26. 4. 2019

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Kybernetická bezpečnost ve veřejných zakázkách

Snad nikoho neminuly informace o potřebě zvýšení kybernetické bezpečnosti v IT zakázkách a zejména ve veřejných zakázkách, jejichž předmětem jsou dodávky a služby používající komunikační a informační technologie. Toto téma je podrobněji medializováno zejména v souvislosti s varováním před použitím technických a programových prostředků konkrétních čínských společností (dále jen „varování“), které vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) dne 17. prosince 2018.

Důvody vycházející ze skutečností zjištěných při výkonu působnosti NÚKIB, které vedly k vydání tohoto varování, jsou podrobně a srozumitelně popsány v dokumentu samém. Varování bylo vydáno podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících předpisů (dále jen „ZKB“).

Pojem kybernetická bezpečnost lze stručně shrnout jako soubor právních, organizačních a technických prostředků směřujících k zajištění ochrany kybernetického prostoru, v němž dochází ke vzniku, zpracování a výměně informací tvořených informačními systémy. Klíčovými předpisy upravujícími tuto oblast jsou zejména již jmenovaný ZKB, vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti, dále jen „VKB“), nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury a vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích (dále jen „VVIS“).

Problematika kybernetické bezpečnosti však není novým tématem, zejména ne u konkrétních povinných osob. Odborná veřejnost o nezbytnosti zajištění kybernetické bezpečnosti zejména ve veřejné správě diskutuje již delší dobu. Dosud však zadavatelé byli v zadávacím řízení na veřejné zakázky v IT oblasti omezeni zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), který zakazuje zadavatelům vytvářet při stanovování zadávacích podmínek bezdůvodné překážky hospodářské soutěže. Nově otevírá varování možnost zadavatelům, jak zajistit v zadávacím řízení potřebnou kybernetickou bezpečnost a současně postupovat souladně se ZZVZ a neomezit hospodářskou soutěž.

Již zmíněné varování má zásadní dopad na připravovaná, probíhající a dokonce již i na ukončená zadávací řízení, jejichž předmětem je obměna komunikačních a informačních technologií, protože vyslovuje odůvodněné obavy z existence potenciálních rizik při využívání technických nebo programových prostředků. Tyto prostředky jsou dodávány do informačních a komunikačních systémů, které mají nebo mohou mít strategický význam pro bezpečnost státu. Existují tedy reálné obavy, že může být narušena bezpečnost informací, jejich dostupnost, integrita nebo důvěrnost nebo

že u služeb rovněž existuje možnost odepření jejich poskytování, přičemž míra potenciálního rizika narušení bezpečnosti systémů důležitých pro stát je nezanedbatelná. Hrozbu, na kterou varování upozorňuje, je tedy v souladu s VKB nutno z hlediska hodnocení rizik hodnotit jako velmi pravděpodobnou až více méně jistou.

Vydání varování má zásadní dopad na konkrétní osoby, kterým jsou dle § 3 ZKB uloženy povinnosti v oblasti kybernetické bezpečnosti (dále jen „povinné osoby"). Jde zejména o správce a provozovatele komunikačních nebo informačních systémů kritické informační struktury nebo správce a provozovatele významných informačních systémů. Mezi kritické informační infrastruktury počítáme zejména sítě a služby nezbytné pro obyvatele státu a dělí se podle odvětvových kritérií na několik oblastí zahrnujících energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, dopravu, komunikační a informační systémy, finanční trh a měnu, nouzové služby a veřejnou správu. Významné informační systémy (konkrétně jich je 153) jsou vyjmenovány v Příloze č. 1 VVIS, přičemž jde zejména o konkrétní informační systémy vyšších územně samosprávních celků (krajů), strategických ministerstev, ČNB, ČTÚ, ERÚ a dalších z hlediska kybernetické bezpečnosti významných úřadů a institucí. Z výše uvedeného a dále rovněž z metodiky, kterou v této souvislosti vydal NÚKIB, vyplývá, že varování nemíří na běžné uživatele. Orgánům a osobám, kterým neukládá žádné povinnosti ZKB, ani varování nezakládá žádnou povinnost a je na jejich uvážení, jak případnou hrozbu ve svých obchodních rozhodnutích zohlední.

Osoby povinné dle ZKB tedy mají povinnost zavést bezpečnostní opatření při hodnocení rizik a v plánu zvládání rizik toto varování zohlednit. Rozšíří se tak povinnost vyplývající z § 5 VKB provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit o zjištění vyplývající z varování. Přijatá bezpečnostní opatření musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika. K posouzení míry rizik vydává NÚKIB potřebné metodiky a poskytuje nezbytnou součinnost. V případě, že povinné osoby hrozby zohlední a vyhodnotí je tak, že riziko nepřekračuje stanovenou mez, lze technologie čínských společností využívat i nadále.

Popsaný proces analýzy a řízení rizik je třeba v souladu s § 4 odst. 4 ZKBS zohlednit při případném výběru dodavatele pro informační nebo komunikační systém a tyto požadavky na zajištění kybernetické bezpečnosti zahrnout do smlouvy, kterou s dodavatelem uzavřou. Za dodavatele se pak považují nejen v samotném varování uvedené čínské společnosti, ale i všechny další společnosti, které technické nebo programové prostředky zmiňovaných společností přeprodávají nebo které dodávají technické celky, jejichž součástí jsou prostředky zmiňovaných společností. Je tedy na zadavateli, aby v zadávacích podmínkách zajistil, případně ve smlouvě v potřebném rozsahu upravil, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem týkající se zajištění kybernetické bezpečnosti. Metodika k varování ze dne 17. prosince 2018, kterou vydal NÚKIB dne 4. ledna 2019, zadavatelům popisuje, jak mohou postupovat ve fázi přípravy zadávacích podmínek, ve fázi již probíhajícího zadávacího řízení, příp. ve fázi po skončení zadávacího řízení a po zadání zakázky konkrétnímu dodavateli. Jde však o nezávazné doporučení NÚKIB, které vždy musí být posouzeno i optikou ZZVZ.

K rozhodování o souladnosti postupu zadavatele při výběru dodavatele se ZZVZ je příslušný Úřad pro ochranu hospodářské soutěže, přičemž vždy je třeba posoudit postup dle konkrétních skutkových okolností. S ohledem na vydání varování NÚKIB, které je aktem oprávněné osoby vydaným dle § 22 písm. b) ZKB, je případné omezení hospodářské soutěže, které se promítne do tvorby zadávacích podmínek, omezením odůvodnitelným oprávněnými potřebami zadavatele. Těmito oprávněnými potřebami zadavatele jsou, jak vyplývá z výše uvedeného, jeho zákonné povinnosti zajistit kybernetickou bezpečnost. Hospodářskou soutěž tedy v konkrétních výše uvedených případech lze omezit a nejedná se tím o porušení ZZVZ. Vždy je však potřeba takový postup podložit aktuální

analýzou a vyhodnocením rizik ve smyslu ZKB.

Adéla Šípová

Weinhold Legal, v.o.s. advokátní kancelář

Na Florenci 2116/15
110 00 Praha 1

e-mail: wl@weinholdlegal.com
Tel.: +420 225 385 333

Další články:

- JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - KVĚTEN 2026
- Hodnocení demo prostředí v IT veřejných zakázkách: užitečný nástroj, nebo cesta k netransparentnosti?
- JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - DUBEN 2026
- Prokazování dostupnosti technického vybavení při zadávání veřejných zakázek – limity sdílení technického vybavení
- JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - BŘEZEN 2026
- Zdrojové kódy jako „pojistka“ proti vendor-lock-inu: judikatorní korekce a její meze
- Spolupráce zadavatele a developera z pohledu rozhodovací praxe ÚOHS a plánovacích smluv
- Listinné nabídky v éře elektronizace: přestupek, nebo legitimní postup?
- JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - ÚNOR 2026
- Změna poddodavatele v průběhu zadávacího řízení
- JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - LEDEN 2026