Dopady kybernetického zákona na poskytovatele zdravotních služeb

Kybernetický zákon přináší do zdravotnictví nové povinnosti i zvýšená očekávání v oblasti ochrany dat. Článek nastiňuje skutečné dopady právní úpravy na poskytovatele zdravotních služeb, upozorňuje na časté mýty a nátlakové praktiky dodavatelů a zdůrazňuje klíčovou roli vzdělávání zdravotníků v době rostoucích kybernetických hrozeb.

V poslední době se vyrojila řada tiskových zpráv na téma kybernetické bezpečnosti v oblasti zdravotnictví a dopady tohoto zákona na poskytovatele zdravotních služeb, kdy řada firem nabízí své služby v této oblasti. Situace nápadně připomíná implementaci obecného nařízení o ochraně osobních údajů (GDPR), kdy se tato problematika dočasně stala středobodem společenského dění a řada firem nabízela školení, zpracování dokumentace a zajištění souladu s uloženou povinností. V této souvislosti lze připomenout, že Česká lékařská komora poskytla poskytovatelům zdravotních služeb součinnost v podobě zpracovaných vzorů, které jsou dostupné na webu komory (www.lkcr.cz), ale i řadu konzultací, zejména v případech, kdy firmy doslova „tlačily" poskytovatele, aby s nimi uzavírali smlouvy na dodání dokumentace GDPR za současného nátlaku v podobě poměrně vysokých pokut v případě nesplnění uložených povinností v rozsahu ochrany osobních údajů. Zde je nutno uvést, že řada společností i nadále oslovuje lékaře se snahou přesvědčit je, že mají uzavřít smluvní vztah, avšak zde se s odstupem času projevuje pozitivně informovanost členů komory v podobě rezervovaného postoje, konzultací s právní kanceláří ČLK a až v následném vyhodnocení, zda službu konkrétní lékař využije, či nikoliv.

Podobně je tomuto i v rámci zákona o kybernetické bezpečnosti. Abychom předešli dojmu, že lze situaci brát na lehkou váhu, doplňujeme informace o kazuistiky skutečných případů z praxe. Cílem není poskytovatele znejistit, ale naopak poukázat na nutnost této oblasti věnovat patřičnou pozornost, neboť se jedná o novodobý fenomén, který postupně mění zavedené procesy ve zdravotnictví, jde-li o výměnu a předávání zdravotnických informací, jejich archivaci a dostupnost. Původně papírové procesy jsou postupně a nevyhnutelně nahrazovány elektronickou formou, a je tedy nezbytné být na tento proces řádně připraven, přičemž není zcela rozhodné, zda se jedná o běžného poskytovatele zdravotních služeb, nebo nemocniční zařízení. Přirozeně na velká zdravotnická zařízení dopadá širší spektrum povinností vyplývajících zejména z implementace evropské směrnice NIS2 do kybernetického zákona, jež rozšířila okruh subjektů, které se jí musí řídit, například v podobě povinné registrace organizace, které poskytují tzv. regulovanou službu (*pozn.: Zde se jedná primárně o velká nemocniční zařízení, nikoliv klasické lékařské praxe*). Řada informačních médií se dnes soustřeďuje na nepříliš ideální připravenost zdravotnických zařízení na případné kyberútoky a s tím související plnění povinností vyplývajících se zákona o kybernetické bezpečnosti v oblasti ochrany a nakládání s daty, které obsahují nejen osobní údaje, ale zejména zvláštní kategorii (citlivých) osobních údajů. Byť jsou mediální výstupy veskrze kritické či nepříliš pozitivní, nelze z dostupných informací činit obecné závěry, a to ani v případech, kdy se terčem kybernetického útoku stane nemocnice. Tyto věci se dnes dějí poměrně běžně a stávají se nedílnou součástí běžného života. Běžný uživatel jakéhokoliv elektronického systému nevidí a nemůže vnímat, že na strategická data denně cílí stovky útoků. Lze však predikovat, že počet kybernetických útoků bude narůstat a nebude cílit jen na strategické systémy, ale v budoucnu se nepochybně zaměří i na běžné uživatele či poskytovatele zdravotních služeb (srov. článek v TM č. 4/2022).

Z dosavadní praxe, a to nejen v oblasti zdravotnictví, je zřejmé, že sebelépe nastavený informační systém je funkční jen do té míry, jak jsou připraveni uživatelé, které lze označit vždy za nejslabší článek v hierarchii bezpečnostních pravidel, jichž prostřednictvím zpravidla ke kybernetickým útokům dochází, a to nikoliv úmyslně, ale velmi často z důvodu nedostatku znalostí, nesprávného přístupu zaměstnavatele, ale i laxnosti samotného uživatele. Právě vzdělávání lékařů, respektive zdravotníků v této oblasti je klíčovým předpokladem pro bezpečné a efektivní fungování zdravotnictví v elektronické formě. Zatímco v oblasti velkých společností či nemocnic lze předpokládat, že školení zaměstnanců probíhají pravidelně v rámci nastavených plánů zaměstnavatele, situace v oblasti menších či malých zdravotnických zařízení je méně příznivá a je výsledkem neobhajitelného tlaku zákonodárce na soukromé lékařské praxe v podobě navyšování zákonných povinností bez adekvátního zohlednění nejen časových, ale především finančních nákladů na jejich implementaci. Tato diskrepance mezi velkými a malými zdravotnickými zařízeními, které disponují profesionály v IT oblasti, může v budoucnu vést k vyšší zranitelnosti menších a malých praxí, kterých i v důsledku tohoto fenoménu – elektronizace zdravotnictví – postupně ubývá, a tyto praxe jsou postupně pohlcovány silnými řetězci, které mají v oblasti

implementace povinností podobné možnosti a zázemí jako velké nemocnice.

Protože běžná praxe nemá možnost proškolit zdravotnický personál v oblasti IT bezpečnosti, která, jak již bylo výše uvedeno, je kruciální podmínkou pro bezpečné fungování praxe v oblasti elektronické komunikace a nakládání s daty, zařadila Česká lékařská komora do systému celoživotního vzdělávání lékařů kurz s názvem „Bezpečný zdravotník“, který by měl malým praxím pomoci proškolit zdravotnický personál, a prohloubit tak jejich znalosti a kvalifikaci v IT oblasti s cílem získání praktických zkušeností a dovedností, jejichž aplikace by měla být dennodenní rutinou v rámci činností souvisejících s poskytováním zdravotní péče pacientům.

Kurz bude lékařům dostupný v rámci celoživotního vzdělávání ČLK ve Vzdělávacím portálu ČLK a rovněž bude v případě zájmu lékařů zpřístupněn i jejich zaměstnancům (zdravotním sestřičkám, recepčním a dalším).

Věříme, že tímto způsobem zvýšíme povědomí členů České lékařské komory o kybernetické bezpečnosti, a předpokládáme, že toto téma se do budoucna stane nedílnou součástí celoživotního vzdělávání lékařů a zdravotníků v ČR, neboť pouze orientovaný a řádně připravený zdravotník může být v IT světě bezpečným prvkem, respektive jeho kvalifikovanou součástí.

Navazujeme na úvodní část a přikládáme kazuistiky z praxe, které mají být poučením o dosavadních zkušenostech s kybernetickými útoky a zejména by měly být v pozitivním smyslu „varováním“, že tyto útoky se týkají nás všech, v běžném občanském životě, ale především v profesní oblasti, kdy útočníci záměrně cílí na data, která mohou být mimo jiné i předmětem vydírání.

Kazuistika 1

Obětí phishingu se v posledním roce stalo až 80 procent organizací kritické infrastruktury

Kritická infrastruktura je velmi atraktivní pro útočníky, a je tak pod neustálým tlakem kybernetických hrozeb. Hlavním vstupním bodem, který útočníci používají, jsou stále e-maily. Na tisíc zaměstnanců připadalo 5,7 úspěšných phishingových útoků za rok. I přesto většina organizací nenahlíží na e-maily jako na nebezpečí. Vyplývá to z údajů české společnosti ComSource, která se zaměřuje na kybernetickou bezpečnost a výzkumy globální bezpečnostní firmy OPSWAT.

Phishingové útoky představují obrovský problém pro kyberbezpečnost kritické infrastruktury. Ochrana před nimi je však bohužel velmi často nedostatečná. V globálním měřítku uvedlo 48 procent společností, že nemá současnou e-mailovou ochranu připravenou na phishingové útoky, 64 procent společností nepovažuje svůj přístup k zabezpečení e-mailů za dostatečný, pouze 34 procent společností se domnívá, že jejich nastavení plně vyhovuje e-mailovým regulacím, jako je GDPR. Jedná se sice o globální čísla, ale dle analýzy ComSource je velmi podobná situace také v ČR.

Více než polovina celosvětových organizací kritické infrastruktury, které se účastnily tohoto výzkumu, vychází z předpokladu, že zprávy a soubory jsou ve výchozím nastavení neškodné. Takový přístup je však mylný. Až 80 procent společností v kritické infrastruktuře se stalo oběťmi phishingových útoků, 75 procent veškerého kybernetického ohrožení přichází skrze e-maily. I proto mnohem více organizací potřebuje zavést přístupy s nulovou tolerancí, aby došlo ke zvýšení bezpečnosti. V současnosti je zabezpečení e-mailů spíše v pozadí, do budoucna se firmy připravují k výraznému zlepšování. Právě toto zvyšování obranyschopnosti bude vyžadovat velké úsilí ze strany firem.

Kazuistika 2

Hackeři úspěšně zaútočili na systém Microsoftu

Mezinárodní síť hackerů zneužila závažnou bezpečnostní chybu v softwaru společnosti Microsoft, konkrétně ve firemním systému SharePoint. Útoky zasáhly státní instituce, podniky i univerzity po celém světě. Cílem hackerů bylo proniknout do citlivých systémů, získat přístup k důvěrným dokumentům a odcizit přihlašovací údaje, upozornila agentura Bloomberg.

Mezi zasaženými mají být vládní systémy v USA, Evropě i na Blízkém východě. Podle zdrojů agentury Bloomberg hackeři pronikli například do systémů amerického ministerstva školství, floridského ministerstva financí nebo Valného shromáždění státu Rhode Island. Útočníci se dostali **i do databází zdravotnických zařízení** v USA.

Kazuistika 3

Totální blackout, nefungoval ani zvonek. Hackeři nymburskou nemocnici paralyzovali

Nymburská nemocnice se stala terčem kybernetického útoku. Nyní funguje v nouzovém režimu. Mluvčí Jan Záruba popsal, že útok ochromil téměř všechno. Jeden z pacientů musel být kvůli němu dokonce převezen do jiné nemocnice. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) poskytuje zdravotnickému zařízení součinnost.

Kazuistika 4

Výkupné za ransomware trhá rekordy a kvůli cynismu zločinců umírají lidé

Podle analytické firmy Chainalysis jsou dnešní kyberzločinci stále troufalejší. Medián výkupného u nejzávažnějších typů útoků se navíc za poslední rok a půl zvýšil ze zhruba 200 tisíc na 1,5 milionu dolarů. Virtuální gangy také mění strategie a více se zaměřují na instituce, kde je pravděpodobnější, že zaplatí více peněz – třeba nemocnice, kde je jakákoliv odstávka ještě tíživější, protože jde doslova o život. Naposledy třeba masivní útoky potrápily zdravotnická zařízení v Londýně.

Útočníci sahají i po zastrašujících telefonátech přímo na mobil obětí či rozesílají výhrůžky klientům. Třeba u onkologického centra v Seattlu chodily pacientům e-maily, že mohou být zveřejněny jejich osobní údaje.

Mgr. Daniel Valášek, MBA, ředitel kanceláře ČLK
Ing. Lubomír Noga, Ph.D., MBA
specialita na kybernetickou bezpečnost