1. 9. 2021

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

Kybernetická bezpečnost: jak a proti komu se efektivně bránit

Stále rostoucí míra digitalizace na všech úrovních naší společnosti vede k výraznému zvýšení počtu kybernetických útoků proti veřejným i soukromým institucím. Zejména instituce ústřední státní správy (jednotlivá ministerstva či úřady s celostátní působností) totiž pro útočníky představují potenciální zdroj zpravodajsky, politicky či ekonomicky významných informací.

Mezi atraktivní cíle kybernetických útoků nicméně stále častěji patří rovněž nedostatečně chráněné územní samosprávné celky, jakož instituce finančního, akademického či zdravotnického sektoru. **Nemusí se však nutně jednat o státní instituce, ale také o subjekty, ve kterých má stát či územní samosprávní celky majetkovou účast** (dopravní podniky, technické služby, letiště, vodárenské společnosti, školy, nemocnice apod.).

Právě do poslední jmenované skupiny lze zařadit například mediálně známý kybernetický útok proti systémům Fakultní nemocnice Brno[1] či obdobný útok na Nemocnici Rudolfa a Stefanie Benešov, v jehož důsledku byla způsobena škoda ve výši více než 59 milionů Kč.[2] V nedávné době pak došlo i ke kybernetickému útoku na Magistrát města Olomouce.[3] **Ochrana kybernetické bezpečnosti je přitom velmi často podceňována také v soukromém sektoru**, což je patrné mj. v zemědělství.[4]

V této souvislosti je třeba připomenout, že kybernetický útok zaměřený například na subjekty, resp. prvky kritické infrastruktury[5], může mít velmi závažné dopady (nejen) na fungování státu. V České republice se celkový počet kybernetických útoků oproti minulému roku více než zdvojnásobil.[6] Lze přitom předpokládat, že množství těchto útoků bude v následujících letech i nadále stoupat. Snaha o předcházení kybernetickým útokům, jakož i o rychlé a efektivní vypořádání se s jejich negativními následky, proto klade **stále vyšší důraz na zajištění kybernetické bezpečnosti**.

Základem tuzemské právní úpravy kybernetické bezpečnosti je **zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů** (dále jen „ZKB“) a jeho prováděcí předpisy[7]. Předmětem ZKB je především zajištění kybernetické bezpečnosti, když za tímto účelem jsou povinným subjektům[8] uloženy povinnosti, jejichž dodržování představuje základní preventivní opatření, které by mělo kybernetickým útokům zabránit (či alespoň v maximální možné míře předcházet). Dozor nad plnění povinností stanovených ZKB vykonává **Národní úřad pro kybernetickou a informační bezpečnost** (dále jen „NÚKIB“).

Jako problematický se však v současné době jeví příliš úzký okruh povinných subjektů, na které ZKB a jeho prováděcí předpisy dopadají. Povinnosti k zajištění kybernetické bezpečnosti jsou totiž uloženy pouze subjektům, které zákonodárce považoval za nejvýznamnější, neboť přímo souvisí se zajištěním bezpečnosti státu a jeho funkcí. Tento postup je však z praktického hlediska přinejmenším diskutabilní, neboť povinné subjekty dle ZKB již dříve splňovaly určitý stupeň kybernetické bezpečnosti (byť nikoliv na stejné úrovni). Sjednocení požadavků kladených na povinné subjekty, jejich postupné zpřísňování a současně postupné rozšiřování okruhu povinných subjektů pak vede k tomu, že se kybernetické útoky stále více zaměřují na subjekty, které se kybernetickou bezpečností dosud vůbec nezabývaly (např. menší nemocnice či školy).

Cílem kybernetického útoku se nicméně může stát prakticky kterýkoliv subjekt, přičemž čím méně je subjekt chráněný, tím více se pravděpodobnost kybernetického útoku zvyšuje. **Nemusí se přitom jednat pouze o subjekty významné z celorepublikového hlediska.** Jak ukázal kybernetický útok na Nemocnici Rudolfa a Stefanie Benešov, cílem mohou být (a s největší pravděpodobností také budou) často velmi nedostatečně chráněné subjekty regionálního významu. Sofistikovaný a soustředěný kybernetický útok zaměřený na konkrétní druh regionální veřejné infrastruktury (např. školy), na jehož základě budou napadené subjekty dočasně paralyzovány, přitom může mít v konečném důsledku i mnohem závažnější následky než útok na instituce ústřední státní správy s celostátní působností (zejm. dopady na vzdělávání, náladu ve společnosti či sekundární ekonomické dopady na rozpočty menších obcí, které jsou zřizovatelem škol apod.).

Výše uvedené případy potvrzují, že hrozby kybernetického útoku by neměly brát na lehkou váhu ani subjekty, na které povinnosti stanovené ZKB a jeho prováděcími předpisy nedopadají. **Je proto na místě doporučit, aby i tyto subjekty dobrovolně implementovaly v rámci svých vnitřních řídících kontrolních systémů nezbytná preventivní bezpečnostní opatření k zajištění co nejvyšší úrovně ochrany pořizovaných, uchovávaných, vytvářených či zpracovávaných informací a následně důsledně dbali na jejich dodržování a pravidelnou aktualizaci**. Při volbě konkrétních bezpečnostních opatření mohou tyto „nepovinné“ subjekty analogicky využít opatření stanovená právními předpisy[9], jejichž rozsah lze s přihlédnutím k předmětu činnosti rozšířit či v odůvodněných případech naopak zúžit.

Milan Kučera,
vedoucí advokát

Petr Šilhán,
advokátní koncipient

CÍSAŘ ČEŠKA SMUTNÝ

CÍSAŘ, ČEŠKA, SMUTNÝ s.r.o., advokátní kancelář

CITY TOWER
Hvězdova 1716/2b
140 00 Praha 4

Tel.: +420 224 827 884
Fax: +420 224 827 879
e-mail: ak@akccs.cz

---

[1] ČTK. Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve. iDnes.cz [online]. MAFRA, a. s., © 1999-2021, pub. 17. dubna 2020 [cit. 17. srpna 2021]. Dostupné >>> zde.

[2] ČTK. Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat

nepodařilo. iRozhlas.cz [online]. Český rozhlas, © 1997-2020, pub. 18. srpna 2020 [cit. 17. srpna 2021]. Dostupné >>> zde.

[3] KAMENSKÝ, Stanislav. Olomoucký magistrát paralyzoval útok hackerů, město podá trestní oznámení. iDnes.cz [online]. MAFRA, a. s., © 1999-2021, pub. 7. dubna 2021 [cit. 17. srpna 2021]. Dostupné >>> zde.

[4] MIKEŠOVÁ, Markéta. Zemědělci zanedbávají kybernetickou bezpečnost. Záškodník by jim mohl zničit úrodu přes zavlažovací systémy. VTM.cz [online]. CZECH NEWS CENTER, a.s., © 2021, pub. 30. října 2020 [cit. 17. srpna 2021]. Dostupné >>>zde.

[5] Podle ust. § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, je kritická infrastruktura definována jako „prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“. Mezi typické prvky kritické infrastruktury patří například elektrárny, přehrady, letiště, telekomunikační sítě či strategické finanční instituce nebo státní úřady. Vyřazení některého z těchto prvků může ochromit poskytování kritických služeb (elektřina, teplo, voda) nebo v krajním případě způsobit i významné škody.

[6] ČTK. Obří kybernetický útok zasáhl stovky firem. Hackeři žádají 70 milionů dolarů. Deník.cz [online]. VLTAVA LABE MEDIA a.s., © 2021, pub. 5. července 2021 [cit. 17. srpna 2021]. Dostupné >>> zde.

[7] Vyhláška Národního bezpečnostního úřadu a Ministerstva vnitra č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, vyhláška Národního úřadu pro kybernetickou bezpečnost č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ve znění pozdějších předpisů a vyhláška Národního úřadu pro kybernetickou bezpečnost č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhlášky o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „Vyhláška o KB“).

[8] Tj. správcům a provozovatelům informačních a komunikačních systémů kritické infrastruktury či významných informačních systémů a sítí, příp. poskytovatelům služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací apod. (srovnej ust. § 3 ZKB).

Později mezi povinné osoby přibyli i provozovatelé základní služby, správci a provozovatelé informačních systémů základních služeb a poskytovatelé digitálních služeb. Blíže viz >>> zde.

[9] Srovnej ust. § 5 ZKB ve spojení s ust. § 3 a násl. Vyhlášky o KB.

Další články:

- Nefungující rozsah péče o dítě. Cesta přes využití terapie a dalších opatření podle ustanovení § 503 zákona o zvláštních řízeních soudních
- De iure traktor, de facto nákladní vozidlo, už ne tolik výhodná dualita
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- Pokuta 32 mil. EUR pro Dacia/Renault – evropské soutěžní úřady tvrdě došlapují na no-poaching. Měla by Vaše společnost být na pozoru?
- Rozdělení společného jmění manželů v případech výdělečné činnosti pouze jednoho z manželů
- Oběť znásilnění má nárok na peněžitou satisfakci
- Digitalizace AML povinností: jak technologie mění plnění povinností pro tisíce povinných osob
- (Ne)vypořádání předmětu řízení u soudního smíru
- Nové limity opatrovnického rozhodování v judikatuře ESLP a Ústavního soudu
- Mimosmluvní odměna při společném zastupování více osob
- Nepřiznané koalice