26. 3. 2021

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

Kybernetická bezpečnost a péče řádného hospodáře

Kybernetická bezpečnost může statutárním orgánům znít jako cosi vzdáleného. Problém skrývající se za dveřmi firemního IT oddělení. Opak je však pravdou.

Proč je otázka kybernetické bezpečnosti relevantní

Kybernetických incidentů bohužel stále přibývá. Jako příklad lze uvést nedávné incidenty spojené se společnostmi SolarWinds, Zyxel nebo Microsoft. V případě incidentu týkajícího se zranitelnosti služby Microsoft Exchange bylo na základě programátorské chyby možné bez autentizace vniknout do emailové pošty a zneužít její obsah. Zranitelnost, před kterou vydal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) 3. března upozornění, bohužel doprovázela řada kybernetických útoků. Mimo útoky např. na Magistrát hlavního města Prahy a Ministerstvo práce a sociálních věcí bylo významně zasaženo i bankovnictví, školství či zdravotnictví, které je v posledních měsících pod permanentním tlakem ze strany hackerů.

Jako odstrašující případ nebezpečných kybernetických útoků lze pak uvést nedávné útoky na nemocnice. V roce 2020 nahlásilo NÚKIB bezpečnostní incidenty šestnáct největších tuzemských nemocnic. Lze připomenout i nechvalně nejznámější útok na nemocnici Rudolfa a Stefanie Benešov z konce roku 2019. Ten způsobil vyřazení nemocnice z provozu na téměř 20 dní a škodu dosahující téměř 60 milionů Kč.

Proč by se otázkou kybernetické bezpečnosti měla zabývat každá právnická osoba?

Kybernetický bezpečnostní incident může způsobit rozsáhlé majetkové škody. V závažnějších případech může zcela paralyzovat činnost daného subjektu. Škodu potom představují nejen náklady na obnovu původního stavu, ale i ušlý zisk, který nebylo možné v době řešení incidentu realizovat. Ještě významnější pak může být reputační újma společnosti v očích svých klientů.

Poškození klienti navíc mohou uplatnit nárok na náhradu škody. Povinnost nahradit škodu (vzniklou porušením smluvní povinnosti) není podmíněna zaviněním.[1] Povinná osoba zároveň může těžko očekávat, že jí škodu nahradí např. zaměstnanec, který ji byť pouhou nedbalostí způsobil. Tuto možnost značně limituje nejen zákoník práce, ale i majetkové poměry běžného zaměstnance.

Zásadní hrozbou jsou i veřejnoprávní sankce. Trestní zákoník zakotvuje celou řadu trestných činů spojených s kybernetickou bezpečností. Některé přitom mohou být spáchány pouhou nedbalostí. Trestní rovinou však nejsou veřejnoprávní sankce vyčerpány. Nezajistí-li osoba např. dostatečně zabezpečení osobních údajů, přichází v úvahu správní postih.

Celou lavinu událostí přitom může spustit i jediné kliknutí myší. Třeba asistentky v kanceláři, která si otevřela přílohu e-mailu. Stačí, když tímto kliknutím spustí ransomware paralyzující činnost svého zaměstnavatele, nebo malware, který z databází dané společnosti (nebo třeba nemocnice) „vytěží“ veškeré osobní údaje, které najde. Takové nebezpečí je nyní navíc ještě mnohem reálnější než dříve. Asistentka totiž může pracovat z vlastního počítače v rámci home office. Jeho omezené zabezpečení v kombinaci s dálkovým přístupem a absencí alespoň základního školení dané pracovnice může

působit jako výbušný koktejl.

Proč by měl kybernetickou bezpečnost řešit její statutární orgán?

Zákon o kybernetické bezpečnosti uvádí výčet orgánů a osob, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti. Mnoho dalších subjektů však jeho působnost nepokrývá. Otázka kybernetické bezpečnosti však rozsahem zákona není omezena.

Člen statutárního (resp. každého voleného[2]) orgánu je zejména zatížen povinností péče řádného hospodáře. Statutární orgán může pověřit výkonem činností, spadajících do jeho působnosti, třetí osobu. Zpravidla tehdy, jestliže nemá znalosti, dovednosti či schopnosti potřebné pro výkon některých z činností svěřených do jeho působnosti (např. rozhodování záležitostí vyžadujících odbornost).[3]

Takto musí zajistit i ochranu před kybernetickými hrozbami. Zpravidla tak učiní pověřením profesionála znalého problematiky kybernetické bezpečnosti. Chybou mnohých společností však bývá, že v tomto smyslu zaměstnají pouze „ajťáka“ a mají za hotovo.

Co by měl statutární orgán konkrétně zajistit?

Co by tedy měla právnická osoba, resp. její statutární orgán, provést prakticky? Mimo mnohá technická opatření zajišťující ochranu dat a jejich bezpečnost v informačních systémech je dobrým krokem zejména vzdělávaní zaměstnanců. Nejčastější bezpečnostní incidenty jsou totiž založeny na lidské chybě, a to se nejspíše nezmění. Společnost by také měla mít vypracovanou komplexní dokumentaci (interních předpisů, metodik, smluv), která bude jasným návodem pro kontinuální zajišťování kybernetické bezpečnosti. Vypracovaná dokumentace následně také slouží za účelem monitoringu dodržování bezpečnostních pravidel a je efektivním nástrojem pro interní a externí audit.

V souvislosti s detailním nastavením interního programu může být praktickou pomůckou např. i „Minimální bezpečnostní standard“, který zpracoval NÚKIB.[4] Dokument je koncipován jako podpůrný materiál (členěný na manažerskou a technickou část) pro subjekty, které nespadají pod zákon o kybernetické bezpečnost. NÚKIB vydává i řadu dalších doporučení a podpůrných materiálů, jejichž nastudování lze doporučit.

Robustní bezpečnostní program může být rozhodujícím prvkem při zamezení zásadních škod, které mohou podceněním kybernetické bezpečnosti vzniknout. Zároveň může představovat zásadní argument ve správním či trestním řízením vedeném proti osobě, u které ke kybernetickému bezpečnostnímu incidentu došlo. Pro člena statutárního orgánu může v dnešní době zajistit podstatně klidnější spaní. Ze všech výše popsaných důvodů je tak popsaný program klíčovým nástrojem, který by neměl být za žádných okolností opomíjen.

Mgr. Petr Motyčka,
advokát

založeno 1990
TOMAN & PARTNEŘI
ADVOKÁTNÍ KANCELÁŘ
www.iustitia.cz
PARTNER PRO VÁŠ PRACOVNÍ I OSOBNÍ ŽIVOT

TOMAN & PARTNEŘI advokátní kancelář, s.r.o.

Trojanova 12
120 00 Praha 2

Tel.: +420 224 918 490
Fax: +420 224 920 468
e-mail: ak@iustitia.cz

---

[1] Smluvní strana se v takovém případě může povinnosti k náhradě zprostit pouze výjimečně pomocí liberačních důvodů.

[2] Dle § 152 odst. 2 občanského zákoníku je členem voleného orgánu fyzická osoba, která je členem orgánu právnické osoby a která je do funkce volena, jmenována či jinak povolána.

[3] Např. rozsudek Nejvyššího soudu ze dne 11. 9. 2019, sp. zn. 31 Cdo 1993/2019

[4] K dispozici >>> zde.

Další články:

- Nová „tlačítková" povinnost pro e-shopy
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Darování pro případ smrti nemovité věci zapsané v katastru nemovitostí a určení výše odměny soudního komisaře
- Flotilová novela: Kdo a kdy musí nově získat licenci k distribuci pojištění?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu