají, a ohrozí tak majetková práva jiného nebo včasné a řádné vyměření daně.*

Trestnoprávna zodpovednosť je v prípade tohto trestného činu založená na niektorých z alternatívnych foriem konania páchateľa, ktorý uvedené doklady:

1) nevedie, hoci jej táto povinnosť vyplýva podľa zákona,
2) uvedie v nich nepravdivé alebo hrubo skresľujúce údaje, alebo
3) zničí, poškodí, urobí nepoužiteľnými alebo zatají,

a tým ohrozí vlastnícke práva iného.

[68] ČENTÉŠ, J. In: ČENTÉŠ, J. a kol. *Trestný zákon – Veľký komentár.* Eurokódex. Žilina, 2013, s. 486.

[69] Podľa § 10 ods. 2 Trestného zákona nejde o prečin, ak vzhľadom na spôsob vykonania činu a jeho následky, okolnosti, za ktorých bol čin spáchaný, mieru zavinenia a pohnútku páchateľa je jeho závažnosť nepatrná.

Pri porovnaní slovenskej a českej právnej úpravy konštatujeme rozdiely v tom, že slovenská právna úprava vyžaduje, aby nepravdivé alebo hrubo skresľujúce údaje sa týkali závažných skutočnostiach, pričom česká právna úprava takúto podmienku vyvodenia trestnoprávnej zodpovednosti nevyžaduje. Pre úplnosť uvádzame, že tieto podmienky vyvodzuje česká odborná literatúra, čo odôvodňuje tým, že musí prísť k ohrozeniu majetkových práv (…) s prihliadnutím aj na judikatúru.[70]

Páchateľom tohto trestného činu môže tak byť štatutárny orgán[71], ako aj iné osoby napr. CEO alebo MKB. Z hľadiska naplnenia zákonných znakov tohto trestného činu podľa českej judikatúry nestačí len formálne označenie funkcie a postavenia, ale je potrebné skúmať konkrétny obsah povinností[72] ustanovených v interných predpisoch právnickej osoby (obchodnej spoločnosti), prípadne delegovaných štatutárnym orgánom na iné osoby (napr. MKB) činné v právnickej osobe, prípadne na externé fyzické alebo právnické osoby a pod. V prípade, ak štatutárny orgán delegoval splnenie povinnosti na iné osoby k tomu určené a spôsobilé, v prípade ktorých sa dôvodne spoliehal, že tieto povinnosti splnia, avšak tieto osoby ich nesplnili, nemožno u štatutárneho orgánu vyvodiť úmyselné zavinenie, a to ani v prípade, keď jeho spoliehanie bolo neprimerané.[73]

K naplneniu skutkovej podstaty tohto trestného činu postačuje ohrozenie majetkových práv iného, nemusí teda prísť k ich narušeniu (porušeniu). Pojem *„majetkové práva"* zahŕňa všetky práva týkajúce sa majetku, t. j. nielen práva vyplývajúce z vlastníctva majetku, ale aj majetkové práva vyplývajúce zo zmluvných vzťahov. V prípade, ak by prišlo k narušeniu majetkových práv v dôsledku napr. neoprávneného nakladania s majetkom mohlo by sa jednať o naplnenie skutkovej podstaty trestného činu sprenevery podľa § 206 trestního zákoníka alebo o niektorý z tzv. úpadkových deliktov podľa § 222 až 224 trestního zákoníka.[74] Podľa judikatúry ustanovenie § 254 ods. 1 trestního zákoníka je vo vzťahu k § 222 ods. 1 trestního zákoníka v pomere subsidiarity, pretože poruchový delikt má prednosť pred ohrozovacím deliktom[75]. Pojem *„jiného"* označuje subjekt odlišný od páchateľa (fyzická alebo právnická osoba) tohto trestného činu, môže ním byť aj právnická osoba (obchodná spoločnosť), v rámci ktorej došlo k porušeniu povinnosti konaním páchateľa. Právnická osoba môže byť dotknutá konaním páchateľa, ak boli takýmto konaním ohrozené jej majetkové práva.[76]

V závislosti na uvedenom scenári je možné, že aj MKB v spoločnosti mohol ohroziť majetkové práva iného subjektu. Ak MKB nedostatočne zabezpečil ochranu citlivých údajov a spôsobil tým zraniteľnosť systému, mohlo to viesť k poškodeniu majetkových práv iných

[70] ŠÁMAL, P., ŘÍHA, J. § 254 [Zkreslování údajů o stavu hospodaření a jmění]. In: ŠÁMAL, P. a kol. *Trestní zákoník*. 3. vyd. Praha: C. H. Beck, 2023, s. 3323 a nasl. a primerane R 16/2017-II.

[71] Primerane pozri Rč 37/2009, Rč 2/2019 a Rč 25/2020.

[72] Primerane pozri Rč 11/2020, Rč 47/2019.

[73] Primerane pozri Rč 4/2022.

[74] Podrobnejšie pozri ŠÁMAL, P., ŘÍHA, J. § 254 [Zkreslování údajů o stavu hospodaření a jmění]. In: ŠÁMAL a kol., 2023, op. cit., s. 3323 a nasl. V podmienkach Slovenskej republiky pozri § 213, § 239 a § 240 Trestného zákona.

[75] Primerane pozri Rč 50/2018-II.

[76] Primerane pozri Rč 37/2009 a Rč 2/2019. Určitú výnimku predstavuje prípad, keď samotná právnická osoba, ktorej sú uložené povinnosti, spáchala trestný čin a možno voči nej uplatniť trestnoprávnu zodpovednosť.

subjektov, ako sú zákazníci alebo obchodní partneri spoločnosti. Príkladom takého konania môže byť situácia, keď nedostatočné zabezpečenie systému umožnilo útočníkom preniknúť do citlivých databáz, čím došlo k úniku alebo poškodeniu údajov zákazníkov. Tento únik údajov môže ohroziť majetkové práva týchto zákazníkov, napríklad ich finančné údaje, ktoré môžu byť zneužité alebo inak kompromitované.

Takýmto konaním MKB môžu byť ohrozené aj majetkové práva samotnej spoločnosti. Príkladom môže byť situácia, keď zraniteľnosti systému umožnia útočníkom získať prístup k obchodnému tajomstvu alebo dôverným informáciám, čo môže mať za následok úbytok majetkových práv právnickej osoby a to následkom finančných strát, poškodenia reputácie spoločnosti, ale aj uloženia sankcií regulátorom. Uvedené tiež priamo ovplyvňuje aj práva spoločníkov právnickej osoby ak v dôsledku tohto konania dôjde k následku v podobe poklesu cien ich akcií, resp. hodnoty ich podielov.

3.2 Nepravdivé alebo značne skresľujúce verejné vyhlásenia a zmluvné záväzky týkajúce sa úrovne kybernetickej bezpečnosti

Zodpovednosť MKB, prípadne iných osôb (ak nemá právnická osoba MKB, takouto osobou môže byť napr. CEO alebo iná osoba, na základe poverenia štatutárnym orgánom, prípadne aj samotný štatutárny orgán) prichádza do úvahy aj pri nepravdivých vyhláseniach alebo značne skresľujúcich informáciách právnickej osoby (obchodnej spoločnosti) o úrovni jej kybernetickej bezpečnosti a/alebo jej digitálnych produktov.

Zvýrazňujeme, že úroveň kybernetickej bezpečnosti v právnickej osobe a predovšetkým jej produktov, priamo súvisí s jej príjmami a ziskom. Podobne ako v prípade SolarWinds, právnická osoba (obchodná spoločnosť) máva svoje top produkty, tzv. vlajkové lode a v prípade ak by sa preukázalo, že tieto trpia vážnymi nedostatkami v oblasti bezpečnosti, znamenalo by to stratu dôvery zákazníkov a obchodných partnerov a tým vážne dopady na jej podnikanie a finančný stav. Tieto prípady môžu zahŕňať situácie, keď právnická osoba vo verejných vyhláseniach, reklame, obchodných podmienkach alebo aj na webovom sídle uvádza nepravdivé informácie o vysokej úrovni kybernetickej bezpečnosti produktov a splnení najvyšších nárokov v tejto oblasti, avšak v skutočnosti je úroveň kybernetickej bezpečnosti v spoločnosti a jej produktov nedostatočná (nízka) a nepravdivé informácie ovplyvňujú rozhodnutia investorov, obchodných partnerov a spotrebiteľov. V takomto prípade sa môže jednať o podvodné konanie. O takéto konanie však nepôjde spravidla v prípade nadsázky v reklame (za predpokladu, že nejde o klamlivú reklamu alebo klamlivé označenie tovaru, ktoré by mohlo byť kriminalizované ako trestný čin porušení předpisů o pravidlech hospodářské soutěže podľa § 248 ods. 1 písm. a) alebo b) trestního zákoníku, a to prípadne v súbehu s trestným činom poškozování spotřebitele podľa § 253 trestního zákoníka).[77] Rovnako tak, treba zobrať do úvahy, že v praxi môže nastať množstvo rôznych situácií, kde MKB nebude konať úmyselne, ale len z nedbanlivosti, čím nenaplní všetky znaky trestného činu podvodu, predovšetkým z dôvodu absencie naplnenia subjektívnej stránky trestného

[77] Podrobnejšie pozri ŠÁMAL, P. § 209 [Podvod]. In: ŠÁMAL a kol., 2023, op. cit., s. 2648 a nasl.

činu. V dôsledku tejto okolnosti nebude možné jej konanie právne kvalifikovať ako trestný čin.

Skutková podstata trestného činu podvodu podľa § 209 ods. 1 trestního zákoníka spočíva v konaní páchateľa, ktorý *sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo* ***zamlčí podstatné skutečnosti***, a spôsobí tak na cizím majetku škodu nikoli nepatrnou. Na rozdiel od českej úpravy, slovenský Trestný zákon v § 221 ods. 1 kriminalizuje konanie páchateľa, ktorý *seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu*. Z porovnania týchto dvoch trestných činov vyplýva, že slovenská právna úprava neobsahuje alternatívny znak skutkovej podstaty spočívajúci v *„zamlčaní podstatné skutečností"*, čo vnímame ako nedostatok a odporúčame tento znak doplniť.

Z hľadiska naplnenia zákonných znakov skutkovej podstaty trestného činu podvodu konštatujeme, že podvodné konanie spočívajúce v uvedení do omylu alebo využití omylu, prípadne zamlčaní podstatných skutočností, môže smerovať nielen voči poškodenému, ale aj inej osobe. Omyl sa môže týkať aj skutočností, ktoré majú nastať, páchateľ však o omyle musí vedieť už v dobe, keď prichádza k jeho obohateniu.[78] V nami uvedenom prípade môže k takejto situácii dôjsť vtedy, keď právnická osoba (obchodná spoločnosť) uviedla napr. zákazníkov, investorov do omylu ohľadom tvrdenia o vysokej úrovni kybernetickej bezpečnosti produktov, pričom títo investovali do produktov s nízkou úrovňou kybernetickej bezpečnosti. V dôsledku kybernetického útoku môže dôjsť k strate finančných prostriedkov a škode na strane zákazníkov, resp. investorov. Poznamenáme, že zamlčanie takýchto (podstatných) skutočností (pri súčasnom splnení aj ďalších zákonných znakov skutkovej podstaty trestného činu podvodu podľa § 209 trestního zákoníka) spočíva v takom konaní páchateľa, ktorý zamlčí zásadné skutočnosti pre rozhodnutie poškodeného, prípadne inej podvádzanej osoby, ktoré keby jej boli známe a ktoré by neviedli k jej následnému konaniu.[79]

Dôležitými faktormi pri vyvodení trestnoprávnej zodpovednosti sú v takomto prípade výška spôsobenej škody (v trestním zákoníku nie nepatrnej škody; v Trestnom zákone malej škody), preukázanie príčinnej súvislosti a úmyselného konania páchateľa (právnická osoba, resp. jej MKB a/alebo CEO). Skutková podstata trestného činu podvodu vyžaduje, aby bolo úmyselným zavinením páchateľa pokryté nielen to, že „iného uvádza do omylu alebo využíva iného omyl", ale úmyselným zavinením páchateľa musí byť pokryté aj to, že takýmto konaním chce „spôsobiť na cudzom majetku škodu" a zároveň chce „seba alebo iného obohatiť".

Uvedenie do omylu môže byť ľsťou, ale môže ísť aj o nepravdivú informáciu. Uvedením do omylu je konanie, ktorým páchateľ predstiera okolnosti, ktoré nie sú v súlade so skutočným stavom veci, napríklad pokiaľ ide o plánovanú obchodnú transakciu s predpokladaným ziskom.[80] Spúšťacím mechanizmom pri trestnom čine podvodu je uvádzanie iného do omylu alebo využívanie omylu iného, pretože len v prípadoch, keď je škoda na cudzom

78 ŠÁMAL a kol., 2023, s. 2653 a nasl.

79 Primerane pozri Rč 47/2002.

80 Uznesenie Najvyššieho súdu SR zo dňa 24. 8. 2022, sp. zn. 4Tdo/51/2021.

majetku spôsobená v príčinnej súvislosti s omylom inej osoby, môže ísť o spáchanie trestného činu podvodu. K naplneniu trestnoprávnej zodpovednosti za následok nie je dostatočné následok len spôsobiť, ale je nevyhnutné ho aj zaviniť. Práve táto podmienka pre naplnenie subjektívnej stránky trestného činu podvodu môže byť zložitá pri preukazovaní, resp. môže absentovať pri dokazovaní konania spočívajúce vo verejných vyhláseniach a / alebo zmluvných záväzkoch.[81] Táto náročnosť spočíva v potrebe preukázať, že páchateľ mal úmyselne klamlivé a vedome uviedol inú osobu do omylu. Pri verejných vyhláseniach, ako sú marketingové kampane alebo tlačové správy, môže byť ťažké preukázať konkrétny úmysel podvodného konania, pretože vyhlásenia často obsahujú všeobecné alebo nepresné informácie, ktoré sa nedajú ľahko interpretovať ako úmyselné uvádzanie do omylu. Okrem toho, v prípade zmluvných záväzkov môžu byť sporné body týkajúce sa zmluvných podmienok alebo obchodných podmienok interpretované rôznymi spôsobmi, čo sťažuje preukázanie zavinenia aj čo do následku.

V prípade subjektov, ktoré sú účastníkmi kapitálového trhu prichádza do úvahy aj naplnenie skutkovej podstaty trestného činu kapitálového podvodu podľa § 224 ods. 1 Trestného zákona, ktorá umožňuje vyvodenie trestnoprávnej zodpovednosti páchateľa, ktorý *v súvislosti s ponukou, predajom alebo rozširovaním cenných papierov alebo iných listín, ktoré sľubujú účasť na majetkových výnosoch podniku, alebo kto v súvislosti s ponukou zvýšiť výnosy takého investovania v prospektoch alebo v iných propagačných materiáloch alebo prehľadoch týkajúcich sa majetkových pomerov alebo výnosov podniku vo vzťahu k väčšiemu počtu osôb uvádza nepravdivé údaje alebo nereálne údaje o výnosoch investovania alebo o majetkových pomeroch podniku, do ktorého sa má investovať, alebo kto nevýhody takého investovania zamlčí.*

Podľa nášho názoru k naplneniu zákonných znakov tohto trestného činu môže dôjsť v súvislosti s ponukou, predajom alebo rozširovaním cenných papierov alebo iných listín, v iných propagačných materiáloch alebo prehľadoch týkajúcich sa majetkových pomerov alebo výnosov podniku (právnickej osoby) vo vzťahu k väčšiemu počtu osôb, ktoré uvádzajú nepravdivé údaje alebo nereálne údaje o majetkových pomeroch právnickej osoby, do ktorej sa má investovať. Majetkovými pomermi podniku (právnickej osoby) v tomto prípade rozumieme aj informačné aktíva a v konečnom zmysle digitálne produkty, ktoré predáva spoločnosť. Na rozdiel od trestného činu podvodu, ktorý ako zákonnú podmienku trestnosti skutku ustanovuje aj spôsobenie škody na cudzom majetku, trestný čin kapitálového podvodu podmienku spôsobenia škody nevyžaduje.

Trestní zákoník poskytuje ochranu kapitálového trhu tiež v prípade trestného činu manipulace s kurzem investičních nástrojů podľa § 250 ods. 1 písm. a) a písm. b), ktorý ustanovuje trestnosť konania páchateľa, ktorý *v úmyslu ovlivnit cenu nebo kurz investičních nástrojů, které jsou přijaty k obchodování v obchodním systému nebo o jejichž přijetí k obchodování v obchodním systému bylo požádáno, rozšíří nebo jinému poskytne nepravdivou nebo hrubě zkreslenou informaci významně ovlivňující cenu nebo kurz takových investičních nástrojů nebo s nimi souvisejících komodit obchodovaných na organizovaném trhu se zbožím anebo výpočet sazeb, indexů nebo kvantitativně vyjádřených ukazatelů určujících pro cenu nebo kurz takových investičních nástrojů, nebo uskuteční obchod, zadá pokyn nebo se dopustí*

[81] Primerane napríklad Uznesenie Krajského súdu v Bratislave zo dňa 4. 6. 2019, sp. zn. 3To/16/2019.

jiného jednání, které je způsobilé vyvolat nesprávnou představu o nabídce, poptávce, ceně nebo kurzu takového investičního nástroje nebo s ním souvisejících komodit obchodovaných na organizovaném trhu se zbožím anebo o hodnotě sazby, indexu nebo kvantitativně vyjádřeného ukazatele určujícího pro cenu nebo kurz takových investičních nástrojů.

Zo skutkovej podstaty tohto trestného činu vyplýva, že predpokladom vyvodenia trestnoprávnej zodpovednosti je rozšírenie alebo poskytnutie nepravdivej alebo hrubo skreslenej informácie, ktorá výrazne ovplyvňuje cenu alebo kurz takýchto investičných nástrojov a pod.

V súvislosti s finančným trhom poukazujeme tiež na osobitnú povinnosť emitentov s finančnými nástrojmi prijatými na obchodovanie na regulovanom trhu, čo najskôr informovať verejnosť o dôverných informáciách, ktoré sa ho priamo týkajú.[82] Emitent je povinný zabezpečiť také sprístupnenie dôverných informácií verejnosti, ktoré umožní rýchly prístup a úplné, správne a včasné posúdenie informácií zo strany verejnosti tak, aby mohla investovať svoje prostriedky do investičných inštrumentov s cieľom dosiahnuť primeraný výnos s ohľadom na ekonomickú situáciu emitenta, segmentu trhu či celej ekonomiky, pričom kontinuálne revidujú už uskutočnené investičné rozhodnutia a analyzujú budúce investičné rozhodnutia.[83] Ako ukazuje aj prípad obchodnej spoločnosti VARTA AG, z februára 2024, emitenti sú povinní na základe tejto povinnosti, informovať verejnosť aj o incidente, odstávke výroby a iných citlivých podnikateľských informáciách.[84]

Osobitne, pri klamlivom resp. podvodnom konaní smerujúcom voči spotrebiteľovi, poukazujme na možnosť naplnenia skutkovej podstaty trestného činu (prečinu) poškodzovania spotrebiteľa podľa § 269 ods. 1 písm. a), písm. b) Trestného zákona. Tento trestný čin kriminalizuje konanie páchateľa, *ktorý klame spotrebiteľa na kvalite, množstve alebo hmotnosti tovaru alebo na druhu, akosti a množstve poskytovaných výkonov, alebo uvedie na trh výrobky, práce alebo služby a zatají pritom ich podstatné vady*. V tomto prípade by takéto konania bolo naplnené, ak spoločnosť klame o kvalite svojho digitálneho produktu (údajná vysoká úroveň kybernetickej bezpečnosti) a zatajuje jeho podstatnú vadu (skutočná, nízka úroveň kybernetickej bezpečnosti). Konaním musí byť spôsobená aspoň malá škoda.

Trestní zákoník zabezpečuje ochranu spotrebiteľa v ustanovení § 253 ods. 1, ktoré umožňuje kriminalizovanie konania páchateľa, ktorý na *cizím majetku poškozuje spotřebitele zejména tím, že je šidí na jakosti, množství nebo hmotnosti zboží, nebo kdo uvede ve větším rozsahu na trh výrobky, práce nebo služby a zatají přitom jejich podstatné vady*. Konaním musí byť spôsobená aspoň nie nepatrná škoda. Vo vzťahu k nami skúmanej problematike primerane odkazujeme na text predchádzajúceho odseku.

82 Porovnaj článok 17 ods. 1 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (nariadenie o zneužívaní trhu). Pozri tiež smernicu Európskeho parlamentu a Rady (EÚ) č. 2014/57/EU o trestných sankciách za zneužívanie trhu (smernica o zneužívaní trhu).

83 Podrobnejšie pozri PÚRY, F., HERCZEG, J. § 250 [Manipulace s kurzem investičních nástrojů]. In: ŠÁMAL a kol., 2023, op. cit., s. 3271 a nasl.

84 Publication of inside information pursuant to Article 17 of Regulation (EU) No 596/2014, VARTA affected by cyberattack, 13. február 2024. Dostupné na: https://www.marketscreener.com/quote/stock/VARTA-AG-646256/news/VARTA-AG-VARTA-affected-by-cyber-attack-45941947/ [cit. 21. 4. 2024].

3.3 Neoznámenie incidentu, podávanie nepravdivých alebo skresľujúcich informácií a nezabezpečenie digitálnych stôp

Z hľadiska vyvodenia zodpovednosti sa ďalej zaoberáme následkami rozhodnutia právnickej osoby (prevádzkovateľa základnej služby) a jej MKB, ktorí nenahlásia incident a nevykonajú aktívne kroky smerujúce k zatajeniu alebo skresľovaniu informácií o incidente. Na účely tohto článku, teda vychádzame z modelového prípadu, že útočníkovi sa podarilo preniknúť do sieťovej infraštruktúry právnickej osoby, exfiltrovať citlivé údaje o zákazníkoch a o jej produktoch, narušiť výrobnú činnosť, v dôsledku ktorej bola právnická osoba donútená úplne odstaviť výrobnú technológie na niekoľko týždňov. Škody odhadom presahujú milión eur. Útočníci požadujú zaplatenie výkupného. Incident vznikol v dôsledku dlhodobo ignorovaných zraniteľností počítačového systému právnickej osoby, čo v prípade ak by bolo zverejnené, by mohlo viesť k jej nenávratným finančným stratám. MKB preto uvedie jednotke CSIRT nepravdivé informácie o skutočnostiach súvisiacich s incidentom ako aj o bezpečnostných opatreniach a postupoch v právnickej osobe. Súčinnosť poskytne len v takej miere, aby mu nemohlo byť vyčítané, že nereagoval na dopyty. MKB presvedčí vedenie právnickej osoby, že zistené skutočnosti nenasvedčujú tomu, že ide o kybernetický útok, ale skôr ide o zlyhanie technológie, a preto nedôjde ani k podaniu trestného oznámenia. MKB zabezpečí, aby neboli uchované logové súbory, ani iné digitálne stopy o priebehu incidentu.

Medzi základné povinnosti prevádzkovateľa základnej služby okrem samotného riešenia incidentu zaraďujeme:

- vo vzťahu k CSIRT:
  - bezodkladne hlásiť závažný incident,
  - spolupracovať pri riešení incidentu,
  - poskytnúť potrebnú súčinnosť, ako aj
  - poskytnúť informácie získané z vlastnej činnosti dôležité pre riešenie incidentu.
- vo vzťahu k orgánu činnému v trestnom konaní:
  - oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa incident týka, ak sa o ňom hodnoverným spôsobom dozvie,
  - v čase incidentu zabezpečiť digitálne stopy (teda potenciálne dôkazy alebo dôkazné prostriedky) tak, aby mohli byť použité v trestnom konaní.[85]

Porušením zákonom ustanovených povinností[86], môže v rovine administratívnoprávnej zodpovednosti dôjsť k spáchaniu priestupku zo strany fyzickej osoby a správneho deliktu[87] zo strany organizácie (prevádzkovateľa základnej služby), pričom v oboch prípadoch hrozí

[85] Porovnaj § 19 ods. 6 SZoKB. V CZoKB tieto povinnosti nie sú formulované v takom rozsahu ako v slovenskej právnej úprave, predovšetkým absentuje explicitne úprava povinnosti oznámiť trestný čin a zabezpečiť digitálne stopy.

[86] Porovnaj § 30 ods. 1 písm. c) SZoKB.

[87] Porovnaj § 31 ods. 2 písm. b), d), e) SZoKB.

uloženie pokuty, eventuálne voči organizácii aj uloženie opatrení na nápravu po vykonaní auditu, avšak NBÚ nemôže fyzickej osobe (MKB) uložiť opatrenia a plnenie povinností, obdobné tým, ktoré uložil FTC v prípade Drizly.

Obdobne v Českej republike, porušením zákonom ustanovených povinností[88] môže dôjsť k spáchaniu priestupku zo strany fyzickej osoby[89] ako aj jednotlivých regulovaných subjektov, pričom v oboch prípadoch hrozí uloženie pokuty, prípadne uloženie nápravné opatrenia po vykonanej kontrole NÚKIB.

Poznamenávame, že v prípade vzniku škody spôsobenej porušením povinností pri správe cudzieho majetku môže prísť k vyvodeniu trestnoprávnej zodpovednosti podľa § 237 a § 238 slovenského Trestného zákona[90], resp. § 220 a 221 trestního zákoníka.

V rámci ďalšieho vývoja tejto oblasti upriamujeme pozornosť na návrh rozšírenia právomoci slovenského NBÚ a českého NÚKIB v rámci dohľadu a kontroly.

Okrem rozšírenia oprávnení prijímať záväzné pokyny, nariadiť dotknutým subjektom, aby upustili od protiprávneho konania, a takéto konanie neopakovali, je podstatná možnosť slovenského NBÚ postihnúť priamo štatutárny orgán alebo člena štatutárneho orgánu prevádzkovateľa základnej služby, ale aj jeho vedúceho zamestnanca zodpovedného za príslušnú činnosť alebo povereného splnomocnenca, tým že bude možné požadovať uloženie dočasného zákazu vykonávať funkciu, zamestnanie alebo činnosť u prevádzkovateľa základnej služby.[91]

V Novom CZoKB sa podstatne rozšíria možnosti spáchania priestupku ako pre regulované subjekty, ale najmä pre fyzické osoby, napríklad neposkytnutím súčinnosti NÚKIB, neposkytnutím informácií alebo súčinnosti pri zvládaní incidentu.[92] Na rozdiel od navrhovanej slovenskej právnej úpravy, NÚKIB by mal možnosť dočasne zakázať výkon funkcie len u člena štatutárneho orgánu, nie aj iných osôb (napr. vedúcich zamestnancov).[93]

S prihliadnutím na vyššie uvedené dôvodov je potrebné posúdiť trestnoprávne aspekty popísaného konania.

3.3.1 Neoznámenie incidentu a nepodanie trestného oznámenia

Z nami popísanej modelovej situácie, vyplývajú predovšetkým podozrenia z naplnenia skutkovej podstaty trestného činu neoznámenie trestného činu podľa § 340 Trestného zákona. K naplneniu objektívnej stránky tohto trestného činu sa vyžaduje, aby sa páchateľ hodnoverne dozvedel, že iná osoba spáchala zločin, za ktorý zákon ustanovuje trest odňatia

88 Porovnaj § 25 a 26 CZoKB.

89 V tomto prípade však vyvodenie zodpovednosti voči fyzickej osoby je limitované len na porušenie § 10 ods. 1 CZoKB, ktorý upravuje povinnosť mlčanlivosti zamestnancov NÚKIB.

90 ČENTÉŠ J., BELEŠ, A., ŠANTA, J. Porušovanie povinnosti pri správe cudzieho majetku – rozhodovacia činnosť súdov. In: FRYŠTÁK, M., BRUCKNEROVÁ, E. *Nové jevy v ekonomické kriminalitě: sborník příspěvků z mezinárodní konference*. 1. vyd. Brno: Masarykova univerzita, 2020, 240 s., s. 30 a nasl.

91 Článok 32 ods. 4, ods. 5 písm. b) smernice NIS 2 a § 29j ods. 4 Novely SZoKB.

92 Porov. návrh § 60 Nového CZoKB.

93 Porov. § 58 Nového CZoKB.

slobody s hornou hranicou trestnej sadzby najmenej desať rokov alebo niektorý z trestných činov korupcie a túto skutočnosť neoznámil bez odkladu príslušným v zákone uvedeným orgánom. Zločinom, za ktorý zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby najmenej desať rokov, v tomto prípade už len vzhľadom na výšku predpokladanej škody bol do 5. augusta 2024 zločin neoprávneného zásahu do počítačového systému podľa § 247a ods. 1 ods. 3 písm. a) Trestného zákona, ako aj zločin neoprávneného zásahu do počítačového údaja podľa § 247b ods. 1, ods. 3 písm. a) Trestného zákona. S účinnosťou od 6. augusta 2024 sa pri týchto zločinoch znížila horná hranica trestnej sadzby trestu odňatia slobody na 8 rokov.

V ďalšom kroku je potrebné posúdiť následky nepravdivých informácií a nedostatočnú súčinnosť v komunikácii s jednotkou CSIRT ako aj následky nepodania trestného oznámenia, čo v konečnom dôsledku môže viesť predovšetkým k zmareniu vyšetrovania incidentu, a tým aj odhalenia páchateľa(ov) útoku.

V podmienkach Českej republiky v CZoKB nie je explicitne upravená povinnosť oznámiť trestný čin v súvislosti s incidentom a zároveň trestnosť neoznámenia je viazaná len na trestné činy, ktoré sú taxatívne uvedené v § 368 ods. 1 trestného zákonníku.[94] V tomto výpočte sa nenachádzajú tzv. počítačové trestné činy v pravom zmysle, t.j. trestné činy spojené s neoprávneným prienikom alebo zásahom do počítačového systému alebo počítačových údajov (§ 230–232 trestného zákonníku). Neoznámenie trestného činu neoprávneného prístupu k počítačovému systému a neoprávneného zásahu do počítačového systému nebo nosiče informací *nie je trestné* (§ 368 ods. 1 arg. *a contrario)*. Rovnako tak nie je trestné *neprekazenie* tohto trestného činu (§ 367 ods. 1 arg. *a contrario)*.[95]

Na druhej strane v praxi motívy právnickej osoby a jej MKB pre neoznámenie trestného činu resp. incidentu ako takého (vrátane neplnenia si ďalších s tým súvisiacich povinností uvedených nižšie), môžu byť rôzne. Tieto motívy môžu byť vedené snahou minimalizovať negatívne dôsledky pre právnickú osobu, avšak takéto konanie vo všeobecnosti nie je dôvodom pre zbavenie sa prípadnej trestnoprávnej zodpovednosti.

Jedným z hlavných motívov býva reputačné riziko. Verejné priznanie kybernetického útoku môže výrazne poškodiť reputáciu spoločnosti, napríklad ak ide o finančnú inštitúciu, kde dôvera zákazníkov je kľúčová. Strata dôvery môže viesť k odchodu zákazníkov, zníženiu trhovej hodnoty a dlhodobým finančným stratám.

Ďalším významným motívom môže byť finančné riziko. Okamžité náklady spojené s reakciou na incident, nápravnými opatreniami, právnym poradenstvom a potenciálnymi sankciami

94 ŠÁMAL, P., RIZMAN, S., TEJNSKÁ, K. § 368 [Neoznámení trestného činu]. In: ŠÁMAL a kol., 2023, op. cit., s. 4596.

95 GŘIVNA, T., DVOŘÁK, M. § 230 [Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací]. In: ŠÁMAL a kol., 2023, op. cit., s. 2970.

môžu byť vysoké. Okrem toho môže byť spoločnosť vystavená žalobám zo strany zákazníkov alebo obchodných partnerov, ktorých údaje boli kompromitované.[96]

Regulačné riziko môžu byť ďalším motívom. Ak by sa odhalilo, že kybernetický incident bol spôsobený dlhodobo ignorovanými zraniteľnosťami v počítačovom systéme, mohlo by to viesť k uloženiu sankcií pre právnickú osobu a jej zodpovedných predstaviteľov zo strany regulátora (najmä NBÚ, NÚKIB).

Ďalší motív môže byť osobné riziko pre MKB. Ak sa zistí, že MKB zanedbal svoje povinnosti a ignoroval známe zraniteľnosti, môže čeliť osobným postihom vrátane straty zamestnania, pokuty alebo iných právnych následkov. Skresľovanie informácií môže byť snahou ochrániť svoju kariéru a reputáciu.

V praxi tiež môže existovať tlak zo strany vedenia spoločnosti, ktoré môže požadovať minimalizovanie škôd a zachovanie dobrého mena za každú cenu. MKB môže byť pod tlakom vedenia, aby situáciu riešil spôsobom, ktorý na prvý pohľad vyzerá najlepšie pre spoločnosť, aj keď nie je v súlade s etickými alebo právnymi predpismi.

V neposlednom rade môže byť dôvodom neoznámenia incidentu aj konkurenčný tlak. V silne konkurenčnom prostredí môže byť každá slabina alebo zlyhanie využité konkurenciou na získanie výhody. Právnická osoba môže mať strach, že priznanie bezpečnostného incidentu oslabí jej pozíciu na trhu.

3.3.2 Nepravdivé alebo skresľujúce informácie a nedostatok súčinnosti

Takéto konanie môže predstavovať pomoc pre páchateľ(ov) – útočníka(ov), a to prinajmenšom na úrovni nepriameho úmyslu. V takomto prípade prichádza do úvahy forma účasti (pomoc) k spáchaniu trestného činu útočníka(ov), prípadne spáchanie trestného činu (prečinu) nadržovania podľa § 339 ods. 1 Trestného zákona. Tohto trestného činu sa dopustí ten kto páchateľovi trestného činu pomáha v úmysle umožniť mu, aby unikol trestnému stíhaniu, trestu alebo ochrannému opatreniu. Objektívna stránka spočíva v pomoci páchateľovi po spáchaní trestného činu, pričom nezáleží, či trestný čin bol dokonaný alebo dospel len do štádia prípravy alebo pokusu.

Z hľadiska subjektívnej stránky ide o úmyselný trestný čin. Pomáhať páchateľovi v úmysle umožniť mu uniknúť trestnému stíhaniu sa rozumie také konanie, ktoré smeruje k tomu, aby sa trestné stíhania ani nezačalo (napr. zahladenie stôp, vytváranie falošných stôp, pomoc pri úteku).[97] Páchateľ nemusí poznať právnu kvalifikáciu hlavného trestného činu, nemusí mať vedomosť o začatí trestného stíhania. Pre jeho trestnú zodpovednosť stačí, že vie,

[96] Podľa správy spoločnosti IBM o nákladoch pri bezpečnostných incidentoch za rok 2024, celosvetovo priemerné náklady v dôsledku incidentu vzrástli o 10 % za jediný rok a dosiahli výšku 4,88 milióna USD, čo predstavuje najväčší nárast od začiatku pandémie. Viac IBM: Cost of a Data Breach Report 2024. Dostupné z: https://www.ibm.com/reports/data-breach [cit. 13. 8. 2024].

[97] ČENTÉŠ, J., MENCEROVÁ, I. § 339 [Nadržovanie]. In: BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J. a kol. *Trestný zákon II*. 1. vyd. Praha: C. H. Beck, 2011.

že ten, komu pomáha, spáchal trestný čin.[98] Zákon tiež nevyžaduje, aby páchateľ základného trestného činu vedel o poskytnutej pomoci.[99]

Problémy v praxi môžu vzniknúť, keď MKB úmyselne (pričom postačí nepriamy úmysel) pomáha páchateľovi vyhnúť sa trestnému stíhaniu. Tieto konania môžu byť právne kvalifikované ako trestný čin (prečin) nadržovania podľa § 339 ods. 1 Trestného zákona. Pojem „pomáha" zahŕňa akúkoľvek pomoc páchateľovi po spáchaní trestného činu[100], t.j. aj pomoc vo forme zničenia, či schovávania usvedčujúcich dôkazov (teda všetko, čo je vedené úmyslom pomôcť páchateľovi trestného činu, aby sa vyhol trestnému stíhaniu).[101] Aj keď MKB koná s cieľom vyhnúť sa reputačným stratám spoločnosti, jeho konanie môže byť v konečnom dôsledku kvalifikované ako trestný čin nadržovania, pretože vedome pomáha páchateľovi.

V podmienkach Českej republiky poukazujeme na trestný čin nadržování podľa § 366 trestního zákoníka, ktorý obsahuje rovnakú právnu úpravu, ako § 339 ods. 1 Trestného zákona.

3.3.3 Nezabezpečenie a ničenie digitálnych stôp (elektronických dôkazov)

V prípade, že právnická osoba (prevádzkovateľ základnej služby) a jej MKB nenahlásia incident a podniknú aktívne kroky smerujúce k zatajeniu alebo skresľovaniu informácií o incidente, môže to mať následok aj v podobe vzniku trestnoprávnej zodpovednosti.

Keď MKB poskytne jednotke CSIRT nepravdivé informácie a zatají skutočné bezpečnostné opatrenia a postupy, môže fakticky dochádzať k mareniu účelu trestného konania. V tomto prípade musí byť splnená podmienka, že trestné konanie už prebieha, teda musí byť minimálne vo fáze postupu pred začatím trestného stíhania. Môže ním byť tiež začatie trestného stíhania, ktoré sa začne už aj len vykonaním zaisťovacieho úkonu, neopakovateľného úkonu alebo neodkladného úkonu.[102] Takýmito úkonmi môže byť zaistenie digitálnych stôp v priestoroch prevádzky napadnutej spoločnosti, spojené so zabezpečením samotných priestorov výrobnej prevádzky ak v dôsledku incidentu napríklad došlo k nebezpečenstvu na zdraví a živote osôb, a pod. Zároveň však je potrebné uviesť, že vo väčšine prípadov hlásených incidentov je pravdepodobnosť kvalifikácie daného incidentu podľa Trestného zákona nízka[103], avšak vychádzame z popísanej modelovej situácie, kde je zjavné podozrenie na spáchanie trestného činu. Digitálne stopy, ako sú logové súbory, záznamy sieťovej komunikácie, časové pečiatky, IP adresy, súbory s metadátami, alebo forenzné obrazy

98 ČENTÉŠ, J., MENCEROVÁ, I. § 339 [Nadržovanie]. In: BURDA, ČENTÉŠ, KOLESÁR, ZÁHORA a kol., 2011, op. cit.

99 ŠÁMAL, P., RIZMAN, S., TEJNSKÁ, K. § 366 [Nadržování]. In: ŠÁMAL a kol., 2023, op. cit., s. 4578.

100 Typicky by išlo o spáchanie najmä niektorých z trestných činov neoprávneného prístupu do počítačového systému podľa § 247 Trestného zákona, neoprávneného zásahu do počítačového systému podľa § 247a Trestného zákona, neoprávneného zásahu do počítačového údaja podľa § 247b Trestného zákona, resp. neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podľa § 230 trestního zákonníku.

101 ŠAMKO, P. Trestný čin marenia spravodlivosti. *Právne Listy* [online]. 10. 1. 2012 [cit. 13. 8. 2024]. Dostupné z: https://www.pravnelisty.sk/clanky/a101-trestny-cin-marenia-spravodlivosti

102 Porov. § 199 ods. 1 Trestného poriadku.

103 POLČÁK, R., HARAŠTA, J., STUPKA, V. *Právní problémy kybernetické bezpečnosti*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2016, 127 s..

diskov, sú kľúčové pre vyšetrovanie kybernetických incidentov. Ich nezabezpečenie alebo zničenie znemožňuje overiť skutočné okolnosti útoku, identifikovať útočníkov a zistiť presný rozsah a dopad incidentu Napríklad, ak by sa uchovali logové súbory, bolo by možné identifikovať časové okno, kedy došlo k neoprávneným prístupom do systému, a IP adresy, z ktorých útoky pochádzali. Záznamy sieťovej komunikácie by mohli ukázať, aké údaje boli exfiltrované a kam boli odoslané. Metadáta súborov môžu poskytnúť informácie o tom, kto, kedy a akým spôsobom pristupoval k citlivým údajom.

Popísaným úmyselným konaním prichádza do úvahy naplnenie skutkovej podstaty trestného činu (zločinu) marenia spravodlivosti podľa § 344 ods. 1 písm. a) resp. aj písm. b) Trestného zákona. Na spáchanie tohto trestného činu postačí, ak páchateľ v konaní pred súdom alebo v trestnom konaní falšuje, pozmení alebo marí dôkaz, alebo bráni v získaní dôkazu.

Vychádzajúc z modelovej situácie je potrebné zamerať pozornosť na otázku naplnenia znaku „pozmenenie", „marenie" a „bránenie" dôkazu. Ak páchateľ manipuloval s dôkaznou situáciou tým, že sfalšoval alebo pozmenil dôkaz, alebo predložil sfalšovaný alebo pozmenený dôkaz na účel, aby sa použil v trestnom konaní ako pravý, narušil Trestným zákonom chránený záujem na spravodlivom a zákonnom rozhodnutí a vyvolal trestnoprávne relevantný následok vymedzený v skutkovej podstate trestného činu (zločinu) marenia spravodlivosti podľa § 344 ods. 1 písm. a) alebo písm. b) Trestného zákona.[104]

O „pozmenený" dôkaz pôjde spravidla vtedy, keď páchateľ vykoná rôzne zásahy do obsahu inak pravého dôkazu (napr. do pôvodného e-mailu alebo iných súborov vkladá nové údaje, respektíve „prepisuje" rôzne údaje napr. ich metadáta a pod.).

Pojmy „marenie" a „bránenie" sú postavené alternatívne vedľa seba, čo však nie je úplne logické, nakoľko za marenie dôkazu možno celkom určite považovať aj bránenie v získaní dôkazu.[105] Pojem „marenie dôkazu" vnímame ako pojem širší ako „bránenie v získaní dôkazu" a zahŕňa celú škálu konaní, ktoré buď úplne znemožňujú (napr. nezvrátiteľné premazanie diskov, zmazanie logových súborov) alebo podstatne sťažujú získanie dôkazu (napr. poskytnutie skreslených informácií o incidente, úprava časových pečiatok alebo obsahu súborov).

Pre trestnosť uvedeného konania nie je podstatné či sa aj takýto dôkaz v ďalšom konaní vykonal. Trestný čin marenia spravodlivosti je dokonaný predložením sfalšovaného alebo pozmeneného dôkazu súdu alebo orgánu činnému v konkrétnom trestnom konaní na účel, aby sa použil ako pravý, a to bez ohľadu na to, či sa v ďalšom konaní tento dôkaz vykonal.[106]

V podmienkach Českej republiky poukazujeme na trestný čin maření spravedlivosti podľa § 347a trestního zákoníka, ktorého sa dopustí páchateľ, ktorý *„pro účely* […] *trestního řízení anebo v takovém řízení předloží věcný nebo listinný důkazní prostředek, který má podstatný význam pro rozhodnutí, o kterém ví, že je padělaný nebo pozměněný, v úmyslu, aby byl použit jako pravý, anebo padělá nebo pozmění takový důkazní prostředek v úmyslu, aby byl použit jako pravý."* České trestné konanie začína spravidla záznamom o zahájení úkonu trestného konania, pokiaľ nezačalo

104 Rozsudok Najvyššieho súdu SR zo dňa 7. 5. 2015, sp. zn. 5 Tdo 8/2015.

105 ŠAMKO, 2012, op. cit.

106 Rozsudok Najvyššieho súdu SR zo dňa 7. 5. 2015, sp. zn. 5 Tdo 8/2015.

už vykonaním neodkladného alebo neopakovateľného úkonu alebo rovno začatím trestného stíhania.[107] V podmienkach Českej republiky však je potrebné pri vyhodnotení podmienok naplnenia znakov tohto trestného činu zobrať do úvahy, že v CZoKB na rozdiel od slovenskej právnej úpravy, sa explicitne neukladá regulovaných subjektom v čase incidentu zabezpečiť digitálne stopy (teda potenciálne elektronické dôkazy) tak, aby mohli byť použité v trestnom konaní.[108] Berúc do úvahy tieto odlišnosti v regulačných povinnostiach, je podľa nás možné spáchať dotknutý trestný čin ak sú v čase incidentu falšované alebo pozmenené potenciálne elektronické dôkazy.

Elektronické dôkazy možno podriadiť pod trestný čin marenia spravodlivosti § 347a ods. 1 trestního zákoníku.[109] V tejto súvislosti aj českí autori[110] uvádzajú, že sa môže jednať o falšovanie nosičov elektronických informácií, napr. vytvorenie falošného odtlačku harddisku počítača s pozmenením niektorých relevantných informácií. Falšovať možno aj samotné elektronické dôkazy tak, že sa vytvorí nový súbor, ktorý je predstieraný ako originálny súbor, hoci bol vytvorený len na dôkazné účely a má budiť dojem staršieho súboru, ktorý existoval v čase skutku. Tento súbor môže byť vložený na zabezpečený nosič informácií alebo použitý dodatočne na samostatnom nosiči informácií.

„Pozmenením" sa všeobecne rozumie neoprávnené vykonanie úpravy originálu tak, aby sa zmenila jeho výpovedná hodnota. Pozmenený originál teda vypovedá o niečom, o čom pred pozmenením nevypovedal, resp. je takto odstránený alebo pozmenený údaj, ktorým pred takýmto zásahom originál disponoval.[111] Pri elektronických dôkazoch môže ísť o pozmeňovanie vykonaním zásahu do nosiča informácií tak, aby bol pôvodný obsah informácií na ňom zaznamenaný určitým spôsobom modifikovaný. Napríklad, ak ide o informácie obsiahnuté v textovom alebo tabuľkovom súbore, alebo o metadáta súborov, napr. fotografií (sprievodné informácie o obrázku, ako dátum, čas a miesto jeho vyhotovenia, veľkosť, počet pixelov, údaje o zariadení, z ktorého bola fotografia vytvorená, vrátane značky prístroja, použitej optiky, údaje o súbore, jeho veľkosti a zmene). Okrem toho môže dôjsť aj k zásahu do samotných fotografií v grafickom editore, kde môžu byť retušované a upravované.[112]

Pokiaľ ide o vzťah s inými trestnými činmi, v nedávnej judikatúre sa český najvyšší súd vyjadril k možnosti súbehu trestných činov podvodu podľa § 209 trestního zákoníku a marenia spravodlivosti podľa § 347a trestního zákoníku, pričom potvrdil, že konaním sa možno dopustiť oboch trestných činov, a to vzhľadom na ich odlišný objekt.[113]

107 ŘÍHA, J. § 347a [Maření spravedlnosti]. In: ŠÁMAL a kol., 2023, op. cit., s. 4366.

108 Porov. § 19 ods. 6 SZoKB.

109 ŘÍHA, J. § 347a [Maření spravedlnosti]. In: ŠÁMAL a kol., 2023, op. cit., s. 4373–4374.

110 Ibid.

111 Usnesení Nejvyššího soudu ČR zo dňa 17. 1. 2024, sp. zn. 8 Tdo 1171/2023.

112 ŘÍHA, J. § 347a [Maření spravedlnosti]. In: ŠÁMAL a kol., 2023, op. cit., s. 4375.

113 Usnesení Nejvyššího soudu ČR zo dňa 31. 5. 2023, sp. zn. 11 Tdo 737/2022.

Záver

V tomto článku sme sa zamerali na problematiku trestnoprávnej zodpovednosti CISO, pričom sme analyzovali prípady identifikovaných protiprávnych konaní manažérov v spoločnostiach SolarWinds a Uber. Tieto prípady poukazujú na vysoké riziko, ktorému sú CISO vystavení nielen v USA, a na nevyhnutnosť dôkladnej analýzy a riadenia kybernetických rizík v rámci organizácií.

Na Slovensku aj v Českej republike dlhodobo evidujeme nedostatok odborníkov v oblasti kybernetickej bezpečnosti, pričom zvlášť citeľný je nedostatok manažérov kybernetickej bezpečnosti. Tento nedostatok je akútny a ovplyvňuje ako súkromný, tak verejný sektor.[114] V oboch krajinách predstavuje nedostatok odborníkov na kybernetickú bezpečnosť jednu z hlavných výziev pre inštitúcie a organizácie, ktoré sa snažia zabezpečiť ochranu svojich informačných systémov a údajov.[115]

MKB a štatutárne orgány čelia značným rizikám spojeným s ich zodpovednosťou. Zastávame právny názor, že primárnym v oblasti kybernetickej bezpečnosti je prevencia, predchádzanie porušenia zákona. Preto aj cieľom tohto článku je predchádzať vzniku týchto rizík, identifikovať rizikové oblasti a naznačiť, že samotné trestné represie nebudú postačujúce na dosiahnutie spoločného cieľa, ktorých je zvyšovanie úrovne kybernetickej bezpečnosti. Je potrebné sa zamyslieť na efektívnosťou trestnej represie aj vzhľadom na možnosti, ktoré prinášajú rôzne opatrenia v netrestnej oblasti. Pôjde predovšetkým o nástroje samoregulácie a správneho trestania. Na druhej strane trestné právo by malo nastúpiť v prípadoch najzávažnejšieho úmyselného protiprávneho konania.

Podstatné zvýšenie počtu MKB, zlepšenie ich odborného vzdelania a vypracovanie primeraných interných predpisov v postupoch a rozhodovaní MKB predstavuje jednu z aktuálnych výziev fungovania organizácií.

Tento článok preto vnímame ako otvorenie diskusie na analyzovanú problematiku a má za cieľ povzbudiť ďalší výskum a dialóg medzi odborníkmi, manažérmi kybernetickej bezpečnosti a regulátormi. Len prostredníctvom spolupráce a zdieľania poznatkov môžeme dosiahnuť vyššiu úroveň kybernetickej bezpečnosti a minimalizovať riziká spojené so zodpovednosťou MKB v tejto dynamicky sa rozvíjajúcej oblasti.

[114] V kybernetickej bezpečnosti máme nedostatok ľudí. Problém nám pomáha riešiť Európska únia. *NBÚ* [online]. 19. 10. 2023 [cit. 21. 4. 2024]. Dostupné z: https://www.nbu.gov.sk/2023/10/19/v-kybernetickej-bezpecnosti-mame-nedostatok-ludi-problem-nam-pomaha-riesit-europska-unia/index.html

[115] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. *NÚKIB* [online]. 19. 7. 2023, s. 12 [cit. 21. 4. 2024]. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/