9. 4. 2021

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

Kybernetická bezpečnost ve zdravotnictví

Zdravotnická zařízení si díky pandemii koronaviru procházejí těžkou dobou. Kromě povinností vyplývajících z jejich činnosti se bohužel tato zařízení musí vypořádávat i s dalšími výzvami, a to zejména ve smyslu stále narůstajících kybernetických hrozeb. Ty, jak nedávné incidenty ukazují, mohou ohrozit i jejich samotný provoz.

V roce 2020 nahlásilo Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen NÚKIB) kybernetické incidenty šestnáct největších tuzemských nemocnic. NÚKIB v této věci 16. 4. 2020 vydal varování před *„hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení.*“

V lednu 2021 renomovaná bezpečnostní firma Check Point uvedla[1], že kyberútoky na zdravotnictví stouply o 45 %. Pavel Krejčí, bezpečnostní expert společnosti Check Point tyto útoky trefně nazval hyenismem a *„parazitování na současné situaci, kdy si nemocnice pod náporem pacientů s koronavirem a vzhledem ke spuštění vakcinačních programů nemohou dovolit jakékoli výpadky a přerušení provozu*.“[2]

Jako příklad škod, které může kyberútok napáchat lze připomenout nechvalně známý útok na nemocnici Rudolfa a Stefanie Benešov z konce roku 2019. Ten mimo jiné způsobil vyřazení nemocnice z provozu na téměř 20 dní a škodu dosahující skoro 60 milionů Kč.

Nemocnice ve většině případech podlehnou tzv. ransomware, škodlivému programu, který zablokuje určitý počítačový systém nebo zašifruje data v něm zapsaná, a pak požaduje od oběti výkupné za obnovení přístupu. Některé formy ransomware šifrují soubory na pevném disku, jiné „jen“ uzamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení. Takové útoky nejčastěji cílí na úřady, nemocnice, obchodní společnosti a instituce, které uchovávají důležitá data a je zde větší pravděpodobnost, že pachatel od napadeného subjektu získá finanční prostředky.

Podcenila se kybernetická bezpečnost ve zdravotnictví?

Povinnosti pro nemocnice na úseku kybernetické bezpečnosti stanovuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a příslušných vyhlášek. Vybraná zdravotnická zařízení jsou povinnou osobou podle § 3 písm. f) a g) zákona o kybernetické bezpečnosti, jakožto poskytovatelé základních služeb dle § 2 písm. i) bod 5) tamtéž.

Do roku 2021 se zákon o kybernetické bezpečnosti díky nastaveným kritériím vztahoval pouze na 16 největších nemocnic a zařízení se specializovaným traumatologickým centrem. Teno okruh byl od 1. ledna 2021 na požadavek Asociace krajů rozšířen vyhláškou Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB),[3] aby zahrnoval i menší nemocnice. Nově tak bude muset své systémy lépe zabezpečit 46 zdravotnických zařízení.

Ze zákona mají vybraná zdravotnická zařízení zejména povinnost zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti a vést o nich bezpečnostní dokumentaci. Bezpečnostní opatření mimo jiné zahrnují komplexní systém řízení rizik, zajištění

organizační bezpečnosti, systém pro zvládání kybernetických bezpečnostních událostí a incidentů i pravidelné bezpečnostní audity.

Otázka kybernetické bezpečnosti však rozsahem zákona omezena není. Legislativa je jistě dobrým základem, ale její dodržování "na papíře" zejména v oblasti kybernetické bezpečnosti není dostačující. Nestačí například metodicky nastavit postupy pro povedení analýzy rizik, když pak v praxi není analýza rizik zavedena do běžného provozu. Zavedená bezpečnostní opatření je v oblasti kybernetické bezpečnosti více než kde jinde nutné chápat, a to i ze strany řadových zaměstnanců, řádně dodržovat a pravidelně aktualizovat.

Tuto skutečnost velmi dobře chápe i NÚKIB, který opakovaně a dlouhodobě upozorňuje na nedostatečnou ochranu proti kybernetickým útokům u velké části organizací. A to nejen v případě regulovaných subjektů, kterým vyplývají povinnosti ze zákona o kybernetické bezpečnosti, ale i zbylých organizací, například zákonem o kybernetické bezpečnosti neregulovaných menších nemocnic. Na ty se proto NÚKIB například zaměřuje vzdělávacími programy a podpůrnými metodickými dokumenty.

Kybernetickou bezpečnost nemocnic dokonce náměstek NÚKIB Lukáš Kintr označil za podceněnou.[4] V tomto smyslu však jistě pandemie koronaviru a s ní spojené kybernetické incidenty uštědřili všem tvrdou lekci a priorita kybernetické bezpečnosti tak bezesporu vzrostla.

Aktuálně lze konstatovat, že nedostatečné zajištění kyberbezpečnosti ze strany nemocnic souvisí zejména s podfinancováním. Jak například uvedla mluvčí nemocnice v Novém Městě na Moravě Tamara Pecková: *„…potřebovali bychom hlavně finanční prostředky, za které bychom pořídili novější technologie. Velký problém by bylo sehnat i vysoce specializované odborníky.*"

S tím by dle NÚKIB měly alespoň částečně pomoct peníze z fondů Evropské unie. Zatím však nelze určit, na co vše lze tyto peníze v oblasti kybernetické bezpečnosti využít. Jako první otázkou v tomto směru lze uvažovat nad využitím těchto prostředků pro bezpečné zavedení cloudů v nemocnicích. Komplexní proces, který mnoho nemocnic v blízké době čeká.

Jak se lze vyvarovat dalším kybernetickým incidentům?

Preventivní bezpečnostní opatření mimo technická bezpečnostní opatření zahrnují zejména přípravu komplexní dokumentace (interních předpisů, metodik, smluv), která bude jasným návodem pro kontinuální zajišťování kybernetické bezpečnosti a následně bude sloužit za účelem monitoringu dodržování bezpečnostních pravidel. Jako příklad lze uvést krizové plánování nemocnice a systém analýzy rizik se zaměřením na možná interní a externí ohrožení v oblasti kybernetické bezpečnosti, která mohou narušit běžný provoz nemocnice.

Dobrým výchozím bodem je najmout si externího experta na kybernetickou bezpečnost, který dokáže zkontrolovat celou interní infrastrukturu nemocnice a analyzovat ji z hlediska kybernetické bezpečnosti. Ta pak odhalí zranitelnosti systému, které je nutné adresovat odpovědné osobě a ta by měla přijmout příslušná opatření. V neposlední řadě je pak zásadní řádné proškolení zaměstnanců.

Z výše uvedeného se vzdělávání všech řadových a vedoucích zaměstnanců v současné krizi jeví jako nejrychlejší a nejefektivnější řešení. Velká část incidentů jde totiž bohužel na vrub osobám uvnitř organizace. V praxi jde nejčastěji o otevírání příloh či odkazů podezřelých e-mailů, nedostatečné zajištění fyzické bezpečnosti přensných úložisť dat, např. ztrácení flash disků, paměťových karet nebo dalších médií, případně jiný únik dat.

Na tomto poli je například stále příkladně aktivnější NÚKIB, který poskytuje prezenční školení a semináře pro úředníky a zaměstnance veřejné správy, jejichž účelem je osvojení základních pravidel

kybernetické bezpečnosti.[5]

Většina nemocnic nyní bohužel neví, jak zvyšovat kybernetickou odolnost a posilovat preventivní opatření, jak efektivně čelit kybernetickým útokům, případně jak řešit jejich následky. Současná krize však jasně ukázala, že se to musí naučit. Rizikům je nutné primárně umět předcházet. Konkrétními otázkami se budeme zabývat v příštím článku.

Mgr. Filip Mamrilla,
advokátní koncipient

Mgr. Šimon Toman,
advokátní koncipient

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] K dispozici >>> zde.

[2] K dispozici >>> zde.

[3] Vyhláška č. 573/2020 Sb. ze dne 17. prosince 2020, kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

[4] K dispozici >>> zde.

[5] K dispozici >>> zde.

Další články:

- AML - od zákona č. 253/2008 Sb. k AMLR: co konkrétně musí česká povinná osoba změnit do roku 2027
- Podmíněné propuštění ve světle zásady ústnosti a přímosti
- Byznys a paragrafy, díl 37.: Povinná forma jednání ve smlouvách
- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy