https://doi.org/10.5817/RPT2021-1-2

VAROVÁNÍ NÚKIB V SYSTEMATICE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A MOŽNOSTI JEHO ZOHLEDNĚNÍ V ZADÁVACÍM ŘÍZENÍ[1]

JAKUB KLODWIG[2]

ABSTRAKT

Článek se nejprve zabývá pojmovou nejednotností a používáním slova „opatření“ v systematice zákona o kybernetické bezpečnosti, tak aby nedocházelo k záměně těchto jazykově velice podobných institutů. Po jasném vymezení názvosloví a charakteru jednotlivých opatření je detailně pojednáno o institutu varování, který je v mezinárodním srovnání poměrně specifický. Klade totiž vysoké nároky na samostatnou činnost povinných osob, díky čemuž však umožňuje vhodně stupňovat bezpečnostní opatření povinných osob, a tak efektivně reagovat na kyberbezpečnostní hrozby různé intenzity. Dále je prakticky pojednáno o problematickém promítnutí performativních pravidel práva kybernetické bezpečnosti a vysoce formalizovaných administrativních pravidel zadávání veřejných zakázek. Po vysvětlení správného zohlednění varování veřejnými zadavateli jsou v souladu s podpůrnými materiály NÚKIB a aktuální rozhodovací praxí předestřeny také způsoby, jakými lze v různých fázích zadávacího řízení obsah varování promítnout do předmětu veřejné zakázky.

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg. č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR.

[2] Mgr. Jakub Klodwig je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně. Kontaktní e-mail: Jakub.Klodwig@law.muni.cz

KLÍČOVÁ SLOVA:

Opatření, protiopatření, varování, kybernetická bezpečnost, veřejné zakázky, právo veřejných zakázek, právo kybernetické bezpečnosti, právo ICT, NÚKIB, ÚOHS, zadávací dokumentace, hospodářská soutěž, diskriminace.

ABSTRACT

At first, the article deals with the conceptual inconsistency and the use of the word "measures" in the system of the Cyber Security Act, to not to confuse these linguistically very similar legal institutes. After a clear definition of the nomenclature and nature of measures, the institute of warning is discussed in detail. It is a specific institute in international comparison, which places high demands on individual activity of its recipients. However, it enables the recipient's security measures to be appropriately stepped up, and thus to respond effectively to cybersecurity threats of different intensity. Furthermore, the problematic projection of performative rules of cyber security law and highly formalized administrative rules of public procurement law are practically discussed. After explaining the correct implementation of warning by public authorities, the ways in which the content of warning could be reflected as a subject of a public contract are also presented at various stages of the procurement procedure, in accordance with the supporting materials of NÚKIB and current decision-making practice.

KEYWORDS

Measure, countermeasure, warning, cyber security, public procurement, public procurement law, cyber security law, ICT law, NÚKIB, ÚOHS, procurement documentation, competition, discrimination.

1. ÚVOD

Česká republika byla v celosvětovém srovnání jedním z prvních států, které přijaly vlastní komplexní právní úpravu kybernetické bezpečnosti.[3] V roce 2015, kdy byl v českém právním řádu již účinný systém skládající se ze zá-

[3] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*. 2015, roč. 6, č. 11, s. 95.

kona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „***ZKB***“), a prováděcích podzákonných právních předpisů, evropský normotvůrce unijní regulaci ve formě Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „***směrnice NIS***“) teprve formoval. Není proto divu, že některé právní instituty práva kybernetické bezpečnosti jsou v českém právním řádu odlišné od právní úpravy jiných členských států Evropské unie, které při přijímání vlastní regulace kybernetické bezpečnosti vycházely primárně z harmonizačních vodítek směrnice NIS. Právní úprava kybernetické bezpečnosti těchto států byla tudíž logicky určována primárně rámcem směrnice NIS a nikoliv již tolik vlastní legislativní invencí, jako tomu bylo v případě České republiky. Ačkoliv tedy byla směrnice NIS promítnuta s účinností od 1. srpna 2017 i do českého ZKB prostřednictvím zákona č. 205/2017 Sb.,[4] kterým byl založen také samostatný Národní úřad pro kybernetickou a informační bezpečnost (dále jen „***NÚKIB***“),[5] tak specifické prvky a originální instituty, které byly tou dobou již etablované, v českém právním řádu zůstaly. Jedním z nich je institut varování dle § 12 ZKB (dále jen „***varování***“),[6] o jehož specifikách a vlivech na právo zadávání veřejných zakázek tento článek pojednává.

[4] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

[5] Vznik samostatného ústředního orgánu státní správy pro kybernetickou bezpečnost byl přitom také důležitým krokem vpřed, který dosud ještě neučinila ani řada vyspělých západních států, včetně např. U.S.A. Tato poměrně brzká emancipace NÚKIB svědčí o významu a snaze o rozvoj kybernetické bezpečnosti v České republice.

[6] Výjimkou je např. právní řád Slovenska, které však vzhledem k historické, kulturní i jazykové blízkosti čerpalo právě z konceptu českého ZKB, viz např. § 27 zákona č. 69/2018 Z.z., o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, když přijalo vlastní „varovanie“, „reaktívne opatrenie“ a „ochranné opatrenie“, nebo právní řád Německa, který stejně nazvaný institut s jinými parametry zakotvuje ve svém § 7 zákona (BSIG) o Spolkovém úřadu pro bezpečnost v informační technice.

2. TERMINOLOGIE OPATŘENÍ DLE ZKB

Varování před kybernetickou hrozbou je jedním ze zákonných nástrojů, kterými může NÚKIB upozornit na existenci hrozby v oblasti kybernetické bezpečnosti a ovlivnit tak bezpečnost v klíčových českých institucích. Kromě varování má NÚKIB k dispozici také další opatření dle § 11 ZKB, kterými jsou reaktivní opatření a ochranná opatření. ZKB definuje v § 11 odst. 1 tato opatření jako: „*úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.*“ Vzhledem k tomu, že označení „opatření“ je dle této definice samostatným pojmem, je z hlediska terminologie ZKB problematické, že slovo „opatření“ je součástí šesti dalších sousloví, které ZKB používá jako další pojmy. Kromě reaktivního opatření a ochranného opatření, která jsou opatřeními definovanými výše, vymezuje ZKB ještě bezpečnostní opatření, organizační opatření, technická opatření a nápravná opatření, která však nejsou opatřeními ve smyslu § 11 ZKB. Otázka, která opatření jsou opatřeními může proto mezi studenty práva nebo právníky neznalými kybernetické bezpečnosti působit oprávněné zmatení.

Bezpečnostní opatření jsou základním pojmem v terminologii kybernetické bezpečnosti, který je definovaný v § 4 odst. 1 ZKB. Pojem bezpečnostní opatření označuje množinu různých úkonů, které mají za cíl zvýšit kybernetickou bezpečnost určitého subjektu, a to ať již z důvodu prevence či v reakci na reálnou hrozbu. Vzhledem k tomu, že základním účelem ZKB a obecně práva kybernetické bezpečnosti je zvýšení kybernetické bezpečnosti informačních a komunikačních systémů (dále jen „***informačních***

systémů“),[7] jsou bezpečnostní opatření všemi těmi úkony, kterými lze tohoto cíle dosáhnout. Základní členění bezpečnostních opatření je vymezené v § 5 odst. 2 a 3 ZKB, a sice na organizační, soustředící se primárně na personální a dokumentační činnosti, a technická opatření. Vzhledem k šíři celého spektra úkonů, které bezpečnostní opatření pokrývají, se tak logicky jedná spíše o výčet kategorií, které vzhledem k performativnímu charakteru regulace musí povinné osoby zohlednit při nalézání a indukci povinností na jejich konkrétní situaci. Jakkoliv tedy byla rozdílná míra konkretizace v taxativně uvedených bezpečnostních opatřeních v minulosti kritizována,[8] lze jejich bližší vymezení najít v části II. vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***VKB***“). Tato specifikace, zřetelně inspirovaná normami ISO/IES 27000, by tak měla posloužit subjektům povinným dle ZKB nalézt konkrétní řešení obecných požadavků ZKB.

Před dalším již detailnějším výkladem konkrétních druhů opatření, je vhodné zmínit ještě nápravná opatření, která stejně jako bezpečnostní opatření nejsou opatřeními ve smyslu § 11 ZKB. Nápravná opatření jsou specifickým institutem situovaným do § 24, který dává NÚKIB pravomoc jejich prostřednictvím nařídit kontrolovanému subjektu konkrétní povinnost a případně i způsob jakým ji musí splnit. Pokud jsou zjištění kontroly NÚKIB v určitých případech tak vážná, že hrozí významné poškození nebo

---

[7] Autor se domnívá, že „*komunikační systém*“ je významově vyprázdněný pojem, od jehož používání bude s vývojem terminologie ZKB upuštěno, jelikož definice informačního systému v sobě zahrnuje také jeho komunikační složku. Z tohoto důvodu bude v této práci nadále pod pojem „*informační systém*“ podřazován také „*komunikační systém*“. Obdobně viz VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0 nebo také ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

[8] POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 603.

zničení informačního systému, může NÚKIB nápravným opatřením používání informačního systému na stanovenou dobu dokonce i zakázat.[9] Jakkoliv se jedná o poměrně velký zásah do autonomie vůle daného subjektu, je NÚKIB oprávněn nápravné opatření použít pouze pro nápravu nedostatků, které identifikoval při kontrole dle zákona č. 255/2012 Sb., o kontrole (kontrolního řádu), ve znění pozdějších předpisů.

Při jednání o bezpečnostních opatřeních, nápravných opatřeních či ochranných opatřeních, může často dojít ke zkrácení těchto výrazů na pouhá „opatření", a to nejen při komunikaci verbální. Záliba zákonodárce ve slově „opatření" proto budí rozpaky, zvláště pokud slovo „opatření" zavede do šesti různých pojmů v ZKB, a k tomu přidá význam i samostatnému slovu „opaření". V takovém případě lze proto uvítat iniciativu akademické obce, která opatřením dle § 11 ZKB začala přezdívat „protiopatření".[10] Tato přezdívka konvenuje významu tohoto právního institutu, který směřuje proti hrozbě či již proti probíhajícímu kybernetickému bezpečnostnímu incidentu a zároveň alespoň částečně řeší předestřený terminologický překryv. Z tohoto důvodu lze iniciativu ocenit a v zájmu vyšší přehlednosti zavedený pojem „protiopatření" dále používat za účelem zpřehlednění celé problematiky.[11]

3. SPECIFIKA PRÁVNÍHO INSTITUTU VAROVÁNÍ

Varování je jedním z trojice protiopatření, které má NÚKIB dle § 11 ZKB k dispozici, pokud zjistí, že míra hrozby překročila určitou hranici, a tudíž o hrozbě nestačí jen neformálně informovat (např. na vlastních webových stránkách nebo na sociálních sítích), ale je nezbytné přistoupit k některému z těchto tří formálních nástrojů. Kritériem pro volbu vhodného protiopat-

[9] Dle § 24 odst. 2 se jedná pouze o případy, kdy toto hrozí pro systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém.

[10] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, s. 30.

[11] V souladu s touto výzvou, bude opatření dle § 11 ZKB nadále v článku označováno již jen jako „protiopatření". Ostatní instituty, které se však do protiopatření řadí (tedy varování, reaktivní opatření a ochranné opatření) není nezbytné přezdívat, jelikož mají díky odlišnému přídavnému jménu v názvu dostatečnou rozlišovací způsobilost bez dalšího. V tomto duchu lze doporučit také úpravu terminologie samotného zákona.

ření přitom není míra rizika, jak by se mohlo na první pohled zdát, ale fáze, ve které se kybernetický bezpečnostní incident v daný okamžik nachází. Těmito fázemi rozumíme:

1. Fázi identifikace hrozby v oblasti kybernetické bezpečnosti;
2. Fázi bezprostředně hrozícího nebo již probíhajícího kybernetického bezpečnostního incidentu;
3. Fázi po ukončení kybernetického bezpečnostního incidentu.

Podle charakteru situace a funkce, kterou v ní hrají jednotlivá protiopatření, se liší také jejich právní forma. Zatímco varování je vydáváno ve formě úkonu podle části čtvrté zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „***správní řád***“), reaktivní i ochranné opatření ZKB umožňuje vydávat formou opatření obecné povahy.[12] Na rozdíl od varování tak reaktivním i ochranným opatřením může NÚKIB povinným osobám přímo uložit konkrétní povinnost. Vrchnostenský příkaz provést konkrétní úkon pod hrozbou pokuty je společný rys, který má jak reaktivní opatření, tak také ochranné opatření. Tato možnost koresponduje se situací, kdy kybernetický bezpečnostní incident bezprostředně ohrožuje nebo již zasáhl větší množství ohrožených subjektů, a je nezbytné, aby všechny tyto subjekty povinně přijaly určitá bezpečnostní opatření. V takovém případě lze reaktivním opatřením vrchnostensky nařídit provedení bezpečnostních opatření k odvrácení kybernetického bezpečnostního incidentu neurčitému množství povinných subjektů vymezených pomocí generických znaků, jako je například používání zranitelného softwaru.[13] K tomu, aby bylo opatření obecné povahy efektivní, využívá zákonodárce výjimky v § 173 odst. 1 správního řádu[14] a v § 15 ZKB stanoví, že protiopatření, která jsou opatřeními obecné povahy, nabývají účinnosti okamžikem jejich vyvěšení na úřední

[12] ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

[13] O tento typ se jednalo například při vydání reaktivního opatření k zabezpečení informačních systémů používajících Microsoft Exchange dne 11. 3. 2021.

[14] § 173 odst. 1 správního řádu: *„[…] Opatření obecné povahy nabývá účinnosti patnáctým dnem po dni vyvěšení veřejné vyhlášky. Hrozí-li vážná újma veřejnému zájmu, může opatření obecné povahy nabýt účinnosti již dnem vyvěšení; stanoví-li tak zvláštní zákon, může se tak stát před postupem podle § 172. Do opatření obecné povahy a jeho odůvodnění může každý nahlédnout u správního orgánu, který opatření obecné povahy vydal.“*

desce NÚKIB. Díky této výjimce zaručující okamžitou účinnost opatření obecné povahy spolu s nemožností podat proti němu opravný prostředek, se jedná o vhodný a efektivní nástroj pro ochranu většího množství subjektů před kybernetickými bezpečnostními incidenty.

Avšak v případě, že kybernetický bezpečnostní incident ohrožuje pouze jeden subjekt nebo více konkrétních subjektů,[15] nelze pak využít opatření obecné povahy.[16] Právě pro tuto druhou variantu kybernetického bezpečnostního incidentu ZKB umožňuje vydat reaktivní opatření formou rozhodnutí, proti němuž nemá případný rozklad odkladný účinek. Zákonodárce tak reaguje i na tuto druhou variantu kybernetického bezpečnostního incidentu, kdy je nezbytné rychle zavést příslušná bezpečnostní opatření u konkrétního napadeného subjektu v zájmu ochrany jeho informačních systémů.

Obdobně také ochranné opatření může formou opatření obecné povahy vrchnostensky uložit povinnost neurčitému množství genericky vymezených subjektů přijmout bezpečnostní opatření po skončení bezpečnostního incidentu. Účelem ochranného opatření je zamezit opakování nebo adekvátně zvýšit ochranu informačních systémů v návaznosti na zkušenosti získané při odrážení již odeznělého kybernetického bezpečnostního incidentu.[17]

Varování je vedle toho právním institutem, který je značně odlišný od ostatních protiopatření. Varování nelze vydat ani formou opatření obecné povahy, ani formou rozhodnutí, ale formou sdělení podle hlavy čtvrté správního řádu. To znamená, že varováním nelze vrchnostensky uložit povinnost, nebo za jeho nedodržení uložit sankci, jako je to možné u ostatních

---

[15] Jedná se tedy o konkrétní předmět regulace.

[16] Okruh adresátů je u opatření obecné povahy z definice vymezen obecně, a tudíž nemůže dopadat adresně na konkrétní subjekt. Více viz HEJČ, David. Reaktivní a ochranná opatření (obecné povahy) před kybernetickým bezpečnostním incidentem. In: *Cofola 2015 : The Conference Proceedings*. 2015. vyd. Brno: Masarykova univerzita, 1975, s. 22–23.

[17] VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0.

protiopatření. Varování také dopadá na jiný okruh povinných subjektů, kterými jsou kromě správců a provozovatelů informačního systému kritické informační infrastruktury (dále jen „***KII***“), správců a provozovatelů významných informačních systémů (dále jen „***VIS***“), a správců a provozovatelů informačních systémů základní služby (dále jen „***ISZS***“), také všechny další subjekty dle § 3 ZKB včetně poskytovatelů služeb elektronických komunikací a subjektů zajišťujících síť elektronických komunikací, orgánů nebo osob zajišťujících významnou síť, provozovatelů základní služby, a také poskytovatelů digitální služby (souhrnně dále jen „***regulované subjekty***“).[18]

K vydání varování je NÚKIB, jakožto ústřední orgán státní správy pro kybernetickou bezpečnost, oprávněn a zároveň povinen[19] v případě, že se dozví z vlastní činnosti, z podnětu provozovatele vládního CERT,[20] anebo od orgánů vykonávajících působnost v oblasti kybernetické bezpečnosti v zahraničí o hrozbě v oblasti kybernetické bezpečnosti. Pokud tedy nestačí na kybernetickou hrozbu upozornit neformálně, například na vlastních webových stránkách,[21] ale výše hrozby překročí určitou míru,[22] zveřejní NÚKIB varování dle § 12 odst. 2 ZKB na svých internetových stránkách, a oznámí jej také regulovaným subjektům.[23] Ty nadále ze samotného titulu varování nemají žádné konkrétní povinnosti, co musí s takto získanou informací dělat. Související povinnosti však vyplývají z jiných titulů, jako např. varování zohlednit v hodnocení rizik, přičemž pravidelně provádět hodnocení rizik je všední odpovědností některých regulovaných subjektů, jak bude uvedeno níže. Role samotného institutu varování by se tedy dala

[18] Výčet je stanoven v § 3 ZKB.

[19] Viz § 22 písm. b) ZKB.

[20] Jedná se o vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT - Computer Emergency Response Team).

[21] Tyto lze sledovat v rubrice „Vybrané aktuality, hrozby a doporučení“ na úvodní stránce NÚKIB, viz: https://www.nukib.cz/.

[22] Tato míra rizika přitom zhruba odpovídá kritickému stupni dle přílohy č. 2 VKB, popisovaném jako riziko nepřípustné, při němž musí být neprodleně zahájeny kroky k jeho odstranění.

[23] Oznámeno bude na příslušné kontaktní údaje regulovaných subjektů, vedené v evidenci podle § 16 odst. 4 ZKB. Současně by varování mělo být zpřístupněno na webových stránkách NÚKIB po celou dobu své platnosti a účinnosti.

označit za oficiální předání aktuální a věrohodné informace o zhoršení kyberbezpečnostní situace od úřední autority. Význam takového prokazatelného sdělení přitom vytváří očekávání společnosti, že regulovaný subjekt bude adekvátně reagovat. Informace totiž není pouhým dohadem, nebo spekulací v tisku, ale vážně míněnou adresnou zprávou, která může pocházet od tuzemských zpravodajských služeb, zahraničních spojenců či v různé míře vycházet z tajných informací. Pokud tedy autorita jako je ústřední orgán státní správy varování vydá, nelze pochybovat o tom, že se jedná o pečlivě vyhodnocené informace, které byly z množství utajovaných informací zformovány do jasného sdělení. Ačkoliv je tedy podstatou varování pouze oficiální předání informací o určité bezpečnostní hrozbě pro informační systémy regulovaných subjektů, má konstrukce varování závažné nepřímé dopady, které v systému práv a povinností regulovaných subjektů dosahují svého účelu i bez hrozeb přímých sankcí či autoritativních zásahů do autonomie vůle regulovaných subjektů.[24]

Obecně totiž mají všichni správci a provozovatelé informačních systémů obecnou odpovědnost za své systémy, a případně také za služby, které prostředním nich poskytují. Slovy § 2903 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***OZ***“): „*Nezakročí-li ten, komu újma hrozí, k jejímu odvrácení způsobem přiměřeným okolnostem, nese ze svého, čemu mohl zabránit.“* Z tohoto důvodu má již neformální informování NÚKIB na svých webových stránkách určitý význam, jelikož průběžně informuje o nejrůznějších hrozbách a zranitelnostech, kterým by osoby odpovědné za bezpečnost informačních systémů měly ve svém zájmu věnovat pozornost. Zejména regulované subjekty, které spravují ty nejvýznamnější informační systémy či kritickou informační infrastrukturu a jsou si vědomi, jaké důsledky by jejich omezení nebo zničení mohlo způsobit, by měly o to více preventivně dbát o jejich bezpečnost. V tomto

[24] O nezanedbatelném efektu ostatně svědčí také mediální popularita a reakce v nejrůznějších světových médiích, které vyvolala v minulosti již vydaná varování NÚKIB. Viz např. KAHN, Jan Lopatka, Michael. Czech cyber watchdog says its Huawei warning took U.S. by surprise. *Reuters* [online]. 2019 [vid. 24. 3. 2021]. ; SANTORA, Marc; GOEIJ, Hana de. Huawei Was a Czech Favorite. Now? It's a National Security Threat. *The New York Times* [online]. 2019 [vid. 24. 3. 2021].

kontextu je proto varování velice vhodným právním institutem, který umožňuje stupňovat povinnosti, a tím adekvátně reagovat na takové hrozby, které by již vyžadovaly vyšší míru pozornosti než při běžné prevenci, ale přímý vrchnostenský zásah do správy regulovaných subjektů je stále nástroj příliš invazivní.[25]

Oficiálním předáním informací od NÚKIB o potenciálně hrozícím bezpečnostním incidentu je tedy do jisté míry povinnost se s hrozbou vypořádat, předána na regulované subjekty, jelikož se varování promítne do dalších povinností regulovaných subjektů, které budou detailněji popsány v následující kapitole. V případě, že by regulovaný subjekt nedbal varování, vystavuje se odpovědnosti nejen za škodu na vlastní infrastruktuře, ale také povinnosti hradit škodu svých zákazníků či obchodních partnerů způsobenou rizikem, o kterém regulovaný subjekt věděl, a neučinil dostatečné kroky k jeho odvrácení. V tomto kontextu přitom hrozí, že regulovaný subjekt může být odpovědný také za škodu nebo jinou újmu způsobenou třetím osobám, pokud se dle § 2901 OZ prokáže, že regulovaný subjekt: „*může podle svých možností a schopností snadno odvrátit újmu, o níž ví nebo musí vědět, že hrozící závažností zjevně převyšuje, co je třeba k zákroku vynaložit.*“[26]

4. DŮSLEDKY VAROVÁNÍ PRO REGULOVANÉ SUBJEKTY V PRAXI

Za dobu své existence vydal NÚKIB již čtyři protiopatření, z čehož se jednalo postupně o dvě varování a následně o dvě reaktivní opatření.[27] Historicky první varování bylo vydáno dne 17. 12. 2018, v následujícím znění: „*Použití technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností představuje hrozbu v oblasti kybernetické bezpečnosti.*“.[28] Druhé varování ze dne 16. 4.

[25] Nutno také zmínit, že je velice problematické pro jakýkoliv externí subjekt včetně NÚKIB diagnostikovat a vyhodnotit vhodná bezpečnostní opatření pro konkrétní informační systém, bez znalosti jeho prostředí a reálného fungování.

[26] POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 610.

[27] Počítáno bez reaktivních opatření, která podléhají utajení ke dni 25. 5. 2021.

[28] Všechna protiopatření jsou dostupná na: https://nukib.cz/cs/uredni-deska/.

2020 pak reagovalo na akutní ohrožení zejména českého zdravotnictví, zatíženého koronavirovou krizí před rozsáhlou kampaní závažných kybernetických útoků. Účinnost druhého varování NÚKIB zrušil 20. 5. 2020, jelikož došlo ke snížení pravděpodobnosti dané hrozby. Dne 16. 12. 2020 vydal NÚKIB reaktivní opatření formou opatření obecné povahy, které ukládalo povinným osobám podle § 3písm. c) až f) ZKB povinnosti v souvislosti s platformou Orion od společnosti SolarWinds, a naposledy 12. 3. 2021 vydal NÚKIB další reaktivní opatření formou opatření obecné povahy k zabezpečení informačních systémů regulovaných subjektů, používajících Microsoft Exchange Server. Vzhledem k povaze reaktivních opatření, které nemají dlouhotrvající efekt a k ukončení druhého z varování, zůstává pro regulované subjekty stále nejvýznamnější první varování ze 17. 12. 2018. V současnosti nic nenasvědčuje tomu, že jeho platnost bude v blízké době ukončena, a v kontextu výrazného rozšiřování regulovaných subjektů, jejichž počet by se měl mezi lety 2020 až 2025 téměř ztrojnásobit, význam tohoto varování opět roste.[29]

V souladu s výše uvedeným lze potvrdit, že varování nestanovuje regulovaným subjektům žádné konkrétní pokyny ani povinnosti, nicméně významově na varování navazují povinnosti stanovené v jednotlivých odstavcích § 4 ZKB, které s ním dále pracují. Nejprve § 4 odst. 2 a 3 stanovuje správcům a provozovatelům informačních systémů KII, VIS, ISZS (dále jen „***povinné osoby***“) a poskytovatelům digitálních služeb[30] obecnou povinnost zavést a provádět vhodná bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti. Odst. 4 ZKB pak následně tuto generální povinnost dále rozvádí, když povinným osobám ukládá, aby zohlednily požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro

[29] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020, s. 10 [vid. 23. 3. 2021].

[30] Poskytovatelům digitální služby na rozdíl od ostatních povinných osob nestanovuje konkrétní povinnosti VKB, ale prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

jejich informační systémy. To znamená, že bezpečnostní opatření, která povinné osoby zavedly na základě vlastních hodnocení rizik, jsou povinny přenést také na své dodavatele skrze smluvní ujednání, která s nimi uzavřou.

Obdobně pak také § 4 odst. 5 ZKB ukládá povinným osobám a provozovatelům základní služby, pokud jsou orgánem veřejné moci,[31] ve smlouvě s poskytovatelem cloud computingu upravit celý výčet nezbytných náležitostí. Všechna tato ustanovení tudíž ukládají povinnosti, do jejichž plnění se obsah varování pravděpodobně promítne. Povinné osoby totiž musí veškerá protiopatření včetně Varování zohlednit ve svých pravidelně prováděných hodnoceních rizik v souladu s § 5 odst. 1 písm. h) č. 3 VKB, a to podle požadavků § 5 VKB zabývajícího se řízením rizik. Povinné osoby musí hodnocení rizik provést také před výběrem významného dodavatele, v souladu s § 8 VKB a pravidelně je přezkoumávat. To obnáší nejprve analyzovat prostředí a prošetřit, jakým způsobem budou rizikové prostředky v informačních systémech využívány, a na základě této znalosti formulovat konkrétní či typové hrozby.[32] Je nutné v dedukci důsledků varování postupovat na základě konkrétních zkušeností zadavatele tak, aby pokud možno nebyly opomenuty žádné aspekty potenciální hrozby.[33] Následně je nezbytné aktualizovat hodnocení rizik a zhodnotit tato rizika ve světle varování. K hodnocení rizik může povinná osoba využít přílohu č. 2 VKB (nebo jakoukoliv jinou metodiku, jenž zabezpečí stejnou nebo vyšší úroveň procesu řízení rizik), pomocí které pro sebe vypočítá na základě hodnoty aktiv dle přílohy č. 1 k VKB, hodnoty hrozby a také zranitelnosti

[31] Toto ustanovení se v případě přijetí právě projednávaného legislativního návrhu, bude pravděpodobně rozšiřovat na všechny orgány veřejné moci.

[32] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení.* [online] 4. 1. 2020, s. 10 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[33] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení.* [online] 4. 1. 2020, s. 10 [vid. 23. 1. 2021]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-2-podpurny-material-nukib-pdf.aspx.

dle přílohy č. 2 k VKB hodnotu rizika.[34] V případě postupu podle VKB se hodnota rizika vypočte na základě hodnoty aktiv dle přílohy č. 1 k VKB, hodnoty hrozby a také zranitelnosti dle přílohy č. 2 k VKB. Výsledná hodnota rizika pak je součinem hodnot hrozby, zranitelnosti a dopadu na aktivum, což je v souladu s § 5 odst. 1 písm. d) VKB.[35] Na základě hodnocení rizik identifikovaných v provedené analýze jsou tedy povinné osoby povinny na riziko adekvátně reagovat. Touto reakcí bude velice pravděpodobně přijetí bezpečnostních opatření, která si v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotu daného rizika povinné osoby samy navrhnou. To znamená, že bezpečnostní opatření snižují pravděpodobnost realizace identifikovaných nežádoucích jevů na přijatelnou úroveň. Díky znalosti vlastních informačních systémů jsou regulované subjekty logicky těmi nejpovolanějšími k posouzení a vyhodnocení vhodných bezpečnostních opatření, které je v dané situaci vhodné přijmout. Bylo by totiž zjevně neefektivní plošně aplikovat na všechny ohrožené informační systémy stejná bezpečnostní opatření bez ohledu na druh, způsob nastavení, či jiná specifika předmětných informačních systémů. Povinnost provést hodnocení rizik platí jak pro stávající, tak i pro nově poptávané informační systémy, přičemž řádně provést hodnocení rizik je alfou omegou pro případné ověření či přezkoumání přiměřenosti přijatých bezpečnostních opatření.

Kromě regulovaných subjektů má varování vliv také na dodavatele, kteří dodávají technické nebo programové prostředky regulovaným subjektům. Ty mohou být buď v pozici provozovatele určeného informačního systému podle § 2 písm. g) ZKB, pokud pro regulovaný subjekt zajišťují funkčnost technických a programových prostředků tvořících informační systém, anebo v pozici běžného dodavatele. Provozovatelům určených informačních

[34] SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.mvcr.cz/soubor/5-saskova-vladena-varovani-pred-kybernetickou-hrozbou-podle-12-zkb.aspx.

[35] Hodnota hrozby po zveřejnění varování bude v nejvyšším stupni, tedy ve výši 4 ze 4, pokud bude použita stupnice podle VKB. Pokud bude použita jiná metoda výpočtu, pak bude obdobně hodnota hrozby zvýšena na nejvyšší hodnotu, a to ačkoliv mohou být vzorce výpočtu různé.

systémů vyplývají povinnosti přímo ze ZKB, zatímco běžným dodavatelům ZKB žádné povinnosti neukládá. Běžní dodavatelé jsou tak dotčeni povinnostmi vyplývajícími ze ZKB pouze nepřímo skrze pokyny zadavatelů, pokud tito mají povinnost běžné dodavatele řídit dle § 8 VKB.

Ačkoliv je varování adresované pouze regulovaným subjektům, mohou ostatní subjekty varování zohlednit dobrovolně (dále jen „***nepovinní***"). Z hlediska kybernetické bezpečnosti není přitom rozhodné, zda má subjekt povinnost varování zohlednit z jiného důvodu (např. požadavek zřizovatele, snaha o získání certifikace ISO 27000, apod.), ale pouze zda tuto povinnost ukládá zákon.[36] V souladu s prevenční povinností dle OZ,[37] je ostatně zavedení přiměřených bezpečnostních opatření dle varování nepovinnými naprosto nezávadné a bezpochyby také v souladu s péčí řádného hospodáře. Je však nezbytné dát si pozor na to, jak budou nepovinní s varováním pracovat. Zásadní totiž je, že kvůli absenci povinnosti varování reflektovat v rámci zavádění a provádění bezpečnostních opatření podle § 4 odst. 2 ZKB se na tyto subjekty neuplatní § 4 odst. 4 ZKB ani odst. § 4 odst. 7 ZKB, zakotvující presumpci souladnosti bezpečnostních opatření s podmínkami hospodářské soutěže, a tudíž bude záviset pouze na provedeném hodnocení rizik nepovinného, a na kvalitě jeho argumentace. Hodnocení rizik a na základě něj přijatá bezpečnostní opatření, tedy musí být o to lépe vyargumentovaná, zdokumentovaná a nesmí být zmatečná a nepřezkoumatelná. Velice snadno se totiž může stát, že nepovinný v dobré víře slepě přejme předmět varování jako dogma, a nikoliv jako vstup pro vlastní zhodnocení rizika. Takové chování by však znamenalo nepochopení právní úpravy a svévolné vytváření podmínek, které mohou být v kontextu zadávání veřejných zakázek posouzeny jako bezdůvodné překážky hospodářské soutěže. V takovém případě se však nepovinný vystavuje souvisejícím sankcím, které pro veřejného zadavatele mohou mimo jiné znamenat i zrušení veřejné zakázky.

---

[36] Rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 13. 1. 2020 sp. zn. S0358/2019/VZ, bod 59. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[37] Detailnější popis prevenční povinnosti viz kapitola III.

5. VZTAH ZZVZ A ZKB

Zadávání veřejných zakázek je právem detailně regulovaný a vysoce formalizovaný proces výběru smluvního partnera pro uzavření smlouvy zadavatelem, upravený zejména v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***“) a příslušných prováděcích předpisech. Zadávání veřejných zakázek se tak odlišuje od jinak málo regulovaného, a principem smluvní svobody a dispozitivnosti se řídícího kontraktačního procesu dle OZ.[38] Kromě zásad transparentnosti, přiměřenosti a rovného zacházení je proces zadávání veřejných zakázek založen zejména na zásadě zákazu diskriminace dodavatelů,[39] což má zajišťovat rovnou a nediskriminační soutěž všech dodavatelů v zájmu hospodárného, efektivního a účelného vynakládání veřejných prostředků.

Vedle toho ZKB sleduje jiné cíle, jakými je zajištění ochrany kybernetického prostoru České republiky, zajištění základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací, a obrana nedistributivních práv státu, včetně veřejného zájmu na KII, VIS a poskytování základních služeb.[40] Tyto kyberbezpečnostní cíle, které jsou dle důvodové zprávy jedním z určujících aspektů bezpečnostního prostředí v České republice,[41] ale nemusí bez dalšího odpovídat výše uvedenému rovnému přístupu ZZVZ k výběru dodavatele. ZKB totiž do zadávacího řízení vnáší jiné hodnoty, než je pouze čistě ekonomický zájem, a sice zájem bezpečnostní. ZKB tak při akcentu na zachování kybernetické bezpečnosti není překážkou hospodářské soutěži, ale vnáší do hospodářské soutěže nové mantinely, ve kterých se hospodářská soutěž odehrává.

---

[38] DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. § 1 [Předmět úpravy]. In: DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. Zákon o zadávání veřejných zakázek. 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 1.

[39] § 6 ZZVZ.

[40] Vláda: Důvodová zpráva k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz.

[41] Ibidem.

ZZVZ a ZKB jsou oba zákonnými předpisy stejné právní síly. Nejsou tedy vůči sobě ve vztahu nadřízenosti a podřízenosti ani obecnosti a speciality.[42] Z toho vyplývá, že subjekty, které současně spadají do působnosti obou zákonů, jsou povinny postupovat tak, aby dostály povinnostem, které na ně kladou současně oba právní předpisy. Není přitom výjimkou, že regulované subjekty jsou současně zadavatelé dle ZZVZ.[43] Propojení těchto dvou předpisů však v praxi způsobuje potíže.[44] Pro mnoho regulovaných subjektů totiž může být velice náročné správně projít vysoce formalizovaným procesem zadání veřejné zakázky, a stejně tak pro mnoho veřejných zadavatelů může být provedení analýzy a hodnocení rizik v oblasti kybernetické bezpečnosti, včetně následného řízení poddodavatelů v souvislosti se ZKB a VKB, velice obtížné. Ve veřejné správě, která dlouhodobě trpí nedostatkem odborného personálu z oblasti ICT,[45] a nedostatečnou úrovní specializace a motivace svých ICT pracovníků,[46] se tyto dva problémy nesčítají, jako spíše násobí. Není proto překvapující, že regulovaný subjekt v pozici veřejného zadavatele (dále jen „***zadavatel***“) s varováním, které klade vysoké nároky na samostatné a odborné plnění povinností dle ZKB a VKB, může mít potíže. Bolestivý je v tomto kontextu fakt, že při zadávání veřejné zakázky může být i drobné procesní zaváhání pro osud veřejné zakázky fatální.

---

[42] SASKOVÁ, Vladěna, *Novela vyhlášky o VIS, varování NÚKIB a zadávání veřejných zakázek*. Národní úřad pro kybernetickou a informační bezpečnost [online] 3. 12. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.cimib.cz/novinka/125-pozvanka-na-konferenci-kbs-2019

[43] KOTZIAN, Robert, Veřejné zakázky a kybernetická bezpečnost. *epravo.*cz [online] 28. 1. 2020 [vid. 18. 1. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/verejne-zakazky-a-kyberneticka-bezpecnost-110558.html.

[44] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, s. 5 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[45] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb* [online]. 17. červen 2014.

[46] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Digitální Česko: Metody řízení ICT veřejné správy ČR* [online]. 19. červen 2020.

6. ZOHLEDNĚNÍ VAROVÁNÍ PŘI ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK

Jak již bylo obecně nastíněno výše, každý zadavatel veřejné zakázky musí v zadávacím řízení postupovat v souladu se zásadami zadávání veřejných zakázek dle § 6 ZZVZ, tedy transparentně, přiměřeně a nediskriminačně a podle § 36 odst. 1 ZZVZ nesmí nastavit zadávací podmínky tak, aby vytvářely bezdůvodné překážky hospodářské soutěže.[47] Současně ale § 4 odst. 4 ZKB uvádí, že „O*rgány a osoby uvedené v § 3 písm. c) až f)*[48] *jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.*“ Ačkoliv by požadavky stanovené na základě povinnosti vyplývající z jiného právního předpisu měly být důvodné již ze své podstaty,[49] tak věta druhá výše uvedené citace znatelně usnadňuje unesení důkazního břemene zadavatele při přijímání soutěž omezujících bezpečnostních opatření. Zavádí totiž povinnou presumpci[50] souladu bezpečnostních opatření, které zadavatel jako povinná osoba přijme na základě požadavků ZKB, s požadavky § 36 odst. 1 ZZVZ.[51] Jinými slovy je tedy vyjádřeno, že přijetí přiměřených bezpečnostních opatření není nezákonným omezením hospodářské soutěže. Podmínkou pro uplatnění presumpce v § 4 odst. 4 ZKB je však přiměřenost

[47] Jedná se pouze o demonstrativní, a nikoliv úplný výčet zásad zadávání veřejných zakázek.

[48] Jedná se o správce a provozovatele informačních systémů KII, správce a provozovatele VIS a správce a provozovatele informačních systémů základní služby.

[49] Srov. “*Nemůže-li tak zadavatel dodržet svou zákonnou povinnost při zadávání veřejné zakázky v oblasti kybernetické bezpečnosti jinak, než přijetím sporného opatření, nejedná se o nedovolenou diskriminaci“* Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 63. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[50] Presumpce v následujícím znění: „*Zohlednění požadavků vyplývajících z bezpečnostních opatření … v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže“* je spíše zákonným příkazem či povinností, která se pohybuje na pomezí právní fikce a nevyvratitelné právní domněnky, přičemž plně nenaplňuje parametry ani jedné z nich.

těchto bezpečnostních opatření, které zadavatel posuzuje a dokládá zpracovaným hodnocením rizik.

Zadavatel tedy může na základě provedeného hodnocení rizik požadovat splnění určitých kritérií omezujících některé dodavatele nebo jimi nabízené zboží, pokud budou tato kritéria odůvodněná bezpečnostní potřebou přiměřeně dané situaci. Zadavatel tudíž musí bezpečnostní opatření volit racionálně a přezkoumatelně, aby byl schopný unést důkazní břemeno důvodnosti omezení hospodářské soutěže. Nelze totiž svévolně omezovat hospodářskou soutěž pod záštitou bezpečnostních zájmů. Omezení, ke kterým povinná osoba v konkrétním případě přistoupí, nesmí být excesivní a nepřiměřená vzhledem k hrozícímu riziku, nýbrž přiměřená a vždy obhajitelná. To potvrzuje i Úřad pro ochranu hospodářské soutěže (dále jen „***ÚOHS***“), který je dle § 248 ZZVZ dozorovým orgánem v oblasti zadávání veřejných zakázek, a je tedy oprávněn k rozhodnutí, zda byl postup zadavatele souladný s pravidly obsaženými v ZZVZ. ÚOHS potvrdil, že lze hospodářskou soutěž oprávněně omezit bezpečnostními opatřeními, které reagují na varování a vycházejí ze zpracovaného hodnocení rizik ve svém rozhodnutí S0262/2019/VZ ze dne 6. 11. 2019, když zamítl návrh společnosti Huawei Technologies (Czech) s.r.o. na zrušení veřejné zakázky, ve které zadavatel stanovil podmínku dodat další (zdvojující) kusy hardware navíc v případě dodání programových prostředků výrobců uvedených ve varování NÚKIB ze 17. 12. 2018, čímž de facto použití hardware společnosti Huawei Technologies s.r.o. vyloučil. ÚOHS však postup zadavatele označil za správný, když ve svém zamítavém rozhodnutí uvedl, že: „*Ke spornému opatření tak zadavatel nepřistoupil svévolně, nýbrž reagoval na varování NÚKIB, a to po řádně provedeném procesu hodnocení rizik.*“

Hodnocení rizik je tedy zásadní pro určení, zda se jedná o nezákonné omezení hospodářské soutěže či nikoliv. Presumpce souladnosti bezpečnostních opatření omezujících hospodářskou soutěž totiž závisí na posouzení, zda byla bezpečnostní opatření nezbytná pro splnění povinností ZKB. Na-

[51] Obdobně pak § 4 odst. 7 ZKB stanoví presumpci souladnosti bezpečnostních opatření sjednaných ve smlouvě s poskytovatelem cloud computingu s podmínkami hospodářské soutěže, pod podmínkou jejich „nezbytnosti pro splnění povinností“ dle ZZVZ.

plnění podmínek ZKB je oprávněn posoudit NÚKIB. Obdobně má ÚOHS pravomoc přezkoumat podmínky ZZVZ, ale není jeho specializací posuzovat, zda byla bezpečnostní opatření přijata v míře nezbytné pro splnění povinností ZKB.[52]

ÚOHS tedy může buď aplikovat presumpci souladnosti zavedených bezpečnostních opatření (a tudíž konstatovat souladnost), nebo požádat o posouzení nezbytnosti uvedených bezpečnostních opatření NÚKIB. V případě, že však NÚKIB rozhodne, že zavedená bezpečnostní opatření nebyla nezbytná, neznamená to nutně, že povinná osoba porušila pravidla hospodářské soutěže. Pakliže tedy povinná osoba přijme bezpečnostní opatření nad rámec požadavků ZKB (a zajistí vzhledem k situaci nadstandardní bezpečnostní opatření), musí si sám toto rozhodnutí odůvodnit a obhájit. Zavedení vyšších bezpečnostních opatření, než vyžaduje ZKB tedy nezbytně nemusí být porušením hospodářské soutěže, pokud je zadavatel schopný své rozhodnutí zdůvodnit v hodnocení rizik. Jak vyplývá z rozhodovací praxe, tak obsah hodnocení rizik je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele, které v souhrnu tvoří proces řízení rizik.[53]

Implementace varování bude vždy pro zadavatele znamenat postupnou identifikaci hrozeb, následnou identifikaci rizik, analýzu rizik a jejich vyhodnocení. Možnosti, které má zadavatel k dispozici, se ale budou lišit v závislosti na procesu zadávání veřejných zakázek, a to jak fází, ve které se zadávání veřejné zakázky nachází v okamžiku, kdy je vydáno varování, tak také druhem zadávacího řízení nebo jiného postupu zadavatele dle ZZVZ (např. zadávání veřejné zakázky malého rozsahu). Z důvodu odlišných možností zadavatele v různých fázích zadávacího řízení je nutné rozlišovat tyto čtyři časové fáze:

1.1.1 Fáze přípravy veřejné zakázky;

[52] *„Z hlediska posouzení, zda zadavatel stanovil spornou podmínku v souladu se zákonem, je rozhodné stanovisko NÚKIB, ze kterého bude vyplývat, zda zadavatel spornou podmínku stanovil v souladu s příslušnými ustanoveními ZKB a VKB či nikoliv*.“ Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 102. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

[53] Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Bod 61. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html.

2.1.1 Fáze po zahájení zadávacího řízení a před uplynutím lhůty k podání žádosti o účast, předběžných nabídek či nabídek;

3.1.1 Fáze po zahájení zadávacího řízení a po uplynutí lhůty k podání žádosti o účast, předběžných nabídek či nabídek;

4.1.1 Fáze po zadání veřejné zakázky.[54]

Pokud se zadávání veřejné zakázky nachází na svém samotném začátku, a tudíž se teprve připravuje zadávací dokumentace či výběrové podmínky včetně smluvních podmínek (dále jen „***zadávací dokumentace***“), pak má zadavatel možnost do obsahové stránky dokumentace zasahovat a přizpůsobovat ji relativně volně. Je-li tedy vydáno varování ve fázi přípravy veřejné zakázky, musí zadavatel v souladu s § 8 odst. 1 písm. E) VKB zejména řídit rizika spojená s potenciálními dodavateli. Jak bylo vysvětleno výše, tak zadavatel nemůže bez dalšího vyloučit např. určité technické prostředky, ale musí nejprve objektivně posoudit dopad varování na jeho situaci a na předmět veřejnou zakázkou poptávaného plnění, než přijme případná bezpečnostní opatření. To zahrnuje zejména provedení hodnocení rizik podle § 5 VKB, a následné zapracování jejích závěrů do zadávací dokumentace.[55] Způsob zapracování takto dovozených požadavků je pak zcela na vůli zadavatele. Lze zvolit různé varianty zohlednění od stanovení nepřekročitelných technických podmínek, použití jako hodnotícího kritéria, stanovení požadavku na dodání redundantních zařízení, výslovného zakázání rizikových produktů, zavedení technických opatření eliminujících zranitelnosti, nebo také rozdělení zakázky na části, a stanovení rozdílných pod-

[54] Srov. SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2020]. Dostupné z: https://www.mvcr.cz/soubor/5-saskova-vladena-varovani-pred-kybernetickou-hrozbou-podle-12-zkb.aspx.

[55] Hodnocení rizik nebo analýzu s hodnocením rizik spojenou, není zadavatel povinen uveřejnit jako součást zadávací dokumentace nebo ji poskytnout dodavatelům jiným způsobem v rámci zadávacího řízení nebo výběrového řízení (současně dle ZKB zadavatel není povinen dokument poskytnout ani dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím ve znění pozdějších předpisů). Zadavatel by pouze měl v případě, že na základě hodnocení rizik stanoví zadávací podmínky omezující např. využití výrobků od určitých dodavatelů, tento svůj postup odůvodnit (detailnost odůvodnění bude odpovídat rozsahu informací, které je zadavatel oprávněn dodavatelům sdělit při současném zachování pravidel kybernetické bezpečnosti - tedy neposkytne hodnocení rizik, ale přiměřeně odůvodní své kroky v dané věci).

mínek pro každou z jejích částí.[56] Při výběru způsobu zohlednění je vhodné upřednostnit nasazení dostupných technických opatření, pokud je to fakticky i finančně možné, a dle hodnocení rizik dostatečné. V opačném případě lze ze zbývajících způsobů doporučit volit spíše méně omezující způsoby, jako např. volbu redundance před výslovným zákazem určitých produktů. Jako do jisté míry jistější řešení se jeví upřednostnit kvalifikaci před hodnotícími kritérii, jelikož ačkoliv vždy záleží na způsobu nastavení hodnotících kritérií, je volba kvalifikace pro zadavatele jistějším způsobem. Při řešení prostřednictvím hodnotících kritérií totiž může nastat situace, kdy rizikové produkty v hodnocení zvítězí díky např. nižší ceně či jiným posuzovaným hodnotícím kritériím, které ve výsledku hodnocení bezpečnosti převáží, což by dostalo zadavatele do svízelné situace.

V případě, že zadávací řízení nebo výběrové řízení[57] bylo již zahájeno, ale ještě neuplynula lhůta k podání žádosti o účast, předběžné nabídky či nabídky, pak lze po řádném provedení analýzy rizik včetně hodnocení rizik v souladu s § 99 ZZVZ (nebo interními předpisy zadavatele, v případě veřejných zakázek malého rozsahu), změnit či doplnit zadávací podmínky obsažené v zadávací dokumentaci.[58] V takovém případě ale zadavatel bude povinen na povinnost změnu či doplnění uveřejnit nebo oznámit dodavatelům stejným způsobem jako původní zadávací podmínky do kterých bylo zasaženo, a také přiměřeně prodloužit lhůtu pro podání žádosti o účast, předběžné nabídky či nabídky.

Po uplynutí lhůty pro podání žádostí o účast, předběžných nabídek či nabídek již nelze zadávací podmínky měnit. Nabízí se tedy možnost pokračovat v zadávacím či výběrovém řízení, a přijmout pouze dílčí bezpečnostní opatření, nebo pozměnit způsob či účel k jakému bude předmět plnění pou-

[56] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, s. 6-7 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[57] Ačkoliv se nejedná o zákonný pojem, je výběrové řízení pojmem užívaným v praxi zadávání veřejných zakázek pro veřejné zakázky malého rozsahu.

[58] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, s. 14 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

žíván, pokud je to v dané situaci možné. Jakoukoliv modifikací však nesmí být dotčen postup v zadávacím řízení nebo výběrovém řízení. Alternativně je možné pokusit se dodavatele vyloučit dle některého z důvodů uvedených v § 48 ZZVZ, pokud k tomu budou splněny příslušné podmínky. V případě, že dle hodnocení rizik nelze učinit žádnou z výše uvedených možností, nezbývá než zadávací řízení zrušit podle § 127 odst. 2 písm. d) ZZVZ (výběrové řízení by se rušilo dle interních pravidel zadavatele). Varování je v tomto kontextu možné považovat za důvod hodný zvláštního zřetele, pro který nelze po zadavateli požadovat, aby v řízení pokračoval, pokud by soutěžené plnění neodpovídalo novým kyberbezpečnostním požadavkům.[59] Rozhodnutí, kterou z možností zadavatel zvolí, by se však mělo vždy odvíjet od řádně provedeného hodnocení rizik.

Jestliže již došlo k zadání veřejné zakázky vybranému dodavateli, pak je v první řadě nezbytné, aby zadavatel provedl hodnocení rizik dle výše uvedeného. Na základě výsledků je pak zadavatel povinen rozhodnout, zda je identifikované riziko akceptovatelné, a postačí zavést bezpečnostní opatření ke snížení rizik, aniž by došlo k podstatné změně závazku ze smlouvy dle § 222 ZZVZ.[60] V opačném případě, pokud zadavatel usoudí, že nestačí přijmout bezpečnostní opatření ke snížení rizika nebo tento postup nebude souladný se ZZVZ, je nutné smlouvu na veřejnou zakázku vypovědět nebo od ní odstoupit.[61] Výše uvedené nebrání zadavateli rozhodnout se ukončit smlouvu podle obecné právní úpravy v OZ, jiných právních předpisů či vlastních specifických ujednání ve smlouvě s dodavatelem. Pokud ale není specificky sjednána možnost smlouvu vypovědět nebo od smlouvy odstoupit a současně v jejím plnění nelze pokračovat z důvodu vydání varování, pak lze v souladu s § 223 odst. 1 ZZVZ závazek ukončit výpovědí či odstoupením na základě tohoto ustanovení.

---

[59] Ibidem, s. 14.

[60] Kritérium podstatné změny je však nezbytné posuzovat vždy ad hoc s ohledem na povahu původního závazku.

[61] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, s. 15 [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

7. ZÁVĚR

Jednoznačnou výhodou české právní úpravy kybernetické bezpečnosti je, že disponuje širší paletou právních institutů, než má většina ostatních států EU, což umožňuje lépe reagovat na rizika rozličné intenzity. Používání podobných označení u různých pojmů však může mít za následek nepřehlednost a vyšší pravděpodobnost jejich záměny. Článek se proto nejprve zabývá obecně opatřeními dle čl. 11 ZKB, vysvětluje terminologii pojmů pracujících s označením „opatření“, a navrhuje přijetí označení „protiopatření“ pro opatření dle čl. 11 ZKB. Smyslem přijetí této přezdívky, která je již částečně používána v akademické sféře[62] je přitom zvýšení přehlednosti a dosažení jasné terminologie ZKB.

Jedním z právních institutů, který není převzat ze směrnice NIS, ale který byl do českého právního řádu přijat na základě vlastní legislativní iniciativy je varování dle § 12 ZKB, které přináší efektivní právní řešení pro hrozby v oblasti kybernetické bezpečnosti, pro něž nestačí obecná prevenční povinnost, ale vrchnostenský zásah do autonomie vůle regulovaných osob, stanovující práva a povinnosti, by byl již nepřiměřeně invazivní. Varování samo o sobě nestanoví regulovaným subjektům žádné přímé povinnosti, ale jeho význam spočívá v oficiálním předání informací o hrozbě. Komplex práv a povinností vyplývající ze ZKB a VKB pak povinné subjekty povinuje zohlednit hrozbu v pravidelně prováděném hodnocení rizik, a pokud zjistí takovou potřebu, pak přijmout nezbytná bezpečnostní opatření k její eliminaci. Za samotné ignorování varování a nezavedení adekvátních bezpečnostních opatřeních v reakci na hrozbu regulovaným subjektům nehrozí přímá sankce. Pokuta však hrozí povinným subjektům dle § 25 odst. 3 až 8 písm. b) ZKB, pokud nezohlední požadavky vyplývající z bezpečnostních opatření (které přijaly na základě varování) při výběru dodavatele. Další rizikem pak je potenciální povinnost hradit škody, vzniklé v důsledku vlastní nečinnosti povinného subjektu a případného omisivního jednání.

[62] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, s. 30.; Shodně též ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti*. Brno. 18. 4. 2021.

V poslední části článku je pojednáno o vztahu ZKB a ZZVZ, jakožto dvou právních předpisů stejné právní síly, ale diametrálně odlišného charakteru. Zatímco ZKB usiluje o zvýšení kybernetické bezpečnosti, čehož dosahuje pomocí performativních pravidel, ZZVZ reprezentuje zájem na rovné a nediskriminační hospodářské soutěži prostřednictvím vysoce formalizovaných administrativních pravidel. Ačkoliv mají oba právní předpisy stejnou právní sílu, skloubit jejich požadavky činí často problém zejména ve veřejném sektoru, který trpí nedostatkem kvalifikovaného personálu, schopného obsáhnout obě tato specifická právní odvětví. Za tímto účelem je proto pojednáno o správném způsobu zohlednění varování v případě, že je veřejný zadavatel dle ZZVZ současně regulovaným subjektem dle ZKB. Vzhledem k tomu, že počet regulovaných subjektů má mezi lety 2020 až 2025 vzrůst téměř trojnásobně, lze předpokládat, že se bude jednat o čím dál častější jev. Nakonec jsou v souladu s podpůrnými materiály NÚKIB předestřeny také možnosti veřejných zadavatelů, jak varování zohlednit v různých fázích zadávacího řízení.

8. SEZNAM POUŽITÝCH ZDROJŮ:

[1]DVOŘÁK, David; MACHUREK, Tomáš; NOVOTNÝ, Petr; a kol. § 1 [Předmět úpravy]. In: DVOŘÁK, David, MACHUREK, Tomáš, NOVOTNÝ, Petr, a kol. *Zákon o zadávání veřejných zakázek.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, 1320 s. ISBN 978-80-7400-651-7.

[2]HEJČ, David. Reaktivní a ochranná opatření (obecné povahy) před kybernetickým bezpečnostním incidentem. In: *Cofola 2015: The Conference Proceedings*. 2015. vyd. Brno: Masarykova univerzita, s. 721–730. ISBN 978-80-210-7976-2.

[3]KAHN, Jan; LOPATKA, Michael. Czech cyber watchdog says its Huawei warning took U.S. by surprise. *Reuters* [online]. 2019 [vid. 24. 3. 2021]. Získáno z: https://www.reuters.com/article/us-huawei-europe-czech-idUSKCN1QN1DI

[4]KOTZIAN, Robert. Veřejné zakázky a kybernetická bezpečnost. *epravo.*cz [online] 28. 1. 2020 [vid. 18. 1. 2021]. Dostupné z: https://www.epravo.cz/top/clanky/verejne-zakazky-a-kyberneticka-bezpecnost-110558.html

[5]MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb* [online]. 17. červen 2014. [vid. 28. 3. 2021] Získáno z: https://ipodpora.odbory.info/soubory/dms/wysiwyg_uploads/a05b113e9f39c8af/uploads/Navrh-opatreni-zvysujicich-efektivnost-sluzeb-verejne-spravy-a-podpurnych-ICT-suzeb.pdf

[6]MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Digitální Česko: Metody řízení ICT veřejné správy ČR* [online]. 19. červen 2020.

[vid. 28. 3. 2021]. Získáno z: https://archi.gov.cz/_media/dokumenty:navazujici_dokument_c_1metody_rizeni_ict_vs.pdf

[7]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost* [online]. 2020. [vid. 23. 3. 2021]. Získáno z: https://nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf

[8]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Metodika k varování ze dne 17. prosince 2018*. [online] 4. 1. 2019, 17 s. [vid. 23. 1. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[9]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost*. [online] 30. 7. 2020, 20 s. [vid. 23. 1. 2021].
Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[10]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení*. [online] 4. 1. 2020, 28 s. [vid. 23. 1. 2021]. Dostupné z: https://www.mvcr.cz/soubor/priloha-c-2-podpurny-material-nukib-pdf.aspx

[11]POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*. 2015, roč. 6, č. 11, s. 95. ISSN 1805-2797.

[12]POLČÁK, Radim. Kybernetická bezpečnost. In: POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, 656 s. ISBN 978-80-7598-046-5.

[13]POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti*. 1. Brno: Masarykova univerzita, 2016, 240 s. ISBN 978-80-210-8426-1.

[14]Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 6. 11. 2019, sp. zn. S0262/2019/VZ. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16400.html

[15]Rozhodnutí Úřadu pro ochranu hospodářské soutěže, ze dne 13. 1. 2020, sp. zn. S0358/2019/VZ. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html

[16]SANTORA, Marc; GOEIJ, Hana de. Huawei Was a Czech Favorite. Now? It's a National Security Threat. *The New York Times* [online]. 2019 [vid. 24. 3. 2021]. ISSN 0362-4331. Získáno z: https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html

[17]SASKOVÁ, Vladěna. *Novela vyhlášky o VIS, varování NÚKIB a zadávání veřejných zakázek*. Národní úřad pro kybernetickou a informační bezpečnost [online] 3. 12. 2019 [vid. 1. 4. 2021]. Dostupné z: https://www.cimib.cz/novinka/125-pozvanka-na-konferenci-kbs-2019

[18]SASKOVÁ, Vladěna. *Varování před kybernetickou hrozbou podle § 12 ZKB*. Národní úřad pro kybernetickou a informační bezpečnost [online] 17. 5. 2019 [vid. 1. 4. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[19]ŠVÉDA, Martin. *Školení na činnost OREG a zákon o kybernetické bezpečnosti.* Národní úřad pro kybernetickou a informační bezpečnost [online přednáška]. [vid. 18. 3. 2021] Brno. 2021.

[20]VLÁDA. Důvodová zpráva k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), č. 181/2014 Dz. *Beck-online* [online]. [vid. 25. 3. 2021]. Získáno z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge2f6mjygfpwi6q&groupIndex=0&rowIndex=0
