MASARYKOVA
UNIVERZITA

PRÁVNICKÁ FAKULTA

Informační a kybernetická bezpečnost ve zdravotnictví

Diplomová práce

HANA VOJTOVÁ

Vedoucí práce: Mgr. Bc. Michal Koščík, Ph.D.

Ústav práva a technologií
Obor Právo

Brno 2023

MUNI
LAW

Bibliografický záznam

Autor: Hana Vojtová
Právnická fakulta
Masarykova univerzita
Ústav práva a technologií

Název práce: Informační a kybernetická bezpečnost ve zdravotnictví

Studijní program: Právo a právní věda

Studijní obor: Právo

Vedoucí práce: Mgr. Bc. Michal Koščík, Ph.D.

Rok: 2023

Počet stran: 130

Klíčová slova: kybernetická bezpečnost, informační bezpečnost, osobní údaje, zdravotnictví, poskytovatel základní služby, zákon o kybernetické bezpečnosti, směrnice NIS, nařízení GDPR

Bibliographic record

Author: Hana Vojtová
Faculty of Law
Masaryk University
Institute of Law and Technology

Title of Thesis: Cybersecurity and Information Security in Healthcare

Degree Programme: Law and Legal Science

Field of Study: Law

Supervisor: Mgr. Bc. Michal Koščík, Ph.D.

Year: 2023

Number of Pages: 130

Keywords: Cybersecurity, Information Security, Healthcare, Personal Data, Operator of Essential Service, Cybersecurity Act, NIS Directive, GDPR Regulation

Anotace

Tato diplomová práce se zabývá informační a kybernetickou bezpečností z pohledu zdravotnických zařízení. Cílem práce je přiblížit důležitost ochrany osobních údajů právě v odvětví zdravotnictví, pro kterou je mimo jiné nezbytné také zajištění kybernetické bezpečnosti. Práce nastiňuje nezbytnost práva na soukromí při poskytování zdravotních služeb, popisuje stěžejní unijní a vnitrostátní právní předpisy týkající se této problematiky. Dále rozebírá nejdůležitější povinnosti stanovené nařízením GDPR a zákonem o kybernetické bezpečnosti. Výzkumná část byla vypracována za pomoci rozhovorů se třemi odborníky zastupujícími zdravotnická zařízení a jedním odborníkem z NÚKIB.

Abstract

This diploma thesis deals with information and cyber security from the perspective of healthcare settings. The aim of the thesis is to present the importance of data protection in the healthcare sector, for which, among other things, it is necessary to ensure cyber security. The thesis outlines the necessity of the right to privacy in the provision of healthcare services, describes the key EU and national legislation on this issue. It also discusses the most important obligations laid down by the GDPR and the Cybersecurity Act. The research part was developed with the help of interviews with three experts representing health care institutions and one expert from the NUKIB.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci a téma **Informační a kybernetická bezpečnost ve zdravotnictví** zpracovala sama. Veškeré prameny a zdroje informací, které jsem použila k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury.

V Brně 29. října 2023 .....

Hana Vojtová

Poděkování

Děkuji panu Mgr. Bc. Michalu Koščíkovi, Ph.D., vedoucímu této diplomové práce, za pomoc, čas a cenné rady, které mi poskytoval. Taktéž děkuji všem respondentům – paní Mgr. et Mgr. Zuzaně Ondrůjové a pánům Ing. Jaroslavovi Třešňákovi, Ing. Aleši Špidlovi a Ing. Lukáši Kintrovi – za jejich příjemný a ochotný přístup, čas a poskytnuté informace.

Dále děkuji svým rodičům, díky nimž jsem mohla vše, co jsem chtěla, kteří mi vždy věřili a nikdy do ničeho nenutili.

Obsah

Seznam tabulek

Seznam pojmů a zkratek

nařízení GDPR	–	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
směrnice 95/46/ES	–	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
směrnice NIS	–	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
směrnice NIS2	–	Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148
Úmluva o biomedicíně	–	Úmluva Rady Evropy č. 164 na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny, sdělení Ministerstva zahraničních věcí č. 96/2001 Sb. m. s.
LZPS	–	Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
ZKB	–	zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
nový ZKB	–	návrh nového zákona o kybernetické bezpečnosti vypracovaného NÚKIB a předložené odborné veřejnosti k zasílání podnětů (stav k 25. 1. 2023)

vyhláška o KB – vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

vyhláška o kritériích pro určení provozovatele základní služby – vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

ZZOÚ – zákon č. 110/2019 Sb., o zpracování osobních údajů

ZZS – zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování

krizový zákon – zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

ÚOOÚ – Úřad pro ochranu osobních údajů

1 Úvod

Zdravotnictví je odvětvím, ve kterém je zvýšená potřeba ochrany osobních údajů, a to především s ohledem na jejich povahu. Pracuje se zde zejména s tzv. pacientskými daty, z nichž ty, které se týkají zdravotního stavu, požívají ochrany jako zvláštní kategorie neboli citlivé osobní údaje.

S ohledem na postupnou elektronizaci zdravotnictví a využívání nových technologií a ostatních prostředků, které přinášejí nejen nové příležitosti a výzvy, ale i nová rizika, je nezbytné regulovat i tuto oblast. Právě zdravotnictví se digitalizace výrazně dotkla a mnoho velmi citlivých osobních údajů je vedeno v informačních systémech. Vedle samotné ochrany osobních údajů je tedy nezbytné zabezpečit i kybernetický prostor, v němž jsou v současnosti velmi často data uložena.

Problematika informační a kybernetické bezpečnosti je velmi rozsáhlá a stejně jako rozlišuje název práce, je rozdělena i právní úprava. Stěžejním předpisem v oblasti ochrany osobních údajů je přímo aplikovatelné nařízení GDPR a jeho adaptační ZZOÚ. Kybernetická bezpečnost je v současné době regulována tuzemským ZKB, který transponuje směrnici NIS. Přičemž na unijní půdě již nabyla účinnosti nová směrnice NIS2, která bude v českých podmínkách promítnuta do zcela nové právní úpravy.

Nařízení GDPR a český ZKB, resp. směrnice NIS, jsou samostatné předpisy, mezi nimiž není přímý vztah. Každá z norem se zaměřuje na odlišné skupiny informací. To však neznamená, že by byly zcela oddělené, doplňují se. Účelem nařízení GDPR je ochrana osobních údajů bez ohledu na to, zda se nachází v elektronické verzi v informačním systému či v listinné podobě. ZKB primárně sleduje ochranu právnických osob s přidruženým know-how, technologiemi a dalšími zájmy. To však neznamená, že by ZKB osobní údaje vylučoval, jen je explicitně nezmiňuje.[1] Je tedy nutné oba předpisy vnímat samostatně, přičemž na konkrétní povinný subjekt se mohou, ale také nemusí, vztahovat oba.

Tato diplomová práce si klade za cíl popsat důležitost ochrany osobních údajů ve vztahu zdravotnického zařízení k pacientovi a povinnosti,

[1] Oubělický, R. Směrnice NIS2 a ochrana osobních údajů: Souvislosti a dopady na GDPR [online]. *kybez.cz.* 14. 7. 2023. [cit. 21. 10. 2023]. https://kybez.cz/smernice-nis2-a-ochrana-osobnich-udaju-souvislosti-a-dopady-na-gdpr/

které musí poskytovatel zdravotních služeb v rámci informační a kybernetické bezpečnosti naplnit. Pozornost bude zaměřena zejména na povinnosti, které nařízení GDPR a ZKB zakládá velkým zdravotnickým zařízením. Především těm, která v současné době spadají pod působnost ZKB jako provozovatelé základní služby. S ohledem na současný růst potřeby kybernetické bezpečnosti i vzhledem k nové právní úpravě, bude pozornost svedena zejména ve výzkumné části na kybernetickou bezpečnost.

První strany, následující po tomto úvodu, se budou snažit zdůvodnit důležitost ochrany soukromí a informací ve zdravotnictví. Stručně zde bude popsána povinná mlčenlivost a vedení zdravotnické dokumentace, k jejichž řádnému plnění je nezbytná činnost především samostatného zdravotnického personálu. Následovat bude kapitola věnována základním pojmům souvisejícím s kybernetickou bezpečností ve zdravotnictví, které je vhodné definovat k pochopení problematiky. Dále budou stručně popsány stěžejní unijní a vnitrostátní právní předpisy, které souvisí s předmětnou problematikou.

V dalších dvou kapitolách budou rozebrány jednotlivé povinnosti, které právní řád stanovuje zdravotnickým zařízením v oblasti kybernetické a informační bezpečnosti. Probrány zde budou nejdůležitější povinnosti určené především největším, a tudíž nejdůležitějším zařízením. Tyto povinnosti nejsou primárně určeny samotnému zdravotnickému personálu, na rozdíl od těch uvedených ve druhé kapitole. Ten o nich, ale musí mít povědomí a nezbytné je také dodržování určitých pravidel a zásad (např. pravidlo čistého stolu), které podporují jejich plnění a přispívají k fungování celého systému bezpečnosti informací.

Výzkumná část bude rozdělena na čtyři části. První dvě shrnou rozhovory s poskytovateli zdravotních služeb, další bude rozebírat rozpravu se zástupcem NÚKIB. Praktická část bude zakončena shrnutím nejdůležitějších poznatků a vyvozenými závěry.

Závěr práce bude věnován problematice, která sice není žádaná, ale je nezbytná – situaci, kdy dojde k porušení zákonných povinností. V poslední kapitole tedy budou popsány správní sankce, které lze nemocnicím za jejich pochybení v podobě spáchání přestupku uložit.

2 Poskytování zdravotních služeb a právo na soukromí

Dle Světové zdravotnické organizace je zdraví *„stav úplné fyzické, duševní a sociální pohody, nikoli pouze nepřítomnost nemoci nebo slabosti“*.[2, 3] Z této definice lze mimo jiné dovodit, že zdraví je komplexní stav fyzické osoby. Toto vymezení je však také poměrně neurčité. Pojem zdraví je natolik široký, že jej zřejmě ani nelze stručně obsáhnout. Každopádně je zdraví pro většinu fyzických osob velmi intimním tématem a lidé mnohdy nemají zájem na zveřejnění či rozšíření informací o svém zdravotním stavu do svého okolí. Vzhledem k citlivosti informací, se kterými je ve zdravotnictví pracováno, se otázky ohledně ochrany soukromí pojí nejen s právními instituty, ale taktéž s etickými problémy.

Lékaři a ostatní zdravotničtí zaměstnanci mají povinnost chránit soukromí svých pacientů, a zejména zachovávat mlčenlivost, chránit osobní údaje a informace o zdravotním stavu, se kterými při výkonu své činnosti přijdou do styku, a řádně vést zdravotnickou dokumentaci, aby nedošlo k jejímu zneužití.

Mimo ochranu soukromí ve smyslu bezpečnosti informací, musí být ve zdravotnictví brán ohled také na ochranu tělesného soukromí a studu. K tomu je pacientům přiznáno právo na volbu poskytovatele zdravotních služeb[4] a právo odmítnout přítomnost jiných osob.[5] Ačkoliv tato práva s ochranou informací přímo nesouvisí, je vhodné je alespoň stručně popsat. Podporují totiž důvěru mezi pacientem a lékařem, resp. zdravotnickým zařízením i zdravotnictvím jako takovým. Je-li důvěra, pak pacient upřímněji sděluje informace, které se stávají předmětem ochrany.

---

[2] World Health Organization. Basic Documents, 49th edition [online]. *who.int.* 2020. [cit. 9. 6. 2023]. https://apps.who.int/gb/bd/pdf_files/BD_49th-en.pdf

[3] Definice Světové zdravotnické organizace (WHO) z r. 1948. V r. 1984 byla zveřejněna poupravená definice, dle které je zdraví *„stav, který na jedné straně umožňuje jednotlivcům i skupinám lidí poznat vlastní cíle a uspokojovat potřeby a na druhé straně reagovat na změny a vyrovnávat se se svým prostředím. Zdraví se chápe jako zdroj každodenního života, a ne jako cíl života.“*

[4] § 28 odst. 3 písm. b) ZZS.

[5] § 28 odst. 3 písm. h) ZZS.

Aby mohlo být ústavně zaručené právo na ochranu zdraví[6] efektivně uplatňováno je mimo jiné potřebné, aby měli pacienti právo na volbu poskytovatele zdravotních služeb. Zvolený poskytovatel by měl odpovídat individuálním zdravotním potřebám pacienta a jeho požadavkům na osobu lékaře. Nezbytné je ovšem poukázat na skutečnost, že poskytovatelem zdravotních služeb se myslí *„fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle ZZS."*[7] Což se projeví v situaci, kdy je poskytovatelem právnická osoba zaměstnávající v téže specializaci více lékařů, typicky větší nemocniční zařízení či kliniky s více lékaři. Tehdy zpravidla není možné vybrat si přesnou osobu, která bude potřebné úkony provádět. Tato možnost volby však může být pacientům konkrétním zařízením poskytnuta.[8]

Právo zvolit si poskytovatele zdravotních služeb je v některých případech a za stanovených podmínek omezeno. Mezi takové situace patří například poskytování zdravotních služeb zdravotnickou záchrannou službou, pracovně-lékařské služby či nařízená izolace, karanténa nebo ochranné léčení.[9] Taktéž může dojít k využití práva zvoleného poskytovatele odmítnout přijetí pacienta do péče. K tomu však může opět dojít pouze v taxativně stanovených případech vyjmenovaných v ustanovení § 48 ZZS.

Zákonná dikce druhého uvedeného oprávnění, dle jejíž první části je možné *„odmítnout přítomnost osob, které nejsou na poskytování zdravotních služeb přímo zúčastněny,"* není přesná. Občasná přítomnost takových osob je nezbytná. Může se jednat například o uklízečky či obsluhu technických zařízení. V praxi se tak možnost odmítnutí přítomnosti bude vztahovat na osoby, které z povahy své činnosti nemají u pacienta co pohledávat, respektive si mohou své povinnosti splnit jinde a jinak.[10] Toto ustanovení by zřejmě šlo použít v případě společných vizit, kdy jsou pa-

[6] Čl. 31 LZPS.

[7] § 2 odst. 1 ZZS.

[8] Sůvová, Z. Právo na svobodnou volbu lékaře v konfrontaci s právem odmítnout pacienta [online]. *advokatijelinek.cz.* 6. 10. 2016. [cit. 17. 9. 2023]. https://www.advokatijelinek.cz/post/pr%C3%A1vo-na-svobodnou-volbu-l%C3%A9ka%C5%99e-v-konfrontaci-s-pr%C3%A1vem-odm%C3%ADtnout-pacienta

[9] Celý taxativní seznam obsahuje ustanovení § 29 ZZS.

[10] Prudil, L. *Právo pro zdravotnické pracovníky*. Praha: Linde, 2014, s. 43.

cientovi před ostatními nemocnými na pokoji sdělovány citlivé informace o jejich aktuální diagnóze, čímž dochází i k porušování povinné mlčenlivosti. Odmítnout lze i přítomnost studentů, kteří se k výkonu zdravotnické profese teprve připravují.

K ochraně soukromí ve zdravotnictví slouží mimo zmíněná práva a odpovídající povinnosti, mnohá další. Soukromí je složitým institutem, jenž je nutné chránit z různých pohledů. Nelze jej ani vyčerpávajícím způsobem obsáhnout v definici, aby v ní byla zahrnuta fyzická i morální integrita osoby.[11] V českém právním řádu legální vymezení neexistuje, ovšem mnozí právní teoretici i soudy se o jeho výklad snaží.

Například Američané S. D. Warren a L. D. Brandeis v roce 1890 definovali právo na soukromí jako právo být ponechán o samotě.[12] Dle Tomáše Sobka je možné tento pojem chápat jako *„vlastní kontrolu nad informacemi o svých osobních záležitostech,"*[13] což spíše odpovídá právu na informační sebeurčení, které je jednou částí práva na soukromí.

Dle Ústavního soudu České republiky: *„právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob."* Taktéž musí respektování soukromého života do určité míry zahrnovat i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.[14]

Právo na ochranu soukromí je chráněno obecnými i speciálními předpisy, ale také etickými a morálními kodexy. Obecná úprava práva na soukromí je obsažena například ve vnitrostátním čl. 7 odst. 1 a čl. 10 odst. 2 LZPS.[15] Tato dvojitá úprava vznikla během legislativního procesu,

---

[11] *S. a Marper proti Spojenému království,* rozsudek Evropského soudu pro lidská práva, 4. 12. 2008, č. stížnosti 30562/04 a 30566/04.

[12] Warren, S. D., Brandeis, L. D. The Right to Privacy. *Harvard Law Review.* 1890, roč. 4, č. 5, s. 195. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[13] Sobek, T. Svoboda a soukromí. In: Šimíček, V. (ed.). *Právo na soukromí.* Brno: Masarykova univerzita, 2011, s. 41.

[14] Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99, právní věta.

[15] Právo na soukromí je v LZPS rozloženo do více ustanovení a doplňováno dalšími aspekty deklarovanými na různých místech (např. listovní tajemství v čl. 13 LZPS).

kdy byl současný čl. 10 inspirován mezinárodní úpravou čl. 8 Evropské úmluvy o lidských právech, ovšem zachována byla i původně navrhovaná úprava současného čl. 7. Důsledkem této roztříštěné úpravy je její překrývání a nesystematické užívání v judikatuře Ústavního soudu.[16]

Právo na soukromí není absolutním právem. Lze jej omezit v zákonem stanovených situacích nebo při jeho konfliktu s jiným základním právem. V případě takového rozporu bývá nejčastěji používán test proporcionality, který zkoumá vhodnost, potřebnost a poměřuje závažnost práv stojících v kolizi.

Ve zmíněných článcích LZPS je široký výčet toho, co spadá do rámce ochrany soukromí. Tento výčet není možné považovat za vyčerpávající a konečný.[17] Právo na ochranu soukromí je velmi široké a zahrnuje rozsáhlé množství aspektů. Zároveň souvisí a prolíná se i dalšími základními právy.

V současné společnosti nabývá na významu právo na informační sebeurčení, deklarované v čl. 10 odst. 3 LZPS. Tato norma přiznává jednotlivci právo na ochranu před neoprávněným shromažďováním, zveřejňováním či jiným zneužíváním údajů o své osobě. Jinými slovy se jedná o oprávnění rozhodnout podle vlastního uvážení zda, popřípadě v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z osobního soukromí jednotlivce zpřístupněny dalším subjektům.[18]

Z mezinárodní úpravy lidských práv konkrétně v oblasti zdravotnictví nelze nezmínit Úmluvu o biomedicíně, která v čl. 2 uvádí: *„Zájmy a blaho lidské bytosti budou nadřazeny zájmům společnosti nebo vědy."* Tato zásada se pak prolíná napříč celou Úmluvou. Čl. 10 Úmluvy o biomedicíně zaručuje každému pacientovi právo na ochranu soukromí ve vztahu k informacím o svém zdraví. Nemocný má taktéž právo znát

Taktéž je toto právo chráněno i prostřednictvím dalších regionálních a mezinárodních katalogů základních práv. Lze zmínit například mezinárodní čl. 8 Evropské úmluvy o lidských právech či regionální čl. 7 Listiny základních práv EU, která v následujícím čl. 8 poskytuje ochranu přímo i osobním údajům.

[16] Nechvátalová, L. Čl. 7. In: Husseini, F., Bartoň, M., Kokeš, M., Kopa, M. a kol. *Listina základních práv a svobod. Komentář. 1. vydání*. Praha: C. H. Beck, 2021, s. 225.

[17] Nález Ústavního soudu ze dne 20. 12. 2016, sp. zn. Pl. ÚS 3/14, bod 56.

[18] Kokeš, M. Čl. 10. In: Husseini, Bartoň, Kokeš, Kopa a kol. *Listina základních práv a svobod,* s. 347.

veškeré shromažďované informace o svém zdravotním stavu. K čemuž je zrcadlově založeno i právo odmítnout informace. Ve výjimečných případech mohou být tato práva v zájmu pacienta omezena, a to zákonnými ustanoveními, která jsou *„nezbytná v demokratické společnosti v zájmu bezpečnosti veřejnosti, předcházení trestné činnosti, ochrany veřejného zdraví nebo ochrany práv a svobod jiných“.*[19]

I tuzemský ZZS přiznává pacientům právo na úctu, důstojné zacházení, ohleduplnost a respektování soukromí při poskytování zdravotních služeb.[20] Taktéž deklaruje právo být či nebýt informován o svém zdravotním stavu, případně určit osobu, které mají být tyto informace sděleny či vyslovit zákaz s poskytováním informací kterékoliv osobě.[21] Při respektování těchto práv, je nutné brát v úvahu skutečnost, že se nejedná o práva absolutní, ale je na ně možné aplikovat různá omezení.

Zajímavé a eticky problematické je zkrácení pacientových práv být či nebýt informován o svém zdravotním stavu, je-li taková redukce v zájmu pacienta. K takové situaci dojde, vznikne-li odůvodněná obava, že by úplná a pravdivá informace pacientovi v dané chvíli mohla, zejména po psychické stránce, spíše ublížit.[22]

K demonstraci si lze představit situaci, kdy pacient chtěl využít právo na informace, ovšem lékař usoudí, že vhodnější bude nesdělení určitých skutečností. K tomu může dojít například v situaci, kdy se pacient dostane do termálního stádia nemoci a sdělení této pravdy by mohlo jeho zdravotní stav vážně zhoršit. K porušení práva na odmítnutí informací, pak lze přistoupit například, když zdravotní stav přestavuje riziko pro okolí, nebo pokud po takovém poznání může pacient učinit určité nezbytné preventivní kroky, které mohou pomoci ke zlepšení jeho zdravotního stavu.[23]

V některých případech vzniká nutnost strpět nezbytné zásahy do soukromí a osobní integrity pacienta. Takovým zásahem může být zejména hospitalizace a poskytování zdravotních služeb bez souhlasu

[19] Čl. 26 odst. 1 Úmluvy o biomedicíně.

[20] § 28 odst. 3 písm. a) ZZS.

[21] § 31 odst. 1 písm. a) a 32 a 33 ZZS.

[22] Mach, J., Buriánek, A., Záleská, D., Máca, M., Vráblová, B. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář.* Praha: Wolters Kluwer, 2018, s. 119.

[23] § 32 odst. 2 ZZS.

pacienta[24] či použití omezovacích prostředků[25] (např. omezení pohybu kurty, použití ochranné vesty, psychofarmaka).

Tyto možnosti lze využít ve výjimečných případech s ohledem na práva ostatních pacientů a práva zdravotnického personálu, jakožto i s ohledem na charakter poskytovaných služeb.[26] Mimo ochranu práv jiných osob, může být účelem těchto opatření ochrana bezpečnosti veřejnosti, předcházení trestné činnosti či ochrana veřejného zdraví.

Právo na ochranu soukromí zahrnuje ve zdravotnictví specifika. Za nejvýznamnější lze považovat povinnost zachovávat lékařské tajemství a řádně vést zdravotní dokumentaci.

2.1 Povinná mlčenlivost

Lékaři během výkonu svého povolání pracují s mnoha citlivými informacemi. Zjišťují je na základě vyšetření pacienta, a taktéž jim jsou sdělovány samotnými fyzickými osobami za účelem zlepšení poskytované zdravotní péče. Nemocní tyto informace sdělují v dobré víře a věří, že když se s lékařem podělí o všechny nejintimnější skutečnosti, které by mnohdy nesdělili ani nejbližším osobám, bude jim poskytnuta pomoc. Vztah pacienta k lékaři je založen na vzájemné důvěře. Lékař věří, že mu pacient sděluje veškeré a pravdivé informace, aby mohl nemocnému pomoci a kvalitně odvedl svoji práci. A pacient doufá, že poskytnuté skutečnosti pomohou ke zlepšení jeho léčby a zdravotního stavu a současně, že nebudou nikterak zneužity. K ochraně informací, které se lékař a další zdravotnický personál dozví v souvislosti s poskytováním zdravotních služeb, slouží institut lékařského tajemství, který lze považovat za pomyslný základ ochrany osobních údajů ve zdravotnictví.

[24] § 38 ZZS.

[25] § 39 ZZS.

[26] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 95.

K jeho dodržování se zavazovali lékaři již v antickém Řecku. Docházelo k tomu prostřednictvím tzv. Hippokratovy přísahy,[27] která se vedle lékařského tajemství skládala z dalších několika slibů. Lékař se jejím složením zavazoval nemocným prospívat, neškodit a být vůči nim diskrétní. Diskrétnost byla v textu přísahy vyjádřena slovy: *„Cokoli, co při léčbě i mimo svou praxi ve styku s lidmi uvidím a uslyším, co nesmí se sdělit, to zamlčím a uchovám v tajnosti."*[28]

Současné lékařské sliby se od antické přísahy obsahově v mnohém liší. Původní znění již není ani možné dodržovat a lékaři v dnešní době dokonce některé obsažené principy hrubě porušují. Nedodržují zejména bezvýhradný zákaz vyvolávání potratů či provádění operací. Zakázáno bylo také provádění eutanazie, které je nyní v některých zemích a za určitých podmínek povoleno. Každopádně jsou otázky potratů a eutanázie, které byly v době vzniku textu přísahy nepřijatelné, i v dnešní době stále velice sporné.

Kromě zásady lékařského tajemství se z původní dikce do současnosti přeneslo i pravidlo konání úkonů ve prospěch pacienta. To bylo přísaháno: *„Lékařské úkony budu konat v zájmu a ve prospěch nemocného, dle svých schopností a svého úsudku. Vystříhám se všeho, co by bylo ke škodě a co by nebylo správné."*[29]

Pravidla obsažená v Hippokratově přísaze byla definována jako morální závazky lékaře, jejichž úkolem bylo především udržet vážnost lékařského stavu, nebyla tedy formulována jako vymahatelná práva pacientů. Taková práva se začala tvořit až po 2. světové válce, kdy docházelo k masivnímu porušování základních lidských práv a svobod.[30]

V současné době je povinná mlčenlivost ve zdravotnictví právním závazkem[31] a lze ji definovat jako zákonem uloženou nebo státem uznanou povinnost fyzické osoby nesdělovat nepovolané osobě určité skutečnosti a současně povinnost nést právní důsledky, pokud by došlo k jejímu

[27] Hippokratova přísaha vznikla kolem r. 400 př. n. l. Připisována je Hippokratovi, ale není známo, zda ji skutečně složil, schválil či vůbec znal. Hippokrates je označován jako zakladatel západní medicíny.

[28] Doležal, T., Doležal, A. *Ochrana práv pacienta ve zdravotnictví.* Praha: Linde, 2007, s. 14.

[29] Tamtéž.

[30] Tamtéž.

[31] § 51 ZZS.

porušení.[32] Nevztahuje se výhradně na lékaře, nýbrž i na další osoby, nejčastěji na zdravotnické a další odborné pracovníky, osoby, které se k takovému zaměstnání připravují či osoby, které je již nevykonávají.

V praxi je tento institut poměrně problematický, a to zejména svým nezřetelným rozsahem, o němž odborná veřejnost neustále vede spory. Zatímco se některé zatížené osoby domnívají, že se tato povinnost vztahuje pouze na medicínské informace ohledně zdravotního stavu pacientů, jiní jsou přesvědčeni, že by o své práci neměli hovořit vůbec.[33]

Někteří autoři jsou názoru, že by měly být chráněny pouze informace získané v bezprostřední souvislosti se samotnými zdravotními výkony a pouhé sdělení, že se nějaký člověk nachází ve zdravotnickém zařízení, není porušením této povinnosti.[34] Autorka práce se přiklání k názoru, že za běžných okolností by takové oznámení vadit nemělo. Ovšem bezesporu existují situace, kdy by i toto mohlo být považováno za zásah do soukromí pacienta, a to zejména v případě hospitalizace například v psychiatrické léčebně.[35]

Zda je sdělení některých informací třetí osobě přijatelné, je nutné posoudit v konkrétní situaci tak, aby byla zachována individuální ochrana soukromí pacienta. Rovněž je nutné myslet na dikci zákona, která hovoří o *„všech skutečnostech, o kterých se dozvěděl v souvislosti s poskytováním zdravotních služeb".* Nelze tedy chránit pouze informace o zdravotním stavu, ale je potřeba poskytovat toto zajištění i informacím o rodinných či sociálních vztazích.[36] Lze uzavřít, že ochráněny musí být veškeré informace, které se lékař o svém pacientovi dozvěděl, a které by mohly nějakým způsobem poškodit jeho či jiné osoby, případně by mohly být jinak zneužity.

---

[32] Uherek, P. *Povinná mlčenlivost zdravotnických pracovníků: komplexní rozbor aktuální právní úpravy.* Praha: Grada, 2008, s. 10–11.

[33] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 241.

[34] Buriánek, J. *Lékařské tajemství, zdravotnická dokumentace a související právní otázky.* Praha: Linde, 2005, s. 14.

[35] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 242.

[36] Prudil. *Právo pro zdravotnické pracovníky,* s. 23.

Lékařské tajemství není absolutní. Existuje z něj poměrně mnoho výjimek, které jsou obsaženy nejen v ZZS,[37] ale i v jiných právních předpisech.[38] V některých případech dokonce vzniká oznamovací povinnost sdělit příslušným orgánům informace, které se osoba dozvěděla při poskytování zdravotních služeb a které by jinak podléhaly povinné mlčenlivosti.[39] Těchto zásahů do institutu lékařského tajemství je široká škála, uvedu proto pouze ty, které jsou v praxi nejvíce používané.

Jednou z nejčastějších výjimek je sdělování nezbytných informací pro zajištění a zkvalitnění návaznosti poskytovaných zdravotních služeb.[40] K tomuto prolamování lékařského tajemství, zákon nevyžaduje souhlasu osoby, o níž jsou informace sdělovány. Je ovšem nezbytné, aby se zdravotnický pracovník, který si pacienta přebírá do péče, dotazoval pouze na informace, které souvisí s následující péčí. Není tedy přípustné, aby se například pracovník RTG oddělení dotazoval na psychiatrickou diagnózu pacienta, kterého má snímkovat.[41]

Dalším příkladem je sdělování informací v případě, kdy je poskytovatel své mlčenlivosti v určitém rozsahu zproštěn.[42] V takové situaci by však osoba, zbavená svého závazku, měla myslet na to, aby v případě potřeby měla nezpochybnitelný důkaz. Je tedy vhodné, vyžadovat od pacienta, nejlépe v písemné podobě, prohlášení s přesným vymezením komu

[37] § 51 odst. 2, 3, 4 ZZS.

[38] Např. § 10 odst. 4 či § 10a zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí.

[39] Jelínková, B. Hippokratova přísada: Jak se slavný slib lékařů měnil a co vlastně dnes slibují? [online]. *stoplusjednicka.cz.* 2. 11. 2021. [cit. 9. 6. 2023]. https://www.stoplusjednicka.cz/hippokratova-prisaha-jak-se-slavny-slib-lekaru-menil-co-vlastne-dnes-slibuji

[40] § 51 odst. 2 písm. a) ZZS.

[41] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 242.

[42] § 51 odst. 2 písm. b) ZZS.

a jaké údaje mohou být sděleny, s připojeným datem a vlastnoručním podpisem pacienta či jeho zákonného zástupce.[43, 44]

Jak již bylo zmíněno, v některých případech vzniká osobám, jinak zatíženým povinnou mlčenlivostí, povinnost oznamovací. Plnění oznamovací povinnosti, která je osobám ukládána zvláštními právními předpisy, nemůže nikdy být porušením původní povinnosti.[45] Pro zdravotnické pracovníky je snad nejdůležitější splnění oznamovací povinnost vůči orgánům činným v trestním řízení. Při jejím opomenutí se totiž sami ocitají v pozici trestně stíhaného pro spáchání trestného činu nepřekažení nebo neoznámení trestného činu.[46] Jejich závazek vzniká v okamžiku, kdy se hodnověrným způsobem dozví, že jiný připravuje nebo páchá, nebo již spáchal některý z trestných činů vyjmenovaných v předmětných ustanoveních trestního zákoníku.

Dalším příkladem může být tzv. signalizační povinnost vůči orgánům sociálně-právní ochrany dětí (např. při opuštění dítěte a jeho zanechání ve zdravotnickém zařízení matkou[47]).

Institut lékařského tajemství po staletí byl, stále zůstává a bezesporu i nadále bude velmi důležitým. Lze se dokonce domnívat, že jeho důležitost v dnešní digitální době stále roste, stejně jako ochrana soukromí celkově. Zabezpečení například zdravotnické dokumentace, o níž bude pojednáváno níže, je spíše věcí technickou. Ochrana informací, které určitá osoba uchovává ve své hlavě je složitější a vždy záleží na konkrétní osobě, do jaké míry povinnost mlčenlivosti ctí. I přes existenci různých sankčních prostředků, které pro porušitele mohou být

---

[43] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 242.

[44] Od této výjimky (zproštění povinnosti mlčenlivosti) je třeba odlišovat právo pacienta garantované v ustanovení § 33 ZZS. Toto právo umožňuje pacientům při přijetí do péče určit, kdo má být informován o jeho zdravotním stavu, zda tyto osoby mohou nahlížet do jeho zdravotnické dokumentace a zda mohou v případech podle § 37 odst. 7 ZZS vyslovit za pacienta souhlas či nesouhlas s poskytnutím zdravotních služeb. Taktéž může pacient zakázat podávání jakýchkoli informací komukoli.

[45] Mach, J. *Lékař a právo. Praktická příručka pro lékaře a zdravotníky.* Praha: Grada, 2010, s. 162.

[46] Viz § 367 a 368 zákona č. 40/2009 Sb., trestní zákoník.

[47] Viz § 10a odst. 1 zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí.

velmi nepříjemné, se jednou vyslovená slova nedají vzít zpět. Pro poškozeného pacienta může mít narušení jeho soukromí daleko širší a hlubší negativní dopady, než sankce pro strůjce takové situace.

2.2 Zdravotnická dokumentace

Zdravotnická dokumentace je souborem veškerých údajů o zdravotním stavu pacienta. Zpravidla je vedena po celý život fyzické osoby. Obsahuje komplexní informace o dosud poskytnuté a případně plánované zdravotní péči, výsledky různých vyšetření, záznam o vývoji zdravotního stavu a další informace, které poskytovatel zdravotních služeb považuje za nezbytné v souvislosti s poskytovanou péčí zaznamenat.[48] Zapisovat do ní mohou pouze pověřené osoby, a jen v rozsahu jejich kompetencí.

Dalšími informacemi, které může zapisující považovat za důležité zaznamenat, mohou být například údaje zjištěné z rodinné, osobní, pracovní, popř. i ze sociální anamnézy.[49] V mnoha případech je tedy možné ze zdravotnické dokumentace pacienta získat citlivé informace i o jiných lidech. Obsah zdravotnické dokumentace a její další součásti jsou podrobněji vyčteny zejména v ustanovení § 53 odst. 2 ZZS a také ve vyhlášce č. 98/2012 Sb., o zdravotnické dokumentaci.

V současné době je možné zdravotnickou dokumentaci vést v listinné nebo elektronické podobě, popř. v jejich kombinaci.[50] Pro případ vedení dokumentace výlučně v elektronické podobě, definuje ZZS v ustanovení § 55 podmínky, vztahující se zejména k technickému zajištění a bezpečnosti uložených záznamů. Zákonné požadavky rozvádí a doplňuje závazné stanovisko České lékařské komory č. 1/2009 – Elektronický způsob vedení zdravotnické dokumentace.[51] Vedením zdravotnické dokumentace v elektronické podobě se dostáváme k regulaci kybernetického prostoru, jehož ochrana je nezbytná k zajištění bezpečnosti zaznamenávaných osobních údajů.

---

[48] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 248.

[49] § 53 odst. 2 písm. e) ZZS.

[50] § 54 odst. 1 ZZS.

[51] Dostupné na https://www.lkcr.cz/zavazna-stanoviska-clk.

Ať už je vedena v jakékoli formě, *„musí být vedena průkazně, pravdivě, čitelně a musí být průběžně doplňována"*.[52] Takové zodpovědné vedení může mimo jiné posloužit jako důkazní prostředek v případě prokazování poskytnuté zdravotní péče a skutečnosti, zda poskytovatel zdravotní péče postupoval *lege artis*. Naopak provedení nezaznamenaných úkonů se poskytovateli prokazuje velmi těžko, a to i při sebelepším poskytnutí zdravotní péče.[53]

Z hlediska ochrany soukromí je důležité právo nahlížet do zdravotnické dokumentace, které zahrnuje i právo pořizovat si její výpisy či kopie.[54] Toto právo je možné uplatnit pouze v přítomnosti zaměstnance zdravotnického zařízení, jímž může být například lékař či jiný pověřený pracovník. Pro poskytování informací je rozhodující právní úprava účinná v době uplatnění požadavku a umožnění přístupu.[55]

V základní podobě náleží toto oprávnění pacientovi, jeho zákonnému zástupci či opatrovníkovi a určeným osobám. Těmto osobám musí být poskytnuty veškeré shromažďované informace ve zdravotnické dokumentaci, včetně rentgenových snímků, CT nálezů apod.[56] Jediné omezení je uloženo pro nahlížení do záznamů autorizovaných psychologických metod a popisu léčby psychoterapeutickými prostředky.[57]

Osobám blízkým[58] zemřelému pacientovi toto právo náleží také.[59] Pacient však za života může vyslovit zákaz sdělování takových informací, který může být porušen pouze v případě zájmu ochrany zdraví.[60] Tuto výjimku lze zřejmě vztahovat na situaci, kdy je u zemřelého objevena například nějaká dědičná choroba, která dosud v jeho rodině nebyla známá.

---

[52] § 54 odst. 2 ZZS.

[53] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 249.

[54] § 65 a násl. ZZS.

[55] Rozsudek Nejvyššího soudu ze dne 30. 8. 2011, č. j. 25 Cdo 3562/2009, právní věta.

[56] Mach. *Lékař a právo. Praktická příručka pro lékaře a zdravotníky*, s. 183.

[57] § 65 odst. 1 písm. a) ZZS.

[58] Osoba blízká je definována v ustanovení § 22 odst. 1 zákona č. 89/2012 Sb., občanský zákoník.

[59] § 65 odst. 1 ZZS.

[60] § 33 odst. 4 věta druhá ZZS.

Další osoby mohou nahlížet v nezbytném rozsahu a v zájmu pacienta nebo pro naplnění ZZS či jiných předpisů, a to i bez souhlasu osoby, o níž je zdravotnická dokumentace vedena.[61] Studenti mohou také nahlížet v nezbytně nutném rozsahu,[62] ovšem stejně jako v případě jejich účasti na léčbě, může být pacientem i tato možnost zakázána.

Soukromí osob může být též zasaženo v případě předávání zdravotnické dokumentace mezi poskytovateli. Při volbě nového poskytovatele zdravotních služeb, ať už se jedná o nového praktického lékaře či ambulantního specialisty, je potřeba poskytnout mu veškeré potřebné informace, které jsou nutné k návaznosti poskytování zdravotní péče. Tyto informace se předávají v podobě výpisu ze zdravotnické dokumentace, popřípadě, je-li to praktičtější, formou kopií veškeré zdravotnické dokumentace.[63] Originál zdravotnické dokumentace by měl vždy zůstat u poskytovatele, který dokumentaci vedl. V případě úmrtí lékaře, který byl podnikající fyzickou osobou či při zániku právnické osoby, která poskytovala zdravotnickou péči, je dokumentace předána orgánu příslušnému k registraci (krajský úřad), který zajistí její předání nově zvoleným lékařům.[64]

Při vedení zdravotnické dokumentace je potřebné myslet na její zvláštní povahu, která neumožňuje nakládání jako s předmětem vlastnického práva a lze s ní tedy disponovat pouze způsobem, který stanoví zákon. Z tohoto důvodu nelze vymáhat přístup pacienta k informacím pomocí vlastnické žaloby na vydání věci (zdravotnické dokumentace).[65] Jejím účelem je po stanovenou dobu uchovávat a poskytovat informace o zdravotní péči, přičemž má být vždy známa skutečnost, kde se konkrétní dokumenty v určitou chvíli nachází (tzv. princip dohledatelnosti).[66]

---

[61] § 65 odst. 2 ZZS.

[62] § 65 odst. 3 ZZS.

[63] Mach, J. *Lékař a právo. Praktická příručka pro lékaře a zdravotníky,* s. 189.

[64] Tamtéž.

[65] Rozhodnutí Nejvyššího soudu ze dne 30. 8. 2011, č. j. 25 Cdo 3562/2009.

[66] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 257.

Důležité je také dodržení skartační doby. Po určitý čas tuto dokumentaci uchovávat a poté zničit, provést skartaci. Doby uchování zdravotnické dokumentace a způsob jejího zničení stanovuje vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci.

Zákonná úprava vedení a ochrany zdravotnické dokumentace obsahuje mnohá specifika, která s ohledem na téma této práce není důležité dále rozebírat. Pro představu se jedná například o způsob vedení zdravotnické dokumentace v případě utajeného porodu[67] či o omezení nahlížení do dokumentace v případě podezření na zneužívání, týrání nebo ohrožování zdravého vývoje nezletilého pacienta.[68]

Aktuálně je v Poslanecké sněmovně České republiky předložena novela ZZS a zákona č. 325/2021 Sb., o elektronizaci zdravotnictví (dále též jen „Návrh“).[69] Jedním z cílů tohoto Návrhu je novelizace úpravy vedení zdravotnické dokumentace v elektronické podobě, tak aby se tato forma stala primární. Současná právní úprava totiž neposkytuje konzistentní, technicky proveditelný a provozně efektivní způsob vedení elektronické zdravotnické dokumentace.[70] V praxi tak převažuje listinná podoba, případně doplněná o digitální.

Předkládaný Návrh chce nově definovat zdravotnickou dokumentaci a zavést i její negativní vymezení. Taktéž je navrhována povinnost podepisování elektronických dokumentů elektronickým podpisem pacienta. Poslední novinkou mají být pravidla pro sdílení údajů, a to pro účely

[67] § 56 ZZS.

[68] § 67 ZZS.

[69] Úřad vlády ČR. Návrh zákona, kterým se mění zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, a zákon č. 325/2021 Sb., o elektronizaci zdravotnictví [online]. *odok.cz.* Datum autorizace 20. 12. 2022. [cit. 20. 6. 2023]. https://odok.cz/portal/veklep/material/KORNCMACTGI2/

[70] Úřad vlády ČR. Důvodová zpráva k Návrhu zákona, kterým se mění zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, a zákon č. 325/2021 Sb., o elektronizaci zdravotnictví [online]. *odok.cz.* 8. 6. 2023. [cit. 20. 6. 2023]. https://odok.cz/portal/veklep/material/KORNCMACTGI2/

vědy, výzkumu a statistiky, pro sdílení mezi poskytovateli zdravotních služeb, ale také pro mezinárodní sdílení.[71]

Všechny tyto úpravy jsou navrhované k úspěšnému provedení elektronizace zdravotnictví. Účinnost Návrhu je dle Důvodové zprávy navrhována k 1. lednu 2024.

V dalších ustanoveních[72] hovoří ZZS také o Národním zdravotnickém informačním systému (dále též jen „NZIS"). Jedná se o jednotný celostátní informační systém veřejné správy, který slouží ke shromažďování a zpracování osobních a dalších údajů ze základních registrů orgánů veřejné správy, od poskytovatelů zdravotních služeb, případně od dalších osob. Účelem tohoto sběru je zejména získání podkladů pro hodnocení zdravotního stavu obyvatelstva a jeho vývoje, či sledování nových případů společensky závažných nemocí.[73]

Pokud zákon nestanoví jinak, jsou informace do NZIS vkládány bez souhlasu subjektů a pouze v anonymizované či pseudonymizované podobě, které znemožní identifikaci konkrétní fyzické osoby.[74] Vkládání informací bez souhlasu je ve smyslu nařízení GDPR možné na základě stanovené právní povinnosti nebo v nezbytném rozsahu k ochraně vlastních práv. V jiných případech jen se souhlasem příslušné fyzické osoby.[75] V tomto případě se bude jednat o plnění určených právních povinností a není tedy nutné souhlas vyžadovat.

---

[71] Kovář, D., Slavíková, K. Jak se (možná) změní vedení elektronické zdravotnické dokumentace? [online]. *havelpartners.blog.* 24. 3. 2023. [cit. 20. 6. 2023]. https://www.havelpartners.blog/jak-se-mozna-zmeni-vedeni-elektronicke-zdravotnicke-dokumentace

[72] § 70 a násl. ZZS.

[73] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 286.

[74] Ústav zdravotnických informací a statistiky ČR. Osobní údaje vedené v registrech a systémech ÚZIS ČR [online]. *uzis.cz.* [cit. 9. 6. 2023]. https://www.uzis.cz/index.php?pg=o-nas--ochrana-osobnich-udaju--osobni-udaje-v-registrech-a-systemech

[75] Mach, Buriánek, Záleská, Máca, Vráblová. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář*, s. 287.

3 Základní pojmy

V následujících podkapitolách budou stručně definovány a vysvětleny nejdůležitější základní pojmy, se kterými se lze při popisování informační a kybernetické bezpečnosti setkat. Tyto termíny jsou nezbytné k pochopení textu, v němž jsou pojmy užívány, a dalších souvislostí týkajících se předmětné problematiky.

3.1 Osobní údaje

Osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Tedy o osobě, kterou lze pomocí takových údajů přímo či nepřímo identifikovat.[76] Typicky se jedná o jméno, rodné číslo, adresu, osobní stav apod.

Identifikace či identifikovatelnost osoby ovšem může nastat různými způsoby, nemusí jít pouze o údaje s ní sepnuté. Důležité je, že se jimi dá dané osoby nějakým způsobem dopátrat, a to i nepřímo. Dle starší judikatury může být takovým údajem i evidence pracovní doby, ve které jsou zaznamenány příchody a odchody, včetně informací o přestávkách a dobách, které se nezapočítávají do pracovní doby.[77] Mohou to tedy být i informace, které se na první pohled jako osobní údaje nejeví.

Při rozhodování o tom, zda může být nějaký údaj považován za osobní, by se mělo přihlédnout k prostředkům, o nichž lze rozumně předpokládat, že budou využity k identifikaci fyzické osoby. Při tom by se měly zvážit všechny objektivní faktory, zejména náklady, čas a dostupné technologie.[78] V úvahu by tedy měla být brána také námaha, kterou bude nutné vynaložit za účelem dopátrání se konkrétního člověka.

Stanovena je také zvláštní kategorie osobních údajů, tzv. citlivé údaje,[79] které požívají zvýšené ochrany. Ta se projevuje v zákazu jejich zpracování. Do této skupiny se řadí informace, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod.[80] Jsou jimi napří-

[76] Čl. 4 odst. 1 nařízení GDPR.

[77] Rozsudek Soudního dvora EU ze dne 30. 5. 2013 ve věci C-342/12.

[78] Recitál 26 preambule nařízení GDPR.

[79] Čl. 9 nařízení GDPR.

[80] Recitál 51 preambule nařízení GDPR.

klad údaje o rasovém či etnickém původu, politických názorech, náboženství či sexuálním životě, ale i informace, se kterými je pracováno zejména ve zdravotnictví. Těmi se rozumí údaje o zdravotním stavu, genetické údaje (např. DNA či krevní skupina) a biometrické údaje (např. daktyloskopické údaje).

Zákaz zpracování citlivých osobních údajů lze prolomit z důvodů vyjmenovaných v čl. 9 odst. 2 nařízení GDPR. Při poskytování zdravotní péče se bude jednat zejména o nezbytnost zpracování pro účely zdravotních služeb či z důvodu významného veřejného zájmu v oblasti veřejného zdraví.[81] Taktéž je možné zpracování citlivých osobních údajů na základě uděleného souhlasu, který je nezbytný, neexistuje-li právní či smluvní vztah nebo oprávněný zájem. Souhlasem se rozumí *„jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.“*[82]

3.2 Kybernetický prostor

K vysvětlení pojmu „kybernetická bezpečnost“ je vhodné nejprve si objasnit pojem „kybernetický prostor“ či zkráceně jen „kyberprostor“. Mezi velkým množstvím definic tohoto prostředí není možné nalézt jedno univerzální vymezení, které by dokázalo kyberprostor komplexně popsat.

Poprvé byl tento pojem použit roku 1982 Williamem Gibsonem v jeho knize Jak vypálit Chrome (Burning Chrome). K samotné definici se stejný autor dostal o dva roky později v románu Neuromancer, kde uvedl, že kyberprostor je:

> *„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie*

[81] Čl. 9 odst. 2 písm. h) a i) nařízení GDPR.

[82] Čl. 9 odst. 2 písm. a) nařízení GDPR.

> *světla seřazené v neprostoru mysli, shluky a souhvězdí dat. …“*[83]

Zákon o kybernetické bezpečnosti chápe kybernetický prostor jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“.*[84]

Kyberprostor je virtuální prostor vytvořený člověkem, který vznikl propojením menších sítí. Toto prostranství je všudypřítomné a nezná hranic. Uživatelé díky němu mohou rychle a jednoduše komunikovat i napříč kontinenty. Virtuální prostředí není opakem prostředí skutečného.[85] Virtuální prostor je realita, která prošla procesem významné změny formálních jevových znaků.[86] Je to reálné prostranství, které žije, a do kterého v současné době většina z nás promítá alespoň část svého života v prostoru, jehož podstata je pro člověka lépe vnímatelná. Obě tyto části lidského bytí jsou v současnosti neoddělitelně propojené. Člověk se může projevovat buď osobně, nebo v kyberprostoru, který mu je schopen poskytnout určitou anonymitu.

V současné době se kyberprostor dotýká každého z nás, přičemž není nutné, abychom v něm byli jakkoliv aktivní. Zejména s postupnou elektronizací veřejné správy totiž dochází v jeho prostředí minimálně k výměně našich, často velmi osobních a citlivých, informací.

Dalo by se říci, že stále více činností běžného života se přesouvá „z papíru do sítě“. S touto provázaností, která je v dnešní době nezbytná, vzniká však i prostor pro zneužití takového stavu. Rodí se tedy nové příležitosti pro počítačovou kriminalitu. Oproti běžným zločincům, musí být ti v kyberprostoru daleko sofistikovanější, musí znát způsoby jak do sítí vniknout a jak se tam chovat. Mohou ovšem získat informace téměř o všem a o všech. Severoatlantická aliance proto kybernetický prostor

---

[83] Gibson, W. *Neuromancer.* Plzeň: Laser, 1998, s. 58.

[84] § 2 písm. a) ZKB.

[85] Lévy, P. Welcome to Virtuality. *Digital Creativity.* 1997, roč. 8, č. 1, s. 3. Dostupné též z: https://www.tandfonline.com/doi/pdf/10.1080/09579139708567068?casa_token=v5cP12748rAAAAAA:CpTsLsZqGqsvqSTfAkKz9MZsrE14eP1PlIqCqASJ-HOGSZ1pk6GD1VVIle0xKUxvl32fZ6kIQis5z

[86] Polčák, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 8.

označila jako tzv. pátou zónu války, vedle země, vody, vzdušného prostoru a vesmíru.[87]

3.3 Kybernetická bezpečnost

Ochrana kybernetického prostoru je, při současném vzestupu a vzrůstající závislosti na informačních technologiích, již nezbytností. V posledních letech se zvyšuje a neustále rozvíjí pozornost poskytována oblasti zabezpečení kybernetického prostoru, a to nejen ze strany státních orgánů, ale i ze strany soukromých právnických či fyzických osob.

S rozvojem informačních technologií je důležité virtuální svět chránit před nebezpečnými vlivy, které se jej snaží ovlivnit či ohrozit. Kybernetická bezpečnost je *„schopnost odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky“*.[88] Kybernetická bezpečnost má zaručovat komplexní ochranu kybernetického prostoru. Nemohou být opomenuty neúmyslné činy, které tento prostor také mohou poškodit. Zajištění bezpečnostních opatření ve chvíli útoku by však bylo neefektivní. Kybernetickou bezpečnost je proto třeba chápat jako kontinuální činnost, při které je největší důraz kladen na prevenci, a která se případně uplatní i v dalších fázích, tj. při detekci hrozby a při represi následků.

Kybernetickou bezpečnost můžeme definovat pomocí tzv. triády CIA, dle které má kybernetická bezpečnost zajišťovat důvěrnost *(Confidentiality)*, integritu *(Integrity)* a dostupnost *(Availability)* dat figurujících v kyberprostoru.[89] Důvěrnost má zabránit přístupu k informacím neoprávněným osobám. Integrita zajišťuje správnost a spolehlivost ulo-

[87] Sedlák, J. NATO posouvá kybernetikou ochranu mezi priority a na nejvyšší úroveň [online]. *E15.cz.* 5. 9. 2014. [cit. 3. 10. 2022]. https://www.e15.cz/magazin/nato-posouva-kybernetickou-ochranu-mezi-priority-a-na-nejvyssi-uroven-1116140

[88] Jirásek, P., Novák, L., Požár, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2012, s. 68. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_V1_5_El.pdf

[89] Graham, J., Howard, R., Olson, R. *Cyber Security Essentials.* Boca Raton: CRC Press, 2011, s. 1.

žených dat a systémů a chrání je před neoprávněnými změnami. A posledního prvku, dostupnosti, dosáhneme zajištěním rychlé a spolehlivé přístupnosti dat a informačních systémů oprávněným uživatelům.[90]

Tato triáda je někdy doplňována o další tři principy, kterými jsou držení či kontrola *(Possession or Control)*, autentičnost *(Authenticity)* a užitečnost *(Utility)*. Tento koncept je znám jako Parkerova šestice či Parkerian hexad.[91][92] Princip držení či kontroly má chránit před myšlenkou, že by informace mohl držet a kontrolovat někdo jiný, aniž by došlo ke skutečnému narušení důvěrnosti.[93] Autentičnost značí jistotu, že informace pochází ze zdroje, ze kterého tvrdí, že pochází.[94] A užitečnost pak znamená podle pojmenování samotnou užitečnost dat. Data mohou splňovat všechny ostatní principy, ale pokud budou nepoužitelná, nebudeme je moci nikterak využít.[95]

Kybernetická bezpečnost je tedy ochrana kyberprostoru a zejména pak ochrana důvěrnosti, integrity a dostupnosti dat v něm kolujících, tak jak popisuje výše zmíněná triáda CIA. Snaží se minimalizovat možná rizika, která vyvolávají kybernetické útoky, popřípadě i dopady těchto hrozeb tak, aby případný zásah měl co možná nejmenší následky. To je ve zdravotnictví, kde narušení sítě může ohrozit pacienty a může mít až fatální následky, velmi důležité.

Stejně jako útočníci hledají stále nové sofistikovanější způsoby, jak proniknout přes určitá zabezpečení, musí zrcadlově i bezpečnostní inženýři přicházet na nové metody, jak jim tomu zabránit. Přesněji možná – jak jim to ztížit, hacker totiž bývá o krok napřed. Jediným řešením je dle

[90] Tamtéž, s. 3–5.

[91] Podle jeho tvůrce Donna B. Parkera (1929 – 2021).

[92] Pender-Bey, G. The Parkerian Hexad: The CIA Triad Model Expanded [online]. *Lewis University*, s. 6. [cit. 21. 10. 2022]. http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[93] Tamtéž, s. 10.

[94] Tamtéž, s. 14.

[95] Tamtéž, s. 18.

některých odborníků pochopit chování aktuálních hrozeb a rychle reagovat na jejich vývoj.[96] Cílem tedy je, když ne „být o krok před hackerem", alespoň se s ním pokusit „sladit krok" a snažit se překážet jeho činnosti.

Vedle pojmu kybernetické bezpečnosti je vhodné zmínit další dva příbuzné termíny, a sice bezpečnost informačních systémů (počítačovou bezpečnost) a informační bezpečnost.

Kybernetická bezpečnost se od bezpečnosti informačních systémů liší prostředím, ve kterém dochází k její realizaci. Bezpečnost informačních systémů chrání počítače a počítačové sítě především na menší lokální úrovni. Tyto menší sítě pak společně s jejich jednotlivými prvky a jinými zařízeními, která mají svoji IP adresu, dohromady tvoří kyberprostor, který je chráněn kybernetickou bezpečností.[97] Dle důvodové zprávy k ZKB je pojmu kybernetické bezpečnosti užito k odlišení od pojmu informační bezpečnosti resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu funkčnosti síťového prostředí.[98]

Informační bezpečnost je ochranou informací jako takových, zahrnuje pod sebe oba výše zmíněné pojmy a je tedy pojmem nejširším. Můžeme pod něj zařadit ochranu informací zachycených na nejrůznějších nosičích,[99] například na papíru, flash disku, ale také právě v kyberprostoru, informačních sítích či na samotných počítačích.

3.4 Kybernetický útok

Jak již bylo zmíněno výše, cílem kybernetické bezpečnosti je minimalizovat rizika, která vyvolávají kybernetické útoky, popřípadě zmírnit jejich

[96] Slávik, M. Útočníci jsou vynalézaví, obyčejný antivirus už k ochraně dat nestačí [online]. *HN.cz.* 18. 7. 2017. [cit. 11. 10. 2022]. https://partner.hn.cz/c1-65803020-utocnici-jsou-vynalezavi-obycejny-antivirus-uz-k-ochrane-dat-nestaci

[97] Smejkal, V., Sokol, T., Kodl, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019, s. 25.

[98] Sněmovní tisk 81/0. Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva. [online]. *Poslanecká sněmovna ČR*, s. 72. [cit. 11. 10. 2022]. https://www.psp.cz/sqw/text/orig2.sqw?idd=90888

[99] Srov. např. Harašta, J. *Právní aspekty kybernetické bezpečnosti ČR.* 2013, diplomová práce, Masarykova univerzita, Právnická fakulta, [vedoucí práce Polčák, Radim], s. 26.

následky. Podle Roberta S. Muellera[100] existují pouze dva typy společností – ty, které byly napadeny a ty, které budou napadeny. Ty se však sbíhají do jedné kategorie a v blízké budoucnosti budou existovat společnosti, které byly napadeny a společnosti, které budou napadeny znovu.[101] K takovému stavu je v některých odvětvích, pokud k tomu již nedošlo, alespoň velmi blízko.

Kybernetický útok lze definovat jako jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby.[102] Kybernetické útoky jsou stále častějším jevem. Útočníky zřejmě motivuje zejména vidina zisků, které může jejich nelegální činnost vynést, společně s určitou anonymitou, kterou umožňuje virtuální svět a která přináší nižší riziko odhalení a následného potrestání. Zároveň se tato trestná činnost zdá být mnohem pohodlnější a čistější než „klasické" protizákonné činy. A to i přes to, že je schopna způsobit rozsáhlejší dopady na majetek, zdraví i životy osob než běžný útok v realitě. Nezbytné však jsou velice dobré programovací a další schopnosti útočníka.

Od kybernetického útoku se odlišují pojmy – kybernetická bezpečnostní hrozba *(information security threat)*, událost *(security event)* a incident *(security incident)*. Užití těchto termínů může být problematické, neboť jsou často používány jako synonyma. Hlavní rozdíl těchto negativních jevů spočívá ve stádiu vývoje a stupni závažnosti, které v kyberprostoru vyvolávají.

Kybernetická bezpečnostní hrozba (Information Security Threat) je *„potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv"*.[103] S tímto termínem splývá kybernetická událost, která je popsána v ustanovení § 7 odst. 1 ZKB jako *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elek-*

[100] Robert Swan Mueller III (*7. 8. 1944) je americký právník a vládní úředník. V letech 2001–2013 zastával funkci ředitele FBI.

[101] RSA Conference. RSA Conference 2012 Keynote – Combating Threats in the Cyber World – Robert S. Mueller, III [online]. *youtube.com.* 2. 3. 2012, 19:47–20:04. [cit. 31. 10. 2022]. https://www.youtube.com/watch?v=MGMOW7nLGvY

[102] Kolouch, J., Bašta, P. a kol. CyberSecurity. Praha: CZ.NIC, 2019, s. 82. https://knihy.nic.cz/files/edice/cybersecurity.pdf

[103] Jirásek, Novák, Požár. *Výkladový slovník kybernetické bezpečnosti*, s. 53.

tronických komunikací". Kybernetická hrozba se, jakožto potenciální příčina události, vývojově nachází před samotnou událostí a spouští ji. Dle některých autorů by bylo vhodnější a srozumitelnější používat pouze označení kybernetická hrozba.[104] Hrozby i události mohou vést k negativnímu následku, ale ani jedna z kategorií k němu nedochází. Jsou jen možnými příčinami, které se však rychle mohou změnit v reálný incident.

Kybernetický bezpečnostní incident označuje podle druhého odstavce výše zmíněného ustanovení ZKB *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací".* Tato fáze nastává v důsledku kybernetické bezpečnostní události a dochází při ní ke skutečnému narušení bezpečnosti kybernetického prostoru. Určitou část incidentů způsobují i náhodné jevy (vyšší moc), chyby hardwaru či softwaru, chyby uživatelů apod.[105] Lidský faktor je obecně považován za nejslabší a nejrizikovější článek celé soustavy kybernetické bezpečnosti, a to zejména v souvislosti s nedbalostním jednáním.

Vyhláška o kybernetické bezpečnosti kategorizuje bezpečnostní incidenty v ustanovení § 31. Incidenty se rozdělují do tří skupin podle významnosti při zohlednění např. počtu dotčených uživatelů, důležitosti dotčených aktiv, délky trvání či zeměpisného rozsahu dotčené oblasti. Dále je možné rozdělit je dle dopadu, a to na kybernetické bezpečnostní incidenty narušující důvěrnost aktiv, integritu aktiv či dostupnost aktiv. Možné jsou i kombinace těchto dopadů.

Pojem „kybernetický incident" je mnohem širší než „kybernetický útok". Zatímco k prvně jmenovaným může dojít i na základě nedbalostního jednání uživatele či vyšší moci, kybernetické útoky jsou projevem pouze cíleného úmyslného jednání útočníka.

Při útocích na české nemocnice byly dosud nejvíce destruktivní tzv. ransomware útoky. Ransomware je škodlivý program, který vnikne dovnitř systému a zašifruje data napadeného subjektu, po němž následně vyžaduje zaplacení výkupného pro odblokování.[106] Nejčastěji se pro-

[104] Srov. Kolouch, J., Bašta, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019, s. 81. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[105] Tamtéž, s. 82.

[106] Jirásek, Novák, Požár. *Výkladový slovník kybernetické bezpečnosti*, s. 78.

gram šíří e-mailem, kde je obsažen v příloze, po jejímž otevření se nainstaluje.[107] Proto je důležité školení zaměstnanců, aby dokázali rozeznat podezřelé zprávy a dále si jich nevšímali. Zprávy obsahující takový škodlivý kód mohou být rozesílány cíleně např. do e-mailových schránek konkrétní společnosti s cílem způsobit jí újmu, nebo náhodně na různé adresy různých osob s vidinou úspěšného činu alespoň u některého z obeslaných subjektů. Do povědomí veřejnosti se ransomware dostal zejména jeho využitím při nejzávažnějších útocích na tuzemská zdravotnická zařízení, a to na Nemocnici Rudolfa a Stefanie v Benešově v prosinci 2019, Fakultní nemocnici Brno 13. března 2020 a na Psychiatrickou nemocnici Kosmonosy pouhé dva týdny po úspěšném útoku v Brně.

Oblíbeným je i útok typu DoS (Denial of Service) či DDoS (Distributed Denial of Service), při němž dochází k připojení mnoha zařízení ke konkrétnímu serveru, což napadený systém nezvládá a dochází k jeho následnému pádu či nefunkčnosti a nedostupnosti pro ostatní uživatele.[108] Při těchto útocích nebývají ohrožena data pacientů, ale může utrpět samotné zdraví pacientů, kdy se lékaři kvůli nefungujícímu systému nemohou dostat např. k záznamům o pacientech a nemohou tak poskytnout řádnou péči.

V současné době je asi nejčastějším způsobem o pokus útoku tzv. phishing. Při něm jsou z uživatelů, pomocí podvodné zprávy šířené elektronickou komunikací lákány přihlašovací údaje, které jsou následně zneužity pro přístup do systému. Zprávy pro větší autentičnost obsahují prvky, aby co nejvíce napodobovaly důvěryhodného odesílatele (např. logo nemocnice, podpis apod.). Pro neúspěšnost těchto útoku je opět nejdůležitějším lidský faktor – proškolený zaměstnanec.[109]

3.5 Kritická (informační) infrastruktura

Kritická informační infrastruktura je *„zákonem vymezený komplex informačních systémů, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních*

[107] Lehto, M., Neittaanmäki, P., ed. *Cyber Security. Critical Infrastructure Protection.* Cham: Springer, 2022, s. 198.

[108] Jirásek, Novák, Požár. *Výkladový slovník kybernetické bezpečnosti,* s. 72.

[109] Tamtéž, s. 73.

potřeb obyvatelstva".[110] Jedná se o systémy, jejichž nedostupnost by výrazně omezila a ohrozila běžný chod současné společnosti.

Vymezení kritické infrastruktury nalezneme v krizovém zákoně, jehož ustanovení § 2 písm. g) tento pojem definuje 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".* Prvkem kritické infrastruktury se podle písm. i) stejného ustanovení rozumí *„zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií"*.

Průřezová a odvětvová kritéria pro určení prvků kritické infrastruktury upravuje nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Průřezová kritéria určují soubor hledisek, kterými se určuje závažnost vlivu narušení kritické infrastruktury. Tato kritéria jsou pro všechny oblasti stejná, spadá mezi ně hledisko obětí, ekonomického dopadu a dopadu na veřejnost,[111] přičemž nařízení ke každému z nich stanovuje mezní hodnoty, které je třeba splnit.

Odvětvová kritéria jsou určena v příloze ke zmíněnému nařízení. Z oblasti zdravotnictví je do této přílohy zařazena činnost poskytování zdravotních služeb a výroba léčivých přípravků, přičemž obě mají stanoveny mezní hodnoty, které musí být splněny, aby provozovatel pod danou úpravu spadal. Dále jsou mezi odvětvová kritéria zahrnuty i nouzové služby, do nichž je řazen mimo jiné i integrovaný záchranný systém – operační středisko zdravotnické záchranné služby.

Pro poskytování zdravotních služeb je určen limit, podle něhož je prvkem kritické infrastruktury zdravotnické zařízení, jehož celkový počet akutních lůžek je nejméně 2 500.[112] Tuto podmínku ovšem nesplňuje žádná z tuzemských nemocnic. Fakultní nemocnice v Motole, která je největším zdravotnickým zařízením v ČR, disponuje celkem 2 199

[110] Tamtéž, s. 15.

[111] § 1 písm. a) až c) nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

[112] Bod IV. písm. A. přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

lůžky.[113] Žádný tuzemský poskytovatel zdravotních služeb není tedy chráněn institutem kritické infrastruktury.

3.6 Poskytovatel základní služby

České zdravotnictví pod působnost ZKB vstupuje coby základní služba.[114] Tento pojem se do tuzemského právního řádu dostal implementací směrnice NIS a fakticky představuje vnitrostátní kritickou infrastrukturu,[115] jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností ve vybraných odvětvích.[116]

Porovnáme-li definici kritické infrastruktury s definicí základní služby, můžeme dovodit, že základní služba je mírnější kategorií, a to zejména s ohledem na zákonem předvídanou intenzitu dopadu případného narušení. Jejím úkolem je rozšíření působnosti ZKB o subjekty, u kterých není potřebné jejich zařazení do přísnější skupiny.

Provozovatelem základní služby je orgán nebo osoba, kterou určí NÚKIB na základě odvětvových a dopadových kritérií.[117] Tato kritéria pro oblast zdravotnictví jsou stanovena v 5. bodě přílohy k vyhlášce o kritériích pro určení provozovatele základní služby. Odvětvová kritéria jsou blíže určena druhem služby, druhem subjektu a jeho speciálními kritérii.

Ve zdravotnictví podléhá úpravě pouze jeden druh služby, a to poskytování zdravotních služeb, přičemž subjektem je poskytovatel zdravotních služeb podle zákona č. 372/2011 Sb., o zdravotních službách.

---

[113] Fakultní nemocnice v Motole v číslech [online]. *FN Motol.* [cit. 8. 3. 2023]. https://www.fnmotol.cz/o-nas/historie-a-soucasnost/fakultni-nemocnice-v-motole-v-cislech/

[114] § 2 písm. i) bod 5. ZKB.

[115] Mareš, D., Crháková, E. Zákon o kybernetické bezpečnosti a jeho aktuální novelizace [online]. *epravo.cz.* 17. 8. 2017. [cit. 8. 3. 2023]. https://www.epravo.cz/top/clanky/zakon-o-kyberneticke-bezpecnosti-a-jeho-aktualni-novelizace-106268.html

[116] § 2 písm. i) ZKB.

[117] § 2 písm. k) a 22a ZKB.

Pro určení povinných osob dle ZKB, má být zohledněna významnost poskytovaných služeb a dopad kybernetického bezpečnostního incidentu,[118] k jejichž určení vyhláška o kritériích pro určení provozovatele základní služby vyjmenovává speciální a dopadová kritéria.

Speciální kritéria jsou definována takovým způsobem, že je v daném odvětví naplní pouze významní provozovatelé služeb.[119] Dopadová kritéria mají zohlednit významnost následků kybernetického bezpečnostního incidentu na rozsah a kvalitu poskytování základní služby uživatelům, ekonomické a společenské činnosti a veřejnou bezpečnost, a vzájemnou závislost odvětví uvedených v § 2 písm. i) ZKB.[120] Dopadová kritéria stanovují hranici škod, kterou by mohl kybernetický incident způsobit.[121]

Odvětvová a dopadová kritéria pro oblast zdravotnictví byla rozšířena vyhláškou č. 573/2020 Sb. ze dne 17. prosince 2020. Tato novelizace vznikla na základě požadavku Asociace krajů a NÚKIB v ní rozšířil speciální kritéria druhu subjektu. Prostřednictvím tohoto kroku je od 1. ledna 2021 povinných 44 poskytovatelů zdravotních služeb.[122] To je sice oproti původním poskytovatelům navýšení, ovšem stále se jedná pouze o pár největších tuzemských poskytovatelů.

[118] § 22a odst. 1 ZKB.

[119] NÚKIB. Informace o institutu základní služby [online]. *nukib.cz.* 22. 12. 2022, s. 4. [cit. 8. 3. 2023]. https://www.nukib.cz/download/publikace/podpurne_materialy/Informace-o-institutu-zakladni-sluzby_v1.5.pdf

[120] § 22a odst. 1 písm. b) ZKB.

[121] NÚKIB. *Informace o institutu základní služby* [online], s. 5.

[122] Skutečnost, že je povinných 44 subjektů z oblasti zdravotnictví byla autorce sdělena v rámci rozhovoru s respondentem č. 3 (zástupce NÚKIB, viz přílohu B.3 Rozhovor s respondentem č. 3). Různé zdroje však uvádí jiné počty, např. 46 povinných subjektů (viz Mamrilla, F., Toman, Š. Kybernetická bezpečnost ve zdravotnictví [online]. *epravo.cz.* 9. 4. 2021. [cit. 8. 3. 2023]. https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html#_ftn3).

3.7 Poskytovatel regulované služby

K dalšímu rozšíření okruhu povinných subjektů mimo jiné i v oblasti zdravotnictví dojde v souvislosti se směrnicí NIS2. Nový zákon o kybernetické bezpečnosti, který má být v souvislosti se zmíněnou směrnicí přijat, sdružuje několik původních typů povinných osob a zavádí jedinou kategorii – poskytovatel regulované služby. Odvětví a kritéria, která pod tuto skupinu budou spadat, bude blíže určovat prováděcí vyhláška.

Zavedení tohoto univerzálního pojmu má praktický význam. Současná úprava, kde jsou regulovaná odvětví výslovně uvedena v textu zákona, neumožňuje zákonodárci ani NÚKIB pružně reagovat na dynamický vývoj společnosti a změny v důležitosti a vlivu upravených oborů.[123] Nová úprava má být co nejvíce flexibilní, aby dokázala reagovat na aktuální společenské potřeby.

Směrnice NIS2 se podle základního pravidla v článku 2 odst. 1 vztahuje na veřejné i soukromé subjekty, jejichž druhy jsou uvedeny v přílohách a které jsou velikostně považovány za střední podniky, nebo které překračují stropy pro střední podniky[124] (tj. velké podniky) a současně poskytují služby nebo vykonávají činnosti v rámci Unie. Z tohoto určení existují různé výjimky, které jsou uvedeny dále ve zmíněném článku.

Povinné subjekty jsou děleny do dvou kategorií – základní *(Essential)* a důležité subjekty *(Important)*.[125] Důvodem tohoto rozlišení, ke kterému dochází na základě důležitosti služby a velikosti subjektů, je přísnost regulace. Do prvně jmenované kategorie se řadí nejdůležitější a největší subjekty, na které jsou kladeny přísnější požadavky.

---

[123] NÚKIB. Odůvodnění zákona o kybernetické bezpečnosti [online]. *osveta.nukib.cz.* Verze 1.0 platná k 25. 1. 2023, s. 3. [cit. 15. 3. 2023]. https://osveta.nukib.cz/pluginfile.php/82880/mod_resource/content/1/1b_Oduvodneni_Zakon-o-kybernetickebezpecnosti.pdf

[124] Střední podniky a stropy pro střední podniky definuje čl. 2 přílohy k doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků. Střední podnik je dle tohoto doporučení podnik, který zaměstnává 50 až 250 osob a jehož roční obrat a/nebo celková roční rozvaha přesahuje 10 milionů EUR, ale roční obrat nepřesahuje 50 milionů EUR a/nebo roční bilanční suma nepřesahuje 43 milionů EUR.

[125] Čl. 3 směrnice NIS2.

Zdravotnictví je zařazeno mezi vysoce kritická odvětví v 5. bodě přílohy I směrnice NIS2. Poskytovatelé zdravotní péče jsou jednou ze tří skupin regulovaných druhů subjektů v tomto sektoru. Dalšími jsou referenční laboratoře EU a subjekty zabývající se výzkumem, vývojem anebo výrobou farmaceutických přípravků.

Na základě článku 3 odst. 1 písm. a) směrnice NIS2 budou největší zdravotnická zařízení, která překročí stropy stanovené pro střední podniky, podléhat přísnější regulaci, jakožto základní subjekty. V tomto sektoru bude zřejmě nejdůležitějším kritériem počet zaměstnanců. Z pohledu tohoto měřítka budou do kategorie základních subjektů spadat všechna zařízení s 250 a více zaměstnanci. Pro představu, evidenční počet zaměstnanců k 31. 12. 2021 v Nemocnici Blansko, která disponuje celkem 190 lůžky, činil 488.[126] Další zařízení s alespoň 50 zaměstnanci budou podléhat mírnější úpravě.

[126] Nemocnice Blansko. Výroční zpráva 2021 [online]. *nemobk.cz.* [cit. 15. 3. 2023]. https://www.nemobk.cz/download/vyrocni-zprava-2021/

4 Právní úprava

Jak bylo naznačeno výše, ochrana informací zjištěných při výkonu lékařské profese, resp. povinná mlčenlivost, byla historicky morální normou, jejíž porušení nebylo možné právně sankcionovat. S modernizací společnosti však bylo nutné zařadit tuto povinnost do právních řádů, aby případné narušení bylo státem vymahatelné.

Porušení lékařského tajemství však zdaleka nepředstavuje jedinou možnost narušení ochrany osobních údajů, s nimiž je ve zdravotnictví pracováno. Vzhledem k citlivosti pacientských dat, která v tomto odvětví zejména kolují, musí být k jejich ochraně přistupováno komplexně a široce. Za účelem zajištění této protekce vzniklo na unijní i tuzemské půdě několik předpisů, z nichž je nejvýraznější aktuálně účinné nařízení GDPR. Tato právní úprava se vztahuje k ochraně osobních údajů bez ohledu na jejich umístění. Použije se na osobní údaje vedené v jakékoliv podobě, listinné i elektronické.

Úprava kybernetické bezpečnosti tedy primárně nechrání osobní údaje v kybernetickém prostoru. Hlavním cílem je ochrana samotného kybernetického prostředí, před neoprávněnými zásahy. Ochranu dat, zahrnující i osobní údaje, lze považovat za sekundární předmět regulace, neboť kybernetický prostor, resp. systémy, které se v něm nacházejí, je nezbytné chránit zejména kvůli informacím, které obsahují.

Zdravotnictví lze považovat za jedno z odvětví, na kterých se technologický pokrok podepsal nejvýrazněji. Prošel zde od jednoduchých, dalo by se říci kancelářských úkonů, mezi které lze zařadit například elektronické vedení zdravotnické dokumentace, až po složité medicínské úkony, kterými jsou nejrůznější operace pomocí robotů či jiných zařízení ovládaných počítači a podobné. Jedná se tedy o velké množství důležitých a velmi citlivých dat, která jsou získávána téměř u všech činností v rámci zdravotnictví a která se pohybují v informačních systémech zdravotnických zařízení či jsou předávána dále.

Vzhledem k citlivosti osobních údajů a důležitosti péče poskytované ve zdravotnictví, ale také s ohledem na výhody, které přináší moderní technologie, je nezbytné chránit nejen samotné osobní údaje, ale i kybernetický prostor, v němž je s těmito informacemi čím dál častěji pracováno. O znemožnění přístupu do informačních systémů mají usilovat technická a organizační opatření, která jsou regulována směrnicí NIS a tuzemským ZKB.

Využívání kybernetického prostoru je tedy v silném vzestupu. Reakce nadstátních organizací a států na tento aktuální celospolečenský jev je proto bezesporu nutná. Následující podkapitoly se budou věnovat stěžejním unijním a vnitrostátním právním předpisům, které se dotýkají kybernetické a informační bezpečnosti ve zdravotnictví. Vyjma předpisů, které se řadí do ústavního pořádku České republiky.

4.1 Unijní předpisy

4.1.1 Nařízení GDPR

Přímo aplikovatelné, obecně závazné nařízení GDPR *(General Data Protection Regulation)* cílí na evropské půdě ke zvýšení ochrany osobních dat fyzických osob. Podobu tohoto předpisu, který byl přijat jako nařízení, lze zdůvodnit zejména zvýšeným objemem toků osobních údajů, které mají přeshraniční charakter.[127] Proto vznikl zájem na odstranění roztříštěnosti a existenci jednotné právní úpravy této problematiky, která ovšem přece jen v některých případech ponechává členským státům prostor pro určité modifikace.[128]

Jak lze dovodit již z názvu, mezi hlavní účely nařízení GDPR patří posílení ochrany základních práv, především práva na ochranu osobních údajů. Dle čl. 1 odst. 1 stanoví nařízení pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla ohledně volného pohybu osobních údajů. Práva dotčených fyzických osob jsou rozvíjena a posilována ve dvou složkách: 1) právo mít a získávat informace o tom, které údaje jsou zpracovávány a proč, 2) právo domáhat se dodržování pravidel (vč. nápravy stavu).[129]

Vhodné je také zmínit, že nařízení GDPR nepřineslo zcela novou úpravu, ale nahradilo předchozí úpravu obsaženou v směrnici 95/46/ES. Mezi nejpodstatnější nové povinnosti, které přineslo nařízení GDPR, adresované mimo jiné i poskytovatelům zdravotních služeb patří povinnost

---

[127] Melotíková, P. *Osobní údaje v kontextu GDPR.* Praha: Leges, 2020, s. 60.

[128] V České republice nařízení GDPR upřesňuje a rozvíjí adaptační ZZOÚ – viz kapitola 4.2 Vnitrostátní předpisy.

[129] Úřad pro ochranu osobních údajů. Obecné nařízení o ochraně osobních údajů (GDPR) [online]. *uoou.cz.* [cit. 27. 9. 2022]. https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938

jmenování pověřence pro ochranu osobních údajů, vytvoření záznamů o činnostech zpracování, posouzení vlivu na ochranu osobních údajů, případně konzultace s dozorovým úřadem, a povinnost zabezpečení a hlášení bezpečnostních incidentů, o nichž bude hovořeno v následující kapitole.[130]

4.1.2 Směrnice NIS a NIS2

V oblasti kybernetické bezpečnosti je bezesporu nejvýznamnější směrnice NIS. Tato směrnice položila základ kybernetické bezpečnosti na unijní úrovni. Jejím úkolem je dle čl. 1 odst. 1. *„dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů v rámci Unie s cílem zlepšení fungování vnitřního trhu“.* Členské státy ji měly povinnost implementovat do 9. května 2018.

Směrnice NIS stanovila povinnosti jednak pro členské státy a jednak pro povinné subjekty. Státy měly za úkol přijmout národní strategii pro bezpečnost sítí a informačních systémů, zřídit centrální orgán na řízení kybernetické bezpečnosti, zřídit bezpečnostní tým typu CSIRT (*Cyber Security Incident Response Team*), který má za úkol budovat důvěru a podporovat rychlou a účinnou operativní spolupráci mezi členskými státy,[131] ustanovit Skupinu pro spolupráci, která má spíše strategickou úlohu a Skupinu CSIRT, ve které by se měla budovat operační spolupráce se všemi CSIRT týmy, které v daném státě fungují.[132]

Směrnice NIS rozděluje subjekty, jimž ukládá povinnosti na provozovatele základních služeb a poskytovatele digitálních služeb. Mezi provozovatele základních služeb spadají subjekty vyjmenované v příloze II k směrnici NIS. Mimo jiné i subjekty z odvětví zdravotnictví, které splňují další stanovená kritéria.[133] Povinnosti uložené provozovatelům základních služeb budou blíže rozebrány dále.[134]

---

[130] Viz kapitolu 5 Povinnosti dle nařízení GDPR.

[131] Čl. 1 odst. 2 písm. c) směrnice NIS.

[132] Duračinská, Z. Co přináší nová směrnice EU o síťové a informační bezpečnosti? *IT Systems.* 2016, roč. 18, č. 10, s. 46. Dostupné též z: https://www.systemonline.cz/it-security/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm

[133] Čl. 4 bod 4) směrnice NIS.

[134] Viz kapitolu 6 Povinnosti dle ZKB.

Druhá skupina povinných subjektů vznikla jako výsledek kompromisu, vztahuje se na ně menší množství povinností a státy by je neměly zatěžovat více povinnostmi, než které stanoví směrnice – tzv. princip maximální harmonizace. Hlavním cílem tohoto principu je, aby nedocházelo k přílišnému omezování trhu a domácí provozovatelé se tak nedostávaly do nevýhodného postavení oproti provozovatelům mimo Evropskou unii.[135]

Dne 16. ledna 2023 vstoupila v platnost směrnice NIS2, jejímž úkolem je prohloubit původní směrnici NIS z roku 2016. Nová unijní regulace směřuje k současné české úpravě, což zvýhodňuje tuzemské organizace, kterých se týkala již původní úprava, a pro které se toho v praxi příliš měnit nebude.[136] Změny v právních řádech členských států mají být provedeny do 17. října 2024.[137]

Směrnice NIS2 významně rozšiřuje okruh povinných subjektů. Kybernetická bezpečnost se bude zajišťovat u poskytovatelů více než šedesáti služeb z osmnácti odvětví. Hlavním kritériem pro zařazení do působnosti směrnice NIS2 je měřítko velikosti.[138] Cílem tohoto kroku je odstranění velkých rozdílů mezi úpravou jednotlivých členských států a zajištění právní jistoty pro všechny příslušné subjekty.[139]

Směrnice také předpokládá několik výjimek. Mimo jiné, že členské státy vztáhnou úpravu kybernetické bezpečnosti na subjekty, které poskytují služby vyčtené v přílohách, bez ohledu na jejich velikost pokud by např. narušení jejich služby mohlo mít významný dopad na veřejný pořádek, veřejnou bezpečnost či ochranu zdraví.[140]

Jak již bylo zmíněno výše, místo dosavadní roztříštěné úpravy několika kategorií s různými povinnostmi, jsou zavedeny dvě nové kategorie jedné povinné osoby, poskytovatele regulované služby. A sice „základní subjekt," který označuje nejdůležitější subjekty a bude tedy podléhat přísnější regulaci a „důležitý subjekt".

---

[135] Duračinská. *Co přináší nová směrnice EU o síťové a informační bezpečnosti?*, s. 47.

[136] NÚKIB. Nová směrnice EU o kybernetické bezpečnosti „NIS2" a návrh nového zákona o kybernetické bezpečnosti [online]. *osveta.nukib.cz.* [cit. 16. 3. 2023]. https://osveta.nukib.cz/mod/page/view.php?id=2582

[137] Čl. 41 odst. 1 směrnice NIS2.

[138] Viz kapitolu 3.7 Poskytovatel regulované služby.

[139] Recitál 7 preambule směrnice NIS2.

[140] Čl. 2 odst. 2 písm. c) směrnice NIS2.

V primární podobě spadají do kategorie základních subjektů velké podniky, které poskytují některou ze služeb uvedených v příloze I. Mezi důležité subjekty pak spadají všechny ostatní subjekty, na které se směrnice NIS2 vztahuje, to znamená střední podniky poskytující některou ze služeb z přílohy I a střední i velké podniky zabývající se službou uvedenou v příloze II.[141]

Z tohoto základního pravidla však existuje několik výjimek, které jsou uvedeny v článku 3 směrnice NIS2. Důležité je také zmínit, že směrnice obsahuje pouze minimální harmonizaci,[142] což umožňuje členským státům přijmout přísnější úpravu, minimálně však musí zachovat povinnosti stanovené směrnicí.

4.1.3 Další unijní předpisy

Z unijních předpisů bude dále zmíněno nařízení eIDAS,[143] jehož cílem je usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru. Nařízení mimo jiné vytvořilo standardy pro elektronickou identifikaci (elektronické podpisy, elektronické pečetě, elektronická časová razítka, aj.).[144] Tyto prostředky mají posílit důvěru v elektronické dokumenty a v celkovou elektronickou komunikaci.

Praktické využití nařízení eIDAS je možné nalézt například při poskytování přeshraniční zdravotní péče, kterou upravuje směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči.[145] Zde je důležité, aby zahraniční poskytovatel měl podrobné aktuální informace o zdravotním stavu pacienta. K výměně takových dat dochází prostřednictvím elektronické komunikace, k čemuž je nezbytná bezpečná identifikace a autentizace.

---

[141] Čl. 3 odst. 1 a 2 směrnice NIS2.

[142] Čl. 5 směrnice NIS2.

[143] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

[144] Čl. 1 nařízení eIDAS,

[145] Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči.

S tím blízce souvisí i problematika certifikace, která je regulována aktem o kybernetické bezpečnosti.[146] Na tento akt navazuje novelizace zákona o kybernetické bezpečnosti ze dne 20. července 2022. Úprava stanovila vnitrostátní orgán certifikace kybernetické bezpečnosti a pravidla pro sankce za porušení nařízení. Smyslem samotné certifikace je zvyšování důvěry v produkty, služby a procesy v oblasti informačních a komunikačních technologií skrze jejich bezpečnost.[147] Certifikace je podle aktu dobrovolná, nestanoví-li budoucí úprava jinak.[148]

4.2 Vnitrostátní předpisy

Z tuzemských předpisů považuji za vhodné nejprve zmínit ZZS, který je základním českým zákonem v oblasti zdravotnictví.[149] Mezi hlavní záležitosti, které ZZS upravuje, lze zařadit definici zdravotní služby a dalších základních pojmů, dále vymezuje vzájemná práva a povinnosti poskytovatelů zdravotních služeb a pacientů, či povinnosti poskytovatelů vůči správním orgánům a dalším subjektům. Úprava ZZS obsahuje povinnost lékařského tajemství, vedení a další nakládání se zdravotnickou dokumentací a definuje NZIS.

Prováděcími předpisy k ZZS vztahujícími se k problematice ochrany a manipulace s osobními údaji je vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci a vyhláška č. 373/2016 Sb., o předávání údajů do NZIS.

V souvislosti se ZZS a jeho aktuálně navrhovanou novelou týkající se elektrického vedení zdravotnické dokumentace[150] je nutné zmínit zákon č. 325/2021 Sb., o elektronizaci zdravotnictví. Jehož úkolem je zrychlit a zefektivnit procesy a zlepšit kvalitu a dostupnost lékařské péče. Ke splnění těchto cílů přinesl ucelený právní rámec pro základní infrastrukturu

[146] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

[147] Recitál 65 preambule aktu o kybernetické bezpečnosti.

[148] Čl. 56 odst. 2 aktu o kybernetické bezpečnosti.

[149] Mimo ZZS patří mezi hlavní zákony upravující oblast zdravotních služeb i zákon č. 373/2011 Sb., o specifických zdravotních službách a zákon č. 374/2011 Sb., o zdravotnické záchranné službě.

[150] Viz kapitolu 2.2 Zdravotnická dokumentace.

elektronizace zdravotnictví a vydefinoval role a odpovědnost subjektů. Zákon také představuje krok k umožnění budoucí mezinárodní spolupráce, neboť jednou z priorit Evropské komise je vytvoření tzv. Evropského prostoru pro zdravotní údaje (*European Health Data Space*, zkratkou *EHDS*), který má usnadnit výměnu různých typů zdravotních údajů a přístup k nim.[151]

Informační bezpečností se v tuzemském právním řádu zabývá ZZOÚ, který do vnitrostátních podmínek adaptuje nařízení GDPR a transponuje směrnici 2016/680.[152] Společně s tímto předpisem byl přijat i zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím ZZOÚ.

ZZOÚ upravuje například složení a činnost ÚOOÚ a dílčí záležitosti, které nejsou nařízením upraveny nebo které jsou přímo vyčleněny úpravě na vnitrostátní úrovni. Důležitými změnami oproti dřívější úpravě je například upřesnění věkové hranice dětí způsobilých k udělení souhlasu se zpracováním osobních údajů či posílení pozice veřejného zájmu. Správci, zpracovávající osobní údaje v takovém zájmu, mají omezenou informační povinnost vůči subjektům údajů. Celkově zvýhodněnou pozici mají správci jednající při plnění právní povinnosti či při výkonu veřejné moci.[153] Úprava ochrany osobních údajů není ani v českém právním prostředí zcela nová. ZZOÚ, který adaptuje nařízení GDPR, nahradil dřívější zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který implementoval směrnici 95/46/ES.

Kybernetické bezpečnosti se věnuje ZKB. Ten byl přijat v červenci 2014 s účinností od 1. ledna 2015, tedy ještě před vznikem unijní úpravy této problematiky. Poskytovatelé zdravotní péče se pod působnost ZKB

[151] Mašková, M., Kupcová, K. Zákon o elektronizaci zdravotnictví [online]. *epravo.cz.* 17. 5. 2022. [cit. 14. 10. 2023]. https://www.epravo.cz/top/clanky/zakon-o-elektronizaci-zdravotnictvi-114665.html

[152] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[153] Chlebus, T., Dostál, J. Nový zákon o zpracování osobních údajů [online]. *epravo.cz.* 30. 5. 2019. [cit. 17. 3. 2023]. https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

dostali transpozicí směrnice NIS, novelou č. 205/2017 Sb. Hlavním smyslem ZKB je ochrana funkčnosti kybernetického prostoru.[154] K jejímu zajištění zákon stanoví mimo jiné bezpečnostní opatření, povinnost hlášení bezpečnostních incidentů a jejich evidenci, způsob kontroly a nápravná opatření ukládaná při zjištění nedostatků.

Relevantními prováděcími předpisy k ZKB jsou vyhláška o KB a vyhláška o kritériích pro určení provozovatele základní služby. První jmenovaná blíže definuje například bezpečnostní opatření, bezpečnostní politiku a dokumentaci, kybernetický bezpečnostní incident a způsob jeho hlášení, provádění reaktivních opatření či likvidaci dat, provozních údajů a informací.[155] Druhá ze zmíněných vyhlášek byla blíže popsána v kapitole 3.6 Poskytovatel základní služby.

Kybernetické a informační bezpečnosti se věnuje velké množství dalších předpisů. Mimo unijní předpisy, zákony a podzákonné právní předpisy, existují také nejrůznější politiky, strategie, metodiky a další dokumenty, vydávané zejména NÚKIB, Úřadem pro ochranu osobních údajů, Národním bezpečnostním úřadem či Ministerstvem zdravotnictví.

4.2.1 Nový zákon o kybernetické bezpečnosti

Vstupem směrnice NIS2 v platnost začala členským státům běžet transpoziční lhůta 21 měsíců pro implementaci směrnice do vnitrostátních právních řádů. Ačkoliv má Česká republika kvalitně zpracovaný původní ZKB a pro současné povinné osoby se toho v praxi příliš měnit nebude,[156] rozhodl se NÚKIB pro přípravu nového aktu a jeho prováděcích předpisů.

Návrh zákona vychází z původního ZKB, splňuje minimální požadavky směrnice NIS2 a reflektuje dosavadní zkušenosti a poznatky z praxe. Cílem je zejména zjednodušení a dosažení přehlednosti právní

[154] Maisner, M., Vlachová, B. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015, s. 62.

[155] § 1 vyhlášky o KB.

[156] NÚKIB. Rada Evropské unie přijala znění nové směrnice NIS2 [online]. *nukib.cz.* 15. 12. 2022. [cit. 17. 3. 2023]. https://www.nukib.cz/cs/infoservis/aktuality/1923-rada-evropske-unie-prijala-zneni-nove-smernice-nis2/

úpravy.[157] Za tímto účelem vznikly v nové úpravě na místě původních několika kategorií povinných osob, pouze dvě kategorie, do nichž může být poskytovatel regulované služby zařazen.[158] Kritéria pro určení samotného poskytovatele bude udávat vyhláška o regulovaných službách.

Jak již bylo zmíněno, tuzemská právní úprava kybernetické bezpečnosti je zpracována kvalitně a pro již povinné subjekty nedojde k velkým změnám. I přes to směrnice NIS2 zavedla několik novinek, které jsou dosud neznámé i pro český právní řád. Jedná se například o povinné vzdělávání vedení organizací a jejich větší odpovědnost za zajišťování kybernetické bezpečnosti, povinnost ověřování dodavatelského řetězce či výrazně vyšší pokuty za nedodržení povinností.

Vedle uvedené vyhlášky o regulovaných službách musí vzniknout další prováděcí předpisy. Mimo již zmíněnou vyhlášku o regulovaných službách jsou navrhovány vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností či nižších povinností a dále vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony, o nepominutelných funkcích stanoveného rozsahu a o kritériích rizikovosti dodavatele.[159]

Dne 19. června 2023 byl návrh nového ZKB zaslán k meziresortnímu připomínkovému řízení. V účinnost by měl zákon vstoupit v říjnu 2024 po uplynutí transpoziční lhůty.

---

[157] NÚKIB. *Nová směrnice EU o kybernetické bezpečnosti „NIS2" a návrh nového zákona o kybernetické bezpečnosti.*

[158] Viz kapitolu 3.7 Poskytovatel regulované služby nebo kapitolu 4.1.2 Směrnice NIS a NIS2 .

[159] Úřad vlády ČR. Návrh zákona o kybernetické bezpečnosti. Návrh prováděcích právních předpisů [online]. *odok.cz.* Datum autorizace 19. 6. 2023. [cit. 26. 8. 2023]. https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/

5 Povinnosti dle nařízení GDPR

Jak již bylo uvedeno, ve zdravotnictví se pracuje s velkým množstvím osobních údajů, z nichž největší část je tvořena tzv. pacientskými daty vedenými ve zdravotnické dokumentaci. Tato data – informace o zdravotním stavu, podléhají zvýšené ochraně jakožto zvláštní kategorie osobních údajů a mohou mít schopnost poškodit nejen konkrétní fyzickou osobu, ale v některých případech i její nejbližší rodinné příslušníky, o nichž může být ve zdravotnické dokumentaci taktéž zmínka. Aby se minimalizovalo riziko úniku dat a jejich případného zneužití a rovněž podpořilo dodržení práva na soukromí a informační sebeurčení, musí poskytovatelé zdravotních služeb a jejich zaměstnanci ctít zásady zpracování osobních údajů a plnit zákonem stanovené povinnosti.

V následující podkapitole budou stručně rozebrány zásady, které sice byly známy již předchozí právní úpravě ochrany osobních údajů, ale nebyla zakotvena povinnost jednat v souladu s nimi. Dále budou rozebrány čtyři, dá se říci nejvýraznější povinnosti, které nařízení GDPR poskytovatelům zdravotní péče uložilo. Většina dalších povinností, které v této práci nebudou zmíněny, korespondují s právy subjektů údajů.[160]

5.1 Povinnost jednat dle zásad GDPR

Osoby povinné dle nařízení GDPR jsou při plnění závazků, vyplývajících z tohoto obecně závazného předpisu, povinny jednat v souladu se zásadami, na kterých je ochrana osobních údajů vystavena. Tyto zásady jsou definovány v čl. 5 nařízení GDPR a *„měly by se uplatňovat na všechny informace týkající se identifikované či identifikovatelné fyzické osoby“*.[161]

Jak bylo naznačeno výše, zásady vymezené v nařízení GDPR nebyly pro právní řád nové. Většina z nich byla vyjádřena jako jednotlivé povinnosti již v předchozí unijní právní úpravě směrnice 95/46/ES. V nařízení GDPR se změnilo jejich pojetí, kdy jsou vyjmenovány jako zásady zpracování osobních údajů.[162] Zavedena byla také zásada odpovědnosti

[160] Viz zejména Kapitola III Práva subjektu údajů (tj. čl. 12 a násl.) a čl. 80 a 82 nařízení GDPR.

[161] Recitál 26 preambule nařízení GDPR.

[162] Žůrek, J. *Praktický průvodce GDPR.* Olomouc: Anag, 2017, s. 58.

správce[163] za jejich dodržení, včetně povinnosti být schopen takový soulad doložit.[164]

První ze zásad ukládá nutnost zákonného,[165] korektního a transparentního způsobu zpracování údajů. Musí se tedy jednat o postup, který je především souladný s právními předpisy a i samotné získávání osobních údajů se musí opírat alespoň o jeden ze zákonných důvodů. Zpracování musí být taktéž věcně správné a ohleduplné. Mělo by zohledňovat zájmy a očekávání dotčených osob, nemělo by využívat jejich mylných představ.[166] Transparentnost vyžaduje snadný přístup, srozumitelnost a použití jasných a jednoduchých jazykových prostředků při sdělování informací subjektu údajů.[167]

Dle druhé, zásady účelového omezení je osobní údaje možné shromažďovat pouze pro určité, výslovně vyjádřené a legitimní účely, které musí být známy již v okamžiku sběru dat. V souladu s účelem shromáždění je nezbytné je i dále zpracovávat. Pozdější změna účelu je možná, není-li neslučitelná s původním, a existuje-li pro to zákonný podklad.[168] V základní rovině není tedy možné s jedním záměrem údaje shromáždit a s jiným zpracovávat.

Zásada minimalizace údajů zabraňuje správci požadovat od subjektů více údajů než je s ohledem na účel shromáždění nezbytně nutné. Lze v ní spatřovat i bezpečnostní prvek, neboť čím méně osobních údajů je zpracováváno, tím menší riziko hrozí v případě jejich úniku.[169]

Další je zásada přesnosti osobních údajů, která vyžaduje i případnou aktualizaci údajů. Povinností správce je s ohledem na účel zpracování přijmout veškerá rozumná opatření k tomu, aby byly chybné údaje vymazány či opraveny. K těmto krokům má přistoupit v případě, kdy si sám všimne zřejmých nejasností nebo na žádost subjektu údajů.[170] Není tedy vyžadována aktivní vyhledávací činnost správce.

---

[163] Definice správce je obsažena v čl. 4 odst. 7 nařízení GDPR.

[164] Čl. 5 odst. 2 nařízení GDPR.

[165] Zásada zákonnosti zpracování je podrobněji rozebrána v čl. 6 nařízení GDPR.

[166] Navrátil, J. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018, s. 40.

[167] Zejména recitály 39 a 58 preambule a čl. 13 nařízení GDPR.

[168] Navrátil. *GDPR pro praxi,* s. 41.

[169] Žůrek, J. *Praktický průvodce GDPR*, s. 61.

[170] Tamtéž.

Zásada omezení uložení vyjadřuje povinnost zlikvidovat osobní údaje, jakmile pomine účel jejich zpracování. Tato zásada se vztahuje na informace umožňující identifikaci subjektu. Likvidace tedy může být provedena i převedením dat do anonymizované podoby, což umožňuje možnost dalšího využívání takových údajů.[171] Související je i tzv. právo na výmaz či právo být zapomenut, které se v tomto případě uplatní z důvodu zániku potřeby údajů pro účel, pro který byly shromážděny.[172]

Nakonec je založena potřeba integrity (celistvosti) a důvěrnosti, dle které by měla být zajištěna přiměřená bezpečnost údajů. To se promítá do nezbytnosti užití vhodných technických či organizačních opatření chránících osobní údaje před neoprávněnými interními i externími zásahy a jinými hrozbami.[173]

5.2 Záznamy o činnostech zpracování

Každý správce a zpracovatel[174] (případně jejich zástupce) má povinnost vést záznamy o činnostech zpracování. Ty lze popsat jako soubory dokumentů, které popisují všechny procesy zpracování, které povinná osoba uskutečňuje a za které je zodpovědná. Jejich obsahem nemají být detailní informace o každodenních činnostech, nýbrž údaje o základních procesech, které jsou schopny poskytnout obecný přehled.[175] Informace, které je nutné zaznamenávat, jsou přímo vyjmenovány v nařízení GDPR.[176]

Tato povinnost vyplývá zejména ze zásady odpovědnosti, dle které je správce povinen prokázat a doložit, že provádí zpracování v souladu s obecnými zásadami.[177] Kromě jejich využití za účelem kontroly ze strany úřadu, slouží také pro interní potřeby a jednodušší orientaci v rámci procesů zpracování.

---

[171] Tamtéž, s. 62.

[172] Čl. 17 odst. 1 písm. a) nařízení GDPR.

[173] Navrátil. *GDPR pro praxi,* s. 43.

[174] Definice zpracovatele je obsažena v čl. 4 odst. 8 nařízení GDPR.

[175] Jarolímková, A. Článek 30. In: Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021, s. 714–715.

[176] V čl. 30 odst. 1 pro správce a jeho případného zástupce, a v odst. 2 pro zpracovatele a jeho případného zástupce.

[177] Jarolímková. *Článek 30,* s. 713.

Tvorba záznamů o činnostech zpracování částečně nahrazuje dřívější oznamovací povinnost. Zásadním rozdílem je, že záznamy dle GDPR nejsou automaticky zasílány dozorovému úřadu,[178] ale jsou mu poskytnuty až na vyžádání.[179]

V čl. 30 odst. 5 nařízení GDPR je z této povinnosti vymezena výjimka, dle které se povinnosti nevztahují *„pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.“*

Výklad této odchylky může v praxi působit problémy, zejména z hlediska, zda postačí splnit jednu z podmínek nebo musí být naplněny všechny. Pokud by se však výklad přiklonil k nezbytnosti všech předpokladů, nebyla by tato výjimka nikdy aplikovatelná, protože i v případě zaměstnávání jednoho zaměstnance není zpracování jeho osobních údajů příležitostné.[180] Vzhledem k tomu, že ve zdravotnictví dochází především ke zpracování zvláštních kategorií údajů, nemůže zde být tato výjimka uplatnitelná.

5.3 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů, taktéž označované zkratkou „DPIA“ (*Data Protection Impact Assessment*) je povinen provést správce, jestliže *„je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a úče-*

[178] V České republice zastává tuto pozici pouze ÚOOÚ.

[179] Fiala, O., Grepl, J., Lichnovský, O. *GDPR. Hmotné a procesní aspekty prakticky.* Praha: C. H. Beck, 2019, s. 22.

[180] Janečková, E. *GDPR. Praktická příručka implementace.* Praha: Wolters Kluwer, 2018, s. 28.

lům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob."[181] Jeho cílem je vyhodnocení zejména původu, povahy, zvláštnosti a závažnosti rizika, výsledek by měl být následně zohledněn při výběru vhodných opatření.[182]

Předchozí úprava směrnice 95/46/ES tuto povinnost přímo neobsahovala, ovšem obecně používala přístup založený na riziku,[183] dle něhož musí správce, již od počátku plánování zpracování osobních údajů, brát v úvahu povahu, rozsah, kontext a účel zpracování a přihlížet k možným rizikům pro práva a svobody fyzických osob, k čemuž musí taktéž přizpůsobit zabezpečení osobních údajů.[184]

V souvislosti s touto povinností vznikla v článku 35 odst. 4 nařízení GDPR povinnost dozorového úřadu sestavit a zveřejnit seznam druhů operací zpracování, k nimž posouzení vlivu na ochranu osobních údajů musí být vypracováno.[185]

Pokud z posouzení vlivu na ochranu osobních údajů vyplyne vysoké riziko, které vhodnými opatřeními a s ohledem na dostupné technologie a náklady nelze zmírnit, měla by být před zpracováním zahájena konzultace s dozorovým úřadem.[186] Tato úprava sleduje jeden z hlavních cílů nařízení GDPR, a sice zajištění vysoké úrovně ochrany osobních údajů.[187] Povinnost předchozí konzultace se vztahuje pouze na nejzávažnější situace, což příliš nepřetěžuje dozorové orgány.

---

[181] Čl. 35 odst. 1 nařízení GDPR.

[182] Recitál 84 preambule nařízení GDPR.

[183] Uřičař, M. Článek 35. In: Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021, s. 800.

[184] Úřad pro ochranu osobních údajů. Nové přístupy a povinnosti [online]. *uoou.cz.* [cit. 10. 6. 2023]. https://www.uoou.cz/2-nove-pristupy-a-povinnosti/d-27268/p1=4744

[185] Demonstrativní seznam případů, při nichž je posouzení vlivu na ochranu osobních údajů nezbytné, obsahuje také čl. 35 odst. 3 nařízení GDPR. V odst. 5 tohoto článku je založena možnost sestavit seznam operací, při nichž naopak vypracování posouzení vlivu nutné není.

[186] Recitál 84 poslední věta preambule a čl. 36 odst. 1 nařízení GDPR.

[187] Novotná, K. Článek 36. In: Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021, s. 825–826.

5.4 Jmenování pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je soukromá osoba, jejímž hlavním úkolem je dohlížet na řádné zpracovávání osobních údajů v organizaci, v níž svoji funkci vykonává.[188] Pověřence bývá označován za „základní kámen odpovědnosti".[189, 190] Existence této funkce uvnitř organizace zvyšuje úroveň ochrany osobních údajů.

Tato role nebyla zcela novou, se jmenováním osoby pověřené ochranou osobních údajů počítal již čl. 18 odst. 2 bod 2. směrnice 95/46/ES. V české právní úpravě však nedošlo k jejímu zavedení, na rozdíl od některých jiných členských států (např. Německo či Slovensko). Pověřenci byli také ustavování v řadě centrálních institucí Evropské unie.[191]

Současná úprava nařízení GDPR stanovila tři situace, kdy je nezbytné pověřence jmenovat.[192] Také je možné přistoupit k jeho dobrovolnému jmenování. Ve dvou ze tří případů, kdy musí být pověřenec jmenován, je hovořeno o „hlavní činnosti" spočívající ve zpracování osobních údajů.[193] Tento pojem by však neměl být vykládán tak, aby vylučoval činnosti, kde zpracovávání údajů tvoří neoddělitelnou část činnosti.[194]

Například v případě nemocnice je hlavní činností poskytování zdravotní péče, nikoli zpracovávání osobních údajů. Ovšem k tomu, aby nemocnice mohla bezpečně a účinně poskytovat zdravotní péči, je ne-

[188] Fiala, Grepl, Lichnovský. *GDPR. Hmotné a procesní aspekty prakticky*, s. 33.

[189] Article 29 Data Protection Working Party. Guidelines on Data Protection Officers (‚DPOs'). WP 243 rev. 01 [online]. *commission.europa.eu.* 30. 10. 2017, s. 4. [cit. 10. 6. 2023]. https://ec.europa.eu/newsroom/article29/items/612048/en

[190] Toto označení provedla Pracovní skupina podle čl. 29 (označována jako Pracovní skupina WP29), v současné době nazývána Evropský sbor pro ochranu osobních údajů (*European Data Protection Board*, zkratkou *EDPB*). Úkolem EDPB je vydávat a veřejně diskutovat materiály, které mají maximálně vysvětlit jednotlivé části a oblasti nařízení GDPR.

[191] Žůrek. *Praktický průvodce GDPR,* s. 102.

[192] Vyjmenováno v čl. 37 odst. 1 nařízení GDPR.

[193] Čl. 37 odst. 1 písm. b) a c) nařízení GDPR.

[194] Article 29 Data Protection Working Party. *Guidelines on Data Protection Officers (‚DPOs'). WP 243 rev. 01* [online], s. 7.

zbytné, aby zpracovávala údaje o zdravotním stavu. Proto by tato zpracovatelská činnost měla být považována za jednu z hlavních činností nemocnic. Z toho důvodu musejí nemocnice pověřence jmenovat.[195]

V případě ambulantních poskytovatelů je tato povinnost dobrovolná. Jmenován může být i jeden pověřenec pro více správců či zpracovatelů, nebo může být tato pozice obsazena pomocí externího dodavatele.[196]

Ačkoliv jsou kladeny požadavky na odborné znalosti a schopnosti pověřence, nejsou tyto nikde blíže definovány. V čl. 37 odst. 5 nařízení GDPR je všeobecně stanovena potřeba profesních kvalit. Taktéž je zdůrazněna nezbytnost odborných znalostí práva, nutná praxe v oblasti ochrany osobních údajů a schopnost plnit úkoly stanovené v článku 39.

Mezi tyto úkoly je zařazena poradenská činnost, která je poskytovaná správcům či zpracovatelům a zaměstnancům, taktéž může být poskytovaná na požádání, jde-li o posouzení vlivu na ochranu osobních údajů a jeho monitorování. Pověřenec také spolupracuje s dozorovým úřadem a působí jako kontaktní místo. V neposlední řadě monitoruje soulad s právními předpisy z oblasti ochrany osobních údajů.

5.5 Ohlašování a oznamování případů porušení zabezpečení osobních údajů

Posledními povinnostmi, které zde budou uvedeny, jsou ohlašování a oznamování případů porušení zabezpečení osobních údajů dozorovému úřadů. Pojmy „ohlašování“ a „oznamování“ jsou legislativní zkratky, jejichž smyslem jsou obsahově odlišné povinnosti. Snad nejvýznamnějším rozdílem je skutečnost, že ohlašování probíhá vůči dozorovému úřadu a adresátem oznámení je samotný subjekt osobních údajů.[197]

---

[195] Tamtéž.

[196] Jak implementovat v ambulantní sféře Nařízení Evropského parlamentu a Rady 2016/679 [online]. *uzis.cz.* 31. 3. 2018, s. 7. [cit. 10. 6. 2023]. https://www.uzis.cz/res/file/gdpr/jak-implementovat-gdpr-v-ambulantni-sfere.pdf

[197] Fiala, Grepl, Lichnovský. *GDPR. Hmotné a procesní aspekty prakticky*, s. 44.

Porušením zabezpečení osobních údajů se rozumí takový zásah do zabezpečení, jehož důsledkem je *„náhodné nebo protiprávní zničení, ztráta, změna nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů"*.[198] Mezi dopady se tedy řadí jak úplná ztráta, respektive zničení, tak i ztráta kontroly nad sesbíranými informacemi, popřípadě další. Důležité je, že musí dojít k narušení zabezpečení a k tomu musí být případně dále splněny další podmínky.[199]

Narušeny mohou být tři základní vlastnosti bezpečnosti informací, a sice důvěrnost, integrita a dostupnost.[200] V případě narušení důvěrnosti se může jednat například o neoprávněné nahlížení do zdravotnické dokumentace či o poskytování informací o zdravotním stavu pacienta nekompetentní osobě. Integrita může být narušena například pozměněním informací o skutečném zdravotním stavu pacienta nebo údajů o podávané medikaci. To může v případě zdravotnictví vést k fatálním následkům, neboť na základě takto změněných informací může být pro pacienta zvolen chybný léčebný postup. K porušení dostupnosti může dojít buď úplnou ztrátou, ke které může dojít především smazáním či skartací dokumentů, nebo ztrátou přístupu k údajům, ke které dojde například zašifrováním nemocniční informační sítě.

Předchozí právní úprava směrnice 95/46/ES, jakožto i tuzemská úprava v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, neobsahovala povinnost hlášení či oznamování porušení zabezpečení, nýbrž pouze povinnosti k zajištění bezpečnosti zpracování.[201] Každopádně v některých státech na unijní půdě ohlašovací po-

[198] Čl. 4 odst. 12 nařízení GDPR.

[199] Např. předpokládané vysoké riziko pro práva a svobody fyzických osob v čl. 34 odst. 1 nařízení GDPR.

[200] Viz kapitolu 3.3 Kybernetická bezpečnost.

[201] Uřičař, M. Článek 33. In: Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021, s. 757.

vinnost v určité podobě existovala i před nařízením GDPR (např. v Německu a Itálii). V Nizozemsku byla dokonce známa povinnost ohlašovat veškerá porušení týkající se osobních údajů.[202]

Dle současné úpravy je ohlašování porušení zabezpečení vůči dozorovému orgánu prováděno vždy, *„ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.“*[203] Taková situace může nastat například v situaci, kdy jsou osobní údaje již veřejně dostupné a další zveřejnění tedy nepředstavuje pravděpodobné riziko pro dotčenou fyzickou osobu.[204]

V opačném případě je důležité náležité a včasné řešení, bez něhož se může začít rozvíjet riziko vzniku negativních následků pro fyzické osoby.[205] Nebezpečí nepříznivých důsledků nemusí hrozit pouze samotným subjektům osobních údajů, ale i jiným lidem, o nichž jsou v pacientově zdravotnické dokumentaci zmínky.

Pro ohlášení porušení je stanovena lhůta *„bez zbytečného odkladu a pokud možno do 72 hodin“* od okamžiku, kdy se správce o porušení dozvěděl.[206] Za takový okamžik *„by se měl považovat okamžik, kdy má správce dostatečnou jistotu, že došlo k bezpečnostnímu incidentu, který vedl k narušení zabezpečení osobních údajů*.“[207] Správce by však mohl tuto svoji povinnost ponechat náhodě. Z toho důvodu by měly být zavedeny interní postupy umožňující případné porušení odhalit a vyřešit.[208]

Nutnost oznámit porušení zabezpečení subjektu údajů bude docházet, vznikne-li pravděpodobnost následku v podobě vysokého rizika pro práva a svobody fyzických osob.[209] Cílem ustanovení je, rovněž jako

---

[202] Article 29 Data Protection Working Party. Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01 [online]. *commission.europa.eu.* 20. 8. 2018, s. 5. [cit. 10. 6. 2023]. https://ec.europa.eu/newsroom/article29/items/612052/en

[203] Čl. 33 odst. 1 nařízení GDPR.

[204] Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01* [online], s. 18.

[205] Vyplývá z recitálu 85 preambule nařízení GDPR.

[206] Čl. 33 odst. 1 nařízení GDPR.

[207] Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01* [online], s. 10–11.

[208] Tamtéž, s. 12.

[209] Čl. 34 odst. 1 nařízení GDPR.

u předchozí povinnosti, snaha zamezit újmě, která může vzniknout a určité zvýhodnění postavení subjektu, který má možnost uvědomit si hrozící či již nastalé škody a zvážit následné kroky, včetně případné právní ochrany.[210]

Podmínka vysokého rizika existuje, pokud porušení může vést k *„fyzické, hmotné nebo nehmotné újmě fyzických osob, u jejichž údajů bylo narušeno zabezpečení"*.[211] Jako příklad takové újmy lze zmínit například diskriminaci, poškození dobrého jména, či krádež nebo zneužití totožnosti. Je-li porušeno zabezpečení údajů mimo jiné o zdravotním stavu, mělo by se mít za to, že k takové újmě pravděpodobně dojde.[212, 213]

Oznámení má být učiněno za použití *„jasných a jednoduchých jazykových prostředků,"* pomocí nichž má být popsána povaha porušení zabezpečení a má obsahovat alespoň informace stanovené v nařízení GDPR.[214] Tyto požadované údaje představují minimální rozsah, který může být podle uvážení rozšířen.

Povinnost je nutné splnit bez zbytečného odkladu. Tato lhůta není blíže konkretizována, jako tomu je v případě hlášení dozorovému úřadu.

Primárním způsobem oznámení je přímé kontaktování dotčených subjektů (např. prostřednictvím e-mailové komunikace, SMS zprávy). Pokud by to však vyžadovalo nepřiměřené úsilí, musí být přistoupeno k vydání veřejného oznámení nebo k přijetí podobného opatření.[215, 216]

Veřejné oznámení je nutno provádět samostatně od jiných oznámení, aby bylo dostatečně jasné a transparentní. K tomu má docházet za pomoci prostředku, který *„maximalizuje pravděpodobnost řádného*

---

[210] Uřičař, M. Článek 33. In: Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021, s. 782.

[211] Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01* [online], s. 23.

[212] Tamtéž, s. 24.

[213] Viz recitály 75 a 85 preambule nařízení GDPR.

[214] Čl. 34 odst. 2 nařízení GDPR.

[215] Čl. 34 odst. 3 písm. c) nařízení GDPR.

[216] Například v situaci, kdy by bylo nezbytné kontaktovat velké množství fyzických osob.

sdělení potřebných informací všem dotčeným fyzickým osobám.“ Jako příklad lze uvést přímou zprávu, oznámení na internetových stránkách, výrazné bannery či inzeráty v tištěných novinách.[217]

[217] Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01* [online], s. 21.

6 Povinnosti dle ZKB

Informace, včetně osobních údajů jsou v současné době stále častěji zaznamenávány či převáděny do digitální podoby. V kybernetickém prostoru je s nimi poté dále manipulováno a může dojít i k jejich zneužití. Vzhledem k rizikům, která toto prostředí přináší, vznikla potřeba jeho regulace. V České republice k tomu došlo prostřednictvím ZKB, který byl později rozšířen o požadavky unijní směrnice NIS.

V případě odvětví, jako je právě například zdravotnictví, je v současné době bezpochyby potřebné využití informačních a komunikačních zařízení. Zajištění jejich provozu a provozu celého informačního systému, který tvoří, však nemusí být v silách samotného poskytovatele zdravotních služeb. V praxi proto velice často dochází k zajišťování těchto služeb prostřednictvím dodavatelských firem. Osoby kolem informačního systému lze navíc rozdělit na správce a provozovatele. Mohou tedy vzniknout až tři odlišné osoby.

Pro řádné plnění povinností při zajišťování kybernetické bezpečnosti a efektivní uplatňování případných sankcí, rozlišuje ZKB povinné subjekty základní služby, kam spadá i zdravotnictví, na správce a provozovatele informačního systému základní služby a samotného provozovatele základní služby.[218] Role správce a provozovatele informačního systému jsou důležitější než třetí zmiňovaná, neboť na nich je závislé skutečné fungování kybernetické bezpečnosti, což se odráží i v katalogu povinností vyčtených v ZKB. Předpis původně dopadal pouze na správce, což se však v praxi ukázalo jako problematické. Jak bylo zmíněno, správce a provozovatel informačního systému nemusí být jedna a táž osoba a v případě špatně nastavených vzájemných práv a povinností v outsourcingových smlouvách docházelo k situacím, kdy správce neměl kontrolu nad činností provozovatele, za kterou však ze zákona odpovídal a mohl být sankcionován výlučně on. Provozovatel se poté stával fakticky nepostižitelným.[219] Přitom je na první pohled zřetelný rozdíl a vliv obou rolí. Provozovatel má na starosti reálné fungování informačního systému a má tak i lepší přístup k plnění některých zákonných povinností, zejména těch technického rázu.

[218] § 3 písm. f) a g) ZKB.

[219] Polčák. *Právo informačních technologií*, s. 599–600.

Povinnosti jsou v ZKB definovány velmi obecně. To povinným osobám ponechává volnost ve volbě způsobů a prostředků pro jejich splnění a umožňuje případnou rychlou obměnu použitých nástrojů. Díky tomu mohou adresáti přizpůsobit technická a další opatření svým individuálním potřebám i efektivně reagovat na nenadálé změny v oblasti informačních technologií. S tím se pojí dva z celkem šesti principů, na kterých je ZKB vystaven.[220] Jedná se o princip technologické neutrality a princip autonomie vůle regulovaných subjektů.[221]

Princip technologické neutrality vztahuje zaměření zákonných povinností především k bezpečnosti fungování služeb, nikoli k obsahu přenášených informací.[222] Předmětem regulace ZKB tedy nejsou například projevy počítačové kriminality (např. šíření dětské pornografie), ale bezpečnost přenosu těchto informací. Dalším projevem tohoto principu je již zmiňovaná možnost užití různých technologií a postupů, kterými může být docíleno stanovených povinností, a které zákon konkrétně nedefinuje. Princip autonomie vůle regulovaných subjektů se mimo volnost ve výběru způsobů naplnění cílů projevuje v možnosti dobrovolného zapojení nepovinných subjektů do systému kybernetické bezpečnosti.[223]

Jak bylo naznačeno v úvodu kapitoly, ZKB ukládá subjektům s reálně vlivnějším postavením více povinností. Mezi ty, kterými jsou vázány osoby správce a provozovatele informačního systému základní služby patří povinnost zavést a provádět bezpečnostní opatření a zohlednit požadavky vyplývající z nich při výběru dodavatele, provádět reaktivní a ochranná opatření, oznamovat provedení reaktivních opatření a detekovat kybernetické bezpečnostní události. Poslední dvě povinnosti, a sice povinnost hlásit kybernetické bezpečnostní incidenty a kontaktní údaje zatěžuje mimo zmíněné osoby i samotného provozovatele základní služby.

---

[220] Parlament ČR, Poslanecká sněmovna. Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva [online]. *psp.cz.* 10. 1. 2014, s. 56. [cit. 11. 6. 2023]. https://www.psp.cz/sqw/text/orig2.sqw?idd=90888

[221] Mimo tyto dva principy je ZKB dále vystaven na principu ochrany informačního sebeurčení člověka, ochrany nedistributivních práv, minimalizaci státního donucení a principu bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství.

[222] Parlament ČR, Poslanecká sněmovna. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva*, s. 56–57.

[223] Tamtéž, s. 59.

Za účelem řádného naplňování ZKB, vzniká nově zvolenému provozovateli základní služby informační povinnost vůči správci a provozovateli svého informačního systému. Provozovatel základní služby je musí neprodleně a prokazatelně informovat o svém určení a o tom, že se stali povinnými osobami dle ZKB.[224]

6.1 Bezpečnostní opatření

Bezpečnostními opatřeními rozumíme *„souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru"*.[225] Jejich účelem je zajištění určité úrovně bezpečnosti informačních a komunikačních systémů, které by tak měly být připraveny na efektivní zvládání kybernetických bezpečnostních událostí a incidentů, a rovněž celkově odolnější vůči kybernetickým útokům.[226] Jedná se tedy o preventivní nástroje, která se dělí na organizační a technická.

Organizační opatření primárně cílí na nastavení politik a pravidel u subjektu, technická se věnují zejména zásadám pro nastavení informačních a komunikačních systémů a služeb.[227] Jako nejjednodušší příklady prvně jmenovaných lze uvést například zavádění různých směrnic, školení zaměstnanců v této problematice či zavedení pravidel pro tvorbu hesel. Zatímco se organizační opatření dotýkají zaměstnanců napříč organizací, technickými se zabývá zejména IT oddělení. Jsou jimi totiž technické prostředky, mezi něž se řadí například výběr a zavedení firewallů, antivirových programů a podobně.

Tyto dvě skupiny bezpečnostních opatření se navzájem doplňují a podporují. Nelze se tedy zaměřit a investovat pouze do technických opatření, jestliže zaměstnanci nemají podvědomí o bezpečnosti a byli by například ochotni sdělit své přístupové údaje cizí osobě. Zároveň se nelze spoléhat pouze na organizační opatření, neboť lidský faktor je považován za nejslabší článek a současně existuje mnoho způsobů, jak se dostat

[224] § 4a odst. 3 ZKB.

[225] § 4 odst. 1 ZKB.

[226] Parlament ČR, Poslanecká sněmovna. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva*, s. 74.

[227] Kolouch, Bašta, a kol. *CyberSecurity,* s. 281.

dovnitř systému, což by bylo nedostatečným technickým zabezpečením jen podpořeno. Zavedená bezpečnostní opatření musí být přiměřená k možným rizikům a úměrná ve vztahu k finanční a administrativní zátěži.[228] Minimální obsah a rozsah bezpečnostních opatření a obsah a strukturu dokumentace k nim stanoví vyhláška o KB.

ZKB ukládá správci a provozovateli informačního systému základní služby povinnost bezpečnostní opatření zavést a provádět v nezbytném rozsahu a vést o nich bezpečnostní dokumentaci.[229] Při výběru dodavatele služeb musí být navíc zohledněny požadavky z bezpečnostních opatření, které musí být zahrnuty do uzavírané smlouvy.[230] Tato úprava byla přidána na základě zkušeností z praxe a její dodržování nelze považovat za nezákonné omezení či neodůvodněnou překážku hospodářské soutěži.[231]

6.2 Detekce kybernetických bezpečnostních událostí a hlášení kybernetických bezpečnostních incidentů

Správce a provozovatel informačního systému základní služby musí detekovat kybernetické bezpečnostní události v informačním systému, který spravují či provozují.[232] V případě překvalifikování kybernetické události na kybernetický bezpečnostní incident vzniká uvedeným osobám i povinnost jejich hlášení.[233] Ta je v případě incidentů narušujících kontinuitu poskytování činnosti rozšířena i na provozovatele základní služby.

---

[228] Parlament ČR, Poslanecká sněmovna. Vládní návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. …/2017 Sb., a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Důvodová zpráva [online]. *psp.cz.* 23. 11. 2016, s. 44. [cit. 11. 6. 2023]. https://www.psp.cz/sqw/text/orig2.sqw?idd=120106

[229] § 4 odst. 2 ZKB.

[230] § 4 odst. 4 věta první ZKB.

[231] § 4 odst. 4 věta druhá ZKB.

[232] § 7 odst. 3 ZKB.

[233] § 8 ZKB.

Dvojí hlášení kybernetických bezpečnostních incidentů bylo zavedeno na základě poznatků z praxe, kdy správce či provozovatel informačního systému nemusí mít žádné povědomí o tom, jak se incident projevil na samotném provozu základní služby.[234] Mimo hlášení kybernetických incidentů osobami, kterým to ukládá zákon, je umožněno i dobrovolné hlášení nepovinnými osobami.[235]

Hlavní rozdíl mezi kybernetickou bezpečnostní událostí a incidentem je ve vývojovém stádiu. Zatímco kybernetická událost je pouze potencionální příčina, která může způsobit narušení bezpečnosti, kybernetický incident ji již narušuje a tím způsobuje negativní následek.

Postup při plnění těchto povinností upravuje vyhláška o KB. Při detekci podezřelé události je nutné ji zejména řádně zaznamenat a uchovat minimálně po dobu 18 měsíců.[236]

V případě určení kybernetického incidentu musí správce či provozovatel informačního systému zajistit jeho zvládání, přijímat opatření pro odvracení a zmírnění dopadu a vést o něm a jeho zvládání záznamy.[237]

Kybernetické bezpečnostní incidenty je nutné bezprostředně po jejich zjištění hlásit. Tato úprava je komplementární k existujícím informačním a ohlašovacím povinnostem podle jiných předpisů.[238] To znamená, že splnění této povinnosti žádným způsobem neovlivňuje povinnost splnit závazky vyplývající z jiných právních aktů.

Hlášení se podává na formuláři zveřejněném na internetových stránkách NÚKIB. Dle vyhlášky o KB má formulář obsahovat pouze základní informace, kterými jsou identifikace odesílatele a informačního a komunikačního systému, datum a čas zjištění a popis incidentu. Hlášení tedy neobsahuje žádné detailní či dokonce citlivé informace.

---

[234] Polčák. *Právo informačních technologií,* s. 608.

[235] § 8 odst. 6 ZKB.

[236] § 22 odst. 3 vyhlášky o KB.

[237] § 14 odst. 1 písm. h), i), k) vyhlášky o KB.

[238] Parlament ČR, Poslanecká sněmovna. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva*, s. 76.

V neposlední řadě je potřeba kybernetické incidenty prošetřit a určit jejich příčiny.[239] Postup při řešení je následně třeba vyhodnotit a stanovit nová či aktualizovat stávající opatření, což má přispět k zamezení toho, aby se již řešený incident opakoval.[240]

6.3 Provádění reaktivních a ochranných opatření

Reaktivní a ochranná opatření jsou společně s varováními řazena mezi opatření podle ustanovení § 11 ZKB. Opatření jsou dle odstavce prvního uvedeného ustanovení *„úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.“* Tato definice popisuje všechna tři opatření, která spolu fungují jako celek, a která mohou vznikat mimo jiné i na základě hlášení kybernetických bezpečnostních incidentů povinnými osobami.

Varování je jednostranné informování o hrozbě v kybernetické bezpečnosti prováděné ze strany NÚKIB. Důvodem k jeho vydání může být libovolné zjištění o hrozícím narušení integrity, důvěrnosti nebo dostupnosti dat.[241] Reaktivní opatření mají na takovou situaci okamžitě odpovídat, snaží se kybernetický bezpečnostní incident odvrátit či zmírnit jeho následky. Smyslem ochranných opatření je zvýšení kvality kybernetické bezpečnosti na základě zkušeností z vyřešených incidentů.[242]

Všechna opatření vydává NÚKIB. Reaktivní opatření je možné vydat jako rozhodnutí, které se zasílá konkrétním adresátům, popřípadě jako opatření obecné povahy směřující k neurčenému okruhu osob a orgánů.[243] Podobu opatření obecné povahy mají i ochranná opatření.[244]

---

[239] § 14 odst. 1 písm. l) vyhlášky o KB.

[240] § 14 odst. 1 písm. m) vyhlášky o KB.

[241] Polčák. *Právo informačních technologií*, s. 608.

[242] Parlament ČR, Poslanecká sněmovna. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva*, s. 78.

[243] § 13 odst. 1 a 3 ZKB.

[244] § 14 ZKB.

Povinné osoby, kterými opět jsou správce a provozovatel informačního systému základní služby, musí provádět reaktivní a ochranná opatření vydaná NÚKIB. Dále v případě reaktivních opatření vzniká adresátům závazek oznámit provedení a jeho výsledek. Náležitosti takového podání stanovuje vyhláška o KB a vzorový formulář, který je možné použít, je zveřejněn i na internetových stránkách NÚKIB.[245]

6.4 Hlášení kontaktních údajů

Poslední z povinností dle ZKB určených povinným osobám v sektoru zdravotnictví je hlášení kontaktních údajů a jejich změn. Ty se opět oznamují provozovateli národního CERT nebo NÚKIB. V odvětví zdravotnictví sdělují tyto informace povinný správce a provozovatel informačního systému a provozovatel základní služby NÚKIB, a to prostřednictvím formuláře zveřejněného na jeho internetových stránkách.

Tato povinnost umožňuje kromě evidence osob a orgánů také komunikaci neformálních i oficiálních informací a závazných individuálních právních aktů.[246] NÚKIB tedy prostřednictvím sdělených informací zasílá osobám a orgánům např. varování, ochranná či reaktivní opatření, pozvánky na různé akce a cvičení apod.

[245] Viz https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/.

[246] Parlament ČR, Poslanecká sněmovna. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva*, s. 79.

7 Kybernetická bezpečnost u poskytovatelů zdravotních služeb

V následující kapitole bude rozebrána aktuální situace v oblasti kybernetické bezpečnosti u vybraných poskytovatelů zdravotních služeb a pohled NÚKIB na stav kybernetické bezpečnosti ve zdravotnictví. Výzkumná část bude primárně zaměřena na oblast kybernetické bezpečnosti. Text bude věnován stanoveným požadavkům a právní úpravě, stručně bude zmíněn osobní pohled respondentů na novou právní úpravu obsaženou v směrnici NIS2. Dále bude prostor věnován nejčastějším cílům útočníků a nejběžnějším hrozbám. Taktéž budou popsány některé aspekty prevence a postup při napadení. Prostor části před závěrem bude vyplněn pohledem zástupce NÚKIB.

7.1 Cíle výzkumu, metodologie sběru dat a výběr respondentů

Tento výzkum měl za úkol získat názory a pohled odborníků, kteří se s problematikou kybernetické bezpečnosti ve zdravotnictví setkávají každodenně při výkonu svého zaměstnání a mohou ji tedy kriticky hodnotit. Cílem rozhovorů bylo zjištění stavu kybernetické bezpečnosti ve zdravotnictví pohledem odborníků v praxi, doplněn o pohled NÚKIB. Výzkumná část tedy měla nastínit skutečný stav v tuzemských nemocnicích.

K získání potřebných informací a naplnění stanovených cílů bylo zvoleno empirického výzkumu, který zkoumá vztah práva s jeho okolím. Tedy to, jakým způsobem právo účinkuje v praxi mimo jeho vlastní uzavřený systém. Poznatky se při tomto způsobu bádání získávají na základě pozorování či zkušenosti.

Vedle empirického výzkumu je vymezen výzkum doktrinální neboli teoretický. Ten se zabývá popisem práva, jeho vývojem a aplikací. Mimo tyto dva hlavní typy je rozlišován i výzkum, který kombinuje oba zmíněné, je jím výzkum kritický.[247]

[247] Smekal, H., Šipulová, K. Empirický právní výzkum. *Jurisprudence.* 2016, č. 6, s. 31–38.

Potřebné informace je možné získat formou kvantitativního či kvalitativního šetření. Hlavním rozdílem mezi těmito postupy je, že při kvantitativním přístupu je kladen důraz na získání dat od velkého množství respondentů, k jejichž zisku je typicky užíváno dotazníků, zatímco cílem kvalitativního šetření je získat podrobné a komplexní informace o výzkumném tématu od malého množství tázaných. Během kvalitativního bádání se typicky začíná výběrem tématu a určením základních výzkumných otázek, které se mohou v průběhu výzkumu, sběru či analýzy modifikovat nebo doplňovat.[248] Jedná se o tzv. polostrukturovaný rozhovor, který byl užit i během tohoto průzkumu.

Výhodou kvalitativního šetření je, jak již bylo naznačeno výše, že umožňuje určitý široký problém prozkoumat do hloubky a zjistit o něm maximální množství informací.[249]

7.2 Okruhy otázek a výběr respondentů

Výzkumná část byla rozdělena na tři části. Prostor prvních dvou částí byl věnován zástupcům zdravotnických zařízení a třetí část zástupci NÚKIB.

Pro vedení rozhovorů se zástupci zdravotnických zařízení byly sestaveny dva okruhy otázek. První se věnoval požadavkům na kybernetickou bezpečnost a právní úpravě. Druhá část se zaměřila na kybernetické hrozby, jejich prevenci a řešení případného útoku. Třetí sada otázek, dle možností korespondující s předchozími, byla určena pro zástupce NÚKIB.

Vzhledem k zaměření práce bylo nezbytné oslovit odborníky zaměstnané v některém ze zdravotnických zařízení spadajících mezi povinné subjekty dle současného ZKB. To zajistilo jejich dobrou znalost užití právní úpravy v praxi. Došlo tedy k oslovení dvou manažerů kybernetické bezpečnosti zaměstnaných u provozovatelů základní služby, přičemž u prvního z nich byl vedle manažera kybernetické bezpečnosti přizván k rozhovoru i pověřenec pro ochranu osobních údajů.

Pro přehlednost odpovědí budou tázaní z prvního zdravotnického zařízení pojmenováni hromadně jako „respondent č. 1“. Pouze v případě

[248] Hendl, J. *Kvalitativní výzkum: základní teorie, metody a aplikace. Čtvrté, přepracované a rozšířené vydání.* Praha: Portál, 2016, s. 46.

[249] Švaříček, R., Šeďová, K. *Kvalitativní výzkum v pedagogických vědách. Vydání druhé.* Praha: Portál, 2014, s. 24–25.

nutnosti jejich oddělení bude manažer kybernetické bezpečnosti tohoto zařízení označován jako „respondent č. 1A“ a pověřenec pro ochranu osobních údajů jako „respondent č. 1B“ (viz Tab. 1: Přehled respondentů).

Rozhovory s těmito osobami probíhaly osobně a s jejich souhlasem byly nahrávány na záznamník. Tázaným bylo nejprve představeno téma diplomové práce a vysvětleno, jak bude rozhovor zaměřen a jakým způsobem bude dále použit v rámci práce. Poté bylo přistoupeno ke kladení samotných otázek. Při vedení takových rozhovorů platí, že míra úspěšnosti rozhovoru a kvality získaných odpovědí se odvíjí od míry důvěry a otevřenosti respondentů.[250]

Dále byl osloven zástupce NÚKIB, který se vyjádřil k aktuálnímu stavu kybernetické bezpečnosti nejen v tomto sektoru a součinnosti NÚKIB se zdravotnickými zařízeními. Stejně jako prvním dvěma respondentům mu bylo popsáno téma práce, důvod vedení rozhovoru a způsob jeho následného použití. Výměna informací s tímto tázaným však probíhala výlučně prostřednictvím e-mailové komunikace.

Tab. 1: Přehled respondentů

Respondent č.		Pozice	Způsob komunikace
1.	A	Manažer kybernetické bezpečnosti	Osobně
	B	Pověřenec pro ochranu osobních údajů	Osobně
2.		Manažer kybernetické bezpečnosti	Osobně, korespondenčně doplněno
3.		Zástupce NÚKIB	Korespondenčně

7.3 Výsledky, vyhodnocení a interpretace

Po provedení potřebných schůzek s respondenty bylo nezbytné nahrané rozhovory přepsat do textové podoby. Text byl následně upraven a ze-

[250] Mišovič, J. *Kvalitativní výzkum se zaměřením na polostrukturovaný rozhovor.* Praha: SLON, 2019, s. 105.

stručněn, aby byla zachována zejména myšlenka odpovědi a názor respondenta. S respondentem č. 2, navíc po přepsání rozhovoru do textové podoby, proběhla e-mailová komunikace, během níž došlo k doplnění a upřesnění získaných odpovědí.

V následujícím textu jsou otázky rozděleny do tří částí. V prvních dvou částech s názvy *„Opatření dle ZKB a největší úskalí kybernetické bezpečnosti“* a *„Aktuální hrozby a postup při jejich řešení“* jsou stručně shrnuty odpovědi respondentů č. 1 a 2. Třetí část *„Pohled NÚKIB“* je věnována respondentovi č. 3. Základní otázka je vždy zvýrazněna a po ní následuje shrnutí odpovědi.

7.3.1 Opatření dle ZKB a největší úskalí kybernetické bezpečnosti

První okruh měl průřezově popsat technická a organizační opatření dle ZKB ve zdravotnických zařízeních, dále zmiňuje způsob vedení IT oddělení organizace a názor na novou právní úpravu směrnice NIS2.

Co musí Vaše zdravotnické zařízení splnit v oblasti kybernetické bezpečnosti? Co považujete za slabiny kybernetické bezpečnosti ve zdravotnictví?

Zde se respondenti nijak zvlášť překvapivě shodli na nutnosti minimálně naplnit zákonem, respektive vyhláškou, stanovené povinnosti, zejména organizační a technická opatření. Mezery při plnění těchto povinností spatřují zejména v personálním a finančním zajištění.

Respondent č. 1 upozornil na podstav IT zaměstnanců v sektoru zdravotnictví. Personální zajištění IT procentuálně vůči velikosti organizace se ve zdravotnictví pohybuje pod 1 % zaměstnanců v IT ze všech zaměstnanců. Například v bankovnictví to bývá 7–9 %. IT technici v nemocnicích navíc primárně zajišťují samotný provoz, jehož součástí je právě i kybernetická bezpečnost. Dalším nedostatkem může dle tohoto respondenta být i to, že určitou znalost má pouze jeden IT zaměstnanec a nikdo jiný. V okamžiku, kdy tento člověk není schopen plnit své povinnosti, vzniká problém.

Další skutečností je zaostání technologií ve zdravotnictví. Investice do těchto prostředků jsou vysoké, ale z celkového rozpočtu nemocnic bývá jen zlomek určen pro informační technologie.

Respondent č. 2 také vnímá nedostatek lidské síly a financí. Dle něj je nedostatek odborníků na kybernetickou bezpečnost obecný problém. Taktéž se dle něj naráží na rezistenci zdravotnického personálu, jehož hlavní pracovní náplní není kybernetická bezpečnost, ale se kterou se při výkonu svého zaměstnání setkává.

Co podle Vašeho názoru patří mezi nejdůležitější zákonné požadavky?

Za důležité považují respondenti vše, ovšem lze podle nich vyspecifikovat určité pořadí. Jako nejdůležitější a současně složité označili evidenci aktiv. Ke každému aktivu je nezbytné určit zodpovědné garanty a provést analýzu rizik. Primárními aktivy[251] lze dle respondenta č. 1 rozumět vše, kde jsou zjednodušeně např. pacientská data. Podpůrnými aktivy poté chápeme technologie, kterými jsou primární aktiva určitým způsobem zpracovávána.

Respondent č. 1B zde také upozornil na průnik do GDPR, kdy uvedl, že *„jednou ze základních povinností každého správce je vést tzv. záznamy o činnostech zpracování, což je de facto evidence procesu zpracování tam, kde jsou osobní údaje"*. Tyto dvě povinnosti splývají tam, kde jsou osobní údaje vedené v elektronické podobě. Mimo uvedené považuje respondent č. 1 za důležité také školení zaměstnanců.

Respondent č. 2 považuje za základní a jednodušší technické požadavky, které nezatěžují uživatele. Organizační povinnosti jsou dle něj také důležité, ovšem zastává názor, že *„k tomu nelze pouze vytvořit e-learning, který každý vyplní,"* ale fakticky nenahradí samotnou edukaci či upozorňování na novinky, které je pro zaměstnance přínosnější.

Největším základem odborníka na kybernetickou bezpečnost je dle něj naučení se a pochopení, jak daná nemocnice funguje. Což je zároveň to nejnáročnější.

[251] Primární aktiva jsou informace, procesy, činnosti, při jejichž narušení nemůže nemocnice plnit své povinnosti. (In: Čermák, M. Jak identifikovat primární a podpůrná aktiva a zachytit závislost mezi nimi [online]. *cleverandsmart.cz.* 12. 3. 2016. [cit. 13. 10. 2023]. https://www.cleverandsmart.cz/jak-identifikovat-primarni-a-podpurna-aktiva-a-zachytit-zavislost-mezi-nimi/

Kdo se v nemocnici stará o IT? Má nemocnice interní oddělení nebo využívá služeb dodavatelských firem (tzv. outsourcing)?

Zdravotnické zařízení, v němž je zaměstnán respondent č. 1 má IT oddělení kompletně interní, v čemž jsou dle vlastních slov v menšině. Dodavatelskými firmami mají řešeny pouze některé vedlejší záležitosti, například servis IT zařízení.

Respondent č. 2 uvedl, že v každé nemocnici musí být nějaké IT oddělení, minimálně jeden IT technik, který je schopen řešit aktuální problémy.

Výhodou řešení informačních záležitostí pomocí dodavatelských služeb, neboli prostřednictvím tzv. outsourcingu mohou dle respondenta č. 1 být ekonomické aspekty, nevýhodu pak spatřuje zejména při řešení mimořádných situací, kdy je nemocnice závislá na jiné firmě.

Úprava NIS2. Je podle Vašeho názoru nutná? Měla dle Vás přijít dřív? Změní se pro Vaše zdravotnické zařízení něco zásadního?

Vzhledem k nové úpravě směrnice NIS2, která má být do právních řádů členských států transponována nejpozději do 17. října 2024, byli respondenti vyzváni ke sdělení svých názorů na příchozí změny.

Respondent č. 1A se ve spojitosti s novou úpravou obává vyvolání podobného efektu, který způsobilo nařízení GDPR. Zejména jeho využití v komerční sféře, která se řešení nových povinností bude snažit zpeněžit. Hlavní změnou pro zdravotnické zařízení, v němž je zaměstnán, bude skutečnost, že se úprava bude nově vztahovat na celou organizaci.[252] Tím vznikne nová administrativa, což je dle jeho názoru poněkud kontraproduktivní.

Respondent č. 1B je názoru, že předpisy jako nařízení GDPR či směrnice NIS/NIS2 a podobné přišly pozdě. Další problém nastává při jejich přenosu do legislativ členských států, kdy zákonodárci nevyužijí toho, co jim tyto předpisy nabízí a mnoho věcí ponechají na vypořádání v praxi, přičemž mnoho odborníků poté neví, jak má postupovat.

Dle respondenta č. 2 je nová úprava nutná. Na evropskou úroveň a za účelem narovnání kybernetické bezpečnosti napříč členskými státy

[252] V současné době se dle slov respondenta č. 1A vztahuje úprava ZKB pouze na základní službu a vše kolem ní. Na podružné systémy, které nemají do základní služby dopad, není kladen takový důraz. NIS2 bude brát organizaci jako celek.

mohla dle jeho názoru přijít dříve. S ohledem na současný ZKB neočekává v nemocnici, ve které působí, zásadní změny. Za velký přínos považuje článek o zodpovědnosti vedení. Ten by měl zvýšit (nejen) v nemocnicích tlak na řešení této problematiky, neboť ne všude je kybernetické bezpečnosti přikládána taková důležitost, jako v místě jeho působiště.

7.3.2 Aktuální hrozby a postup při jejich řešení

Druhý okruh se zabývá kybernetickými hrozbami, se kterými se poskytovatelé v současné době nejvíce setkávají, postupem při jejich prevenci a případném následném řešení nastalých situací.

Na co se útočníci v současné době nejčastěji zaměřují (krádež dat či paralyzace nemocnice)?

Respondent č. 1 v současné době spatřuje velký zájem o pacientská data, s nimiž se obchoduje.

Dle respondenta č. 2 záleží na typu viru, a pokud by útočníkům šlo o paralyzaci nemocnice, muselo by jít opravdu o hodně cílený útok.[253] Na druhou stranu, jde útočníkům zejména o peníze, které nejlépe dostanou právě, když nemocnici paralyzují. *„Takovou situaci totiž musí vedení rychle vyřešit, a prvním a nejrychlejším řešením ve chvíli paniky je zaslání peněžního obnosu za účelem rychlého obnovení provozu.“* Poté však vzniká riziko, že hackeři budou požadovat další peníze. V případě krádeže dat, ovšem může nemocnice nadále fungovat a není vyvolán takový tlak na vyřešení situace, respektive zaslání peněz, jako v případě zašifrování nemocnice.

Která kybernetická hrozba je v současné době nejběžnější?

U kybernetických hrozeb se respondenti shodli, že nejběžnější jsou phishingové kampaně, které do e-mailových schránek chodí v podstatě neustále. Jejich vlastností je, že jednoduše dokáží zasáhnout velké množství zaměstnanců, resp. jejich e-mailových schránek.

[253] Dle respondenta č. 2 není pravidlem, že by hackeři útočili cíleně na nemocnice. Dle jeho slov: *„Jsou známé situace, kdy byla zašifrována dětská nemocnice. Hackeři poté zjistili, kam se dostali, odšifrovali ji a omluvili se. Zkrátka měli nějaký etický kodex.“*

Ransomware útok, ke kterému došlo např. v Brně Bohunicích, Ostravě či Benešově, považuje respondent č. 1 za fatální kybernetický útok, který vede k ochromení IT a v podstatě i celé instituce. Respondent č. 2 upozornil na nové hrozby, kterými je například využívání přihlášení přes vzdálenou plochu a známé jsou již také případy využití umělé inteligence k vytvoření viru schopného obejít i lepší způsoby zabezpečení.

Respondent č. 1 zmínil sofistikované útoky, které dokáží změnit integritu a důvěrnost dat. K tomu může dojít v evidenčních systémech, ale i u medicinských přístrojů. V evidenčních systémech může dojít ke změně pacientských dat, dle kterých může být poté pro pacienta zvolena špatná medikace. V případě medicínských zařízení lze průběh takového útoku demonstrovat na příkladu infuzních pump, při jejichž ovládnutí s nimi může útočník manipulovat takovým způsobem, že zařízení navenek sice ukazuje správná data, ale dávkují například dvakrát rychleji. Takových útoků se dle slov respondenta č. 1 v nemocnicích nejvíce obávají.

Jak ve Vašem zdravotnickém zařízení probíhá prevence kybernetických útoků? Jak probíhá školení zaměstnanců (např. prostřednictvím e-learningu či osobními školními)?

Dle respondenta č. 2 je nezbytné po technické stránce udržovat všechna aktiva, servery a další aktuální. Také je nutné vytvářet zálohy a kontrolovat jejich funkčnost. Zjištění případné nefunkčnosti v okamžiku problému je již pozdní.

Z organizačních opatření je důležitá edukace zaměstnanců. Ve zdravotnickém zařízení, kde působí respondent č. 1, probíhá edukace zejména prostřednictvím plošných e-learningových školení, které je nutné splnit, jak k problematice GDPR, tak i ke kybernetické bezpečnosti.

U některých zaměstnanců podle potřeby probíhají i osobní školení. Například respondent č. 1B školil v oblasti GDPR zdravotníky a výzkumníky pracující s daty, respondent č. 1A biomedicínské inženýry obsluhující zdravotní techniku, která má v současné době charakter IT zařízení.

Řízené phishingové útoky v současné době prováděny nejsou, neboť je respondent č. 1 názoru, že jsou zaměstnanci trénováni neustále probíhajícími skutečnými kampaněmi.

Respondent č. 2 považuje hromadné školení zaměstnanců v nemocničním prostředí za složité, až nereálné. Snaží se tedy, vedle e-learningového školení, zasílat e-maily s aktuálními hrozbami a provádět osobní

schůzky se zaměstnanci na odděleních. Obzvláště tyto osobní schůzky považuje respondent č. 2 za přínosné, neboť během rozhovoru se zaměstnancům může mnoho informací propojit i s osobním životem a jsou schopni si tak zapamatovat více poznatků.

Jaké první kroky musí nemocnice učinit po útoku? Existuje nějaký interní předpis? Jsou nějakým způsobem prováděny zkoušky takové situace?

Oba respondenti tuto otázku zodpověděli z jiného úhlu pohledu. Respondent č. 1 uvedl, že v jeho zdravotnickém zařízení existuje Odbor bezpečnosti a krizového řízení, který má na starost všechny krizové stavy. Tomuto odboru je podřízený Výbor pro kybernetickou bezpečnost.

Všechny postupy při mimořádných situacích jsou popsány v interních směrnicích, v nichž je mimo jiné vylíčen proces při opětovném zprovoznění vyřazených systému, včetně pořadí jejich obnovení.

Průběžná dílčí cvičení jsou v této nemocnici prováděna jedenkrát do roka. Taktéž zde probíhají zkoušky evakuačních plánů.

Respondent č. 2 se zaměřil přímo na interní předpisy. Sdělil, že postup v případě útoku popisuje Plán kontinuity činnosti, na který navazuje Havarijní plán, jehož obsahem je postup při obnově. Oba dokumenty je důležité průběžně zkoušet, čímž se zároveň mohou zdokonalovat. K takovému testování si stačí představit modelovou situaci a začít odříkávat postup při řešení, kdyby takový stav skutečně nastal.

Na co se dle Vašeho názoru budou útočníci v budoucnosti zaměřovat? Co považujete za příchozí hrozby?

Respondent č. 1 vidí hrozbu v umělé inteligenci a její aplikaci v kybernetických útocích. K automatizovaným útokům a k automatizované obraně to dle jeho slov již směřuje.

Respondent č. 2 je názoru, že útočníkům půjde stále o to stejné, a sice o peněžní prospěch, jehož zisk je u nemocnic jednodušší, neboť zde jde o lidské životy.

7.3.3 Pohled NÚKIB

Obsahem nyní předkládané části bude shrnutí pohledu zástupce NÚKIB (dále také označován jako „respondent č. 3“) na některé aspekty kybernetické bezpečnosti v odvětví zdravotnictví. Některé úseky navazují na výzkumné okruhy provedené se zástupci poskytovatelů zdravotních služeb.

Jak poskytovatelé zdravotních služeb přistupují k plnění zákonných povinností v oblasti kybernetické bezpečnosti? Co je v tomto ohledu největším problémem?

K zajišťování kybernetické bezpečnosti je dle názoru zástupce NÚKIB potřeba dlouhodobého a systematického přístupu. Obecně je problémem absence systematického přístupu, mezi jejíž nejčastější příčiny lze zařadit nedostatečné financování, nedostatek odborníků a nedostatečné bezpečnostní povědomí (proškolení) zaměstnanců.

Respondent č. 3 dále uvedl: *„Sektor zdravotnictví pracuje s citlivými daty nás všech a také proto je v ČR jedním z nejčastějších cílů kybernetických útoků (z pohledu sektorů, které spadají pod ZKB).“* Kybernetické zabezpečení zařízení ve zdravotnictví se sice zlepšuje, ovšem stále je právě ve zdravotnictví *„opravdu velký prostor ke zlepšení“.*

Jak je na tom české zdravotnictví po stránce kybernetické a informační bezpečnosti ve srovnání s jinými evropskými státy?

„Takováto porovnání se,“ dle respondenta č. 3, *„spíše neprovádí, a když už ano je otázkou, nakolik relevantní jsou jejich výstupy.“* Důvodem je mimo jiné rozdílný přístup k hodnocení, a to jednak v jednotlivých zemích, ale také mezi jednotlivými institucemi na národní úrovni. Problémem je také určení měřitelných kritérií a skutečnost, že každá organizace je do značné míry unikátní.

Úprava NIS2. Je změna nutná? Měla přijít dříve?

Změna je dle zástupce NÚKIB nutná, neboť *„nelze nereflektovat kontinuálně probíhající technologický vývoj“*. K druhé otázce uvedl: *„‚novelizace‘ směrnice přišla po přibližně 6 letech. Pokud chceme racionálně zhodnotit efekt takového předpisu, potřebujeme na to dostatečně dlouhou dobu.*

A 6 let je s přihlédnutím k transpozičním lhůtám z mého pohledu téměř minimum."

Respondent č. 3 také zmínil, že *„NIS2 není revolucí, ale evolucí".* Nová směrnice zejména prohlubuje a rozšiřuje původní směrnici NIS. Česká republika má výhodu, a sice v podobě kvalitně zpracovaného aktuálního zákona, neboť velká část příchozích změn je v souladu se systematikou českého ZKB.

Změní se s novým ZKB pro stávající povinné subjekty něco zásadního?

Pro povinné subjekty dle současného ZKB se nic zásadního měnit nebude. Zásadní změnou bude navýšení počtu regulovaných subjektů. Novinkou pak bude mechanismus na prověřování bezpečnosti dodavatelských řetězců, který se však bude týkat pouze asi 150 nejkritičtějších subjektů.

Máte odhad na kolik nových povinných osob ze sektoru zdravotnictví se nový ZKB bude vztahovat (v režimu základních i důležitých subjektů)? Nebudou povinnosti pro nové subjekty příliš zatěžující?

V sektoru zdravotnictví se předpokládá nárůst ze současných 44 subjektů na asi 1100 povinných subjektů.[254] Konečné rozdělení do dvou režimů je stále proměnlivé.

Při zvažování ukládané zátěže je nezbytné zohlednit citlivost dat, s nimiž se ve zdravotnictví pracuje a postup digitalizace tohoto sektoru. S tím musí souznít také bezpečnost. Respondent č. 3 tuto odpověď zakončil slovy: *„Pro toho, kdo věnuje otázce bezpečnosti zdravotnických dat dostatečnou pozornost již dnes, nebudou nové povinnosti zátěží."*

[254] Pokud jde o všechny regulované subjekty napříč odvětvími, očekává se dle respondenta č. 3 navýšení ze současných 400 subjektů na více než 6000 subjektů. (Viz přílohu B.3 Rozhovor s respondentem č. 3)

Jak NÚKIB přistupuje k prevenci kybernetických hrozeb? Liší se nějak prevence v oblasti zdravotnictví od prevence v jiných oblastech?

Respondent č. 3 zde uvedl, že NÚKIB v oblasti prevence a osvěty vykonává mnoho aktivit a činností. Mezi něž lze zařadit osvětové a vzdělávací činnosti napříč všemi sektory, spolupráci s národními i mezinárodními organizacemi, pořádání i účast na kybernetických cvičeních a mnohé další. Taktéž se věnuje dění v kybernetickém prostoru a všechny podněty průběžně vyhodnocuje a případně vydává upozornění, varování či jiná opatření.

V současné době se přístup NÚKIB k prevenci ve zdravotnictví od jiných sektorů neliší. K tomu však respondent č. 3 dodal, že *„po sérii mediálně známých incidentů z let 2019 a 2020 jsme zdravotnickým zařízením v následujících 2 letech věnovali abnormální pozornost po všech stránkách."* Z preventivních kroků stojí za zmínku například dva ročníky cvičení HealthCzech, audity a metodická pomoc v 16 největších nemocnicích či e-learning upravený pro potřeby zdravotnického personálu a další. Taktéž byl vydán minimální bezpečnostní standard, který se NÚKIB (bohužel marně) snažil zapracovat do legislativy o poskytování zdravotní péče.

Jak probíhají kybernetická cvičení? Jak často se provádějí?

Kybernetická cvičení dle respondenta č. 3 plní nezastupitelnou roli při zajišťování kybernetické bezpečnosti, neboť umožňují simulovat různé typy krizových situací a prověřují různé plány a postupy konkrétních organizací. Prostřednictvím čehož mohou být odhaleny a napraveny nedostatky.

Průběh a zaměření cvičení se odvíjí od toho komu je určeno a jaké požadavky jsou na něj kladeny. Různorodá je také jejich četnost. Jsou cvičení, která se opakují každý rok, ale také ta, která se odehrají pouze jednou. Například v roce 2022 se NÚKIB zapojil celkem do 10 mezinárodních a národních cvičení, a to jako cvičící, spoluorganizátor nebo organizátor.

Jak probíhá součinnost NÚKIB s napadenou nemocnicí při řešení kybernetického útoku a při řešení jeho následků?

Zde respondent č. 3 uvedl, že řešení bezpečnostních incidentů patří mezi stěžejní činnosti vládního CERT. Odborníci pomáhají napadené organizaci po technické stránce a poskytují rady pro další preventivní opatření. Tým CERT je schopen poskytnout celou řadu služeb, včetně komunikace se zahraničními partnery při řešení mezinárodních bezpečnostních incidentů. Poskytovaných služeb je dle slov tohoto respondenta celá řada, záleží na konkrétní situaci, ale také například i na zájmu zasažené organizace. Ve vážných případech vyráží CERT tým do napadené nemocnice, kde se po nezbytně dlouhou dobu stává součástí týmu řešícího incident.

Dále respondent č. 3 zmínil hlavní cíle takové podpory, kterými jsou poskytnout maximální možnou součinnost, minimalizovat škody a další negativní dopady (např. nedostupnost služby). Za klíčový aspekt při řešení kybernetických útoků označil včasnost zahájení komunikace, nahlášení incidentu či podezřelých událostí.

7.4 Závěry

V poslední podkapitole budou shrnuty nejzásadnější poznatky, se kterými se autorka shoduje. Tyto informace budou rozšířeny o její postřehy a názory. Pro zachování systematiky bude i tento text rozdělen na dvě části, a to podle dvou skupin otázek určených pro zástupce poskytovatelů zdravotních služeb, k nimž bude dle vhodnosti přiřazen pohled NÚKIB.

7.4.1 Opatření dle ZKB a největší úskalí kybernetické bezpečnosti

V oblasti kybernetické bezpečnosti je nezbytné alespoň naplnit zákon, zejména technická a organizační opatření. Technická opatření jsou jednodušší na zavedení, ovšem jsou finančně nákladné a při jejich nasazování jsou nezbytní IT odborníci.

Při zavádění organizačních opatřeních se naráží zejména na rezistenci zdravotnického personálu, jehož primárním úkolem je poskytovat zdravotní péči. Lidský faktor je ovšem nejslabším článkem při zajišťo-

vání kybernetické bezpečnosti, proto jsou organizační opatření nezbytná. V nemocničním prostředí navíc toto tvrzení, vzhledem k tlaku, který v tomto odvětví je, nabývá na síle.

Za největší problém při zajišťování kybernetické bezpečnosti, a to nejen v oblasti zdravotnictví, lze označit nedostatek odborníků a financí. Tyto nedostatky narušují systematičnost, která je vedle dlouhodobosti, jedním z prvků zajišťujících kvalitní kybernetickou bezpečnost.

Pro vyhovující kybernetickou bezpečnost je potřeba poskládat ji takovým způsobem, aby bylo hrozící riziko maximálně minimalizováno. Vzhledem k finanční náročnosti využívaných prostředků je nutné potřebné technologie zavádět postupně. Takové rozplánování je úkolem manažera a architekta kybernetické bezpečnosti, jejichž základní potřebou je pochopení, jak nemocnice funguje.

S ohledem na citlivost dat, s nimiž je ve zdravotnictví pracováno, a skutečnost, že se toto odvětví týká všech fyzických osob, je kybernetická bezpečnost ve zdravotnictví vážným tématem. A to především vzhledem k současnému technologickému vývoji. Zejména proto je současných 44 povinných osob dle ZKB ze sektoru zdravotnictví silně nedostatečných. I menší nemocnice okresního typu schraňují velké množství citlivých osobních údajů, a to jak v listinné, tak elektronické podobě. K razantní a potřebné změně dojde prostřednictvím nové právní úpravy, která tento počet navýší na asi 1 100 subjektů.

Dle respondenta č. 3 (zástupce NÚKIB) se pro nyní povinné osoby dle ZKB, mezi něž se řadí i respondenti č. 1 a 2, nic zásadního měnit nebude. To je důsledkem kvalitního tuzemského ZKB. Diskuze by se ovšem dala vést o zajištění zákonných povinností u velkého počtu nově určených subjektů, a to s ohledem na finanční i personální zajištění.

Největší novinkou, která se bude týkat všech povinných osob, bude zavedení článku o odpovědnosti vedení organizace. Další bude povinnost prověřování dodavatelského řetězce, ta se ovšem bude týkat pouze asi 150 nejkritičtějších subjektů napříč všemi sektory.

7.4.2 Aktuální hrozby a postup při jejich řešení

Nejčastějšími a také zřejmě nejjednoduššími jsou phishingové útoky, které v jednom okamžiku dokáží oslovit velké množství lidí. Lidský faktor je považován za nejslabší článek a v případě zdravotnických pracovníků je tato skutečnost s ohledem na vytíženost, tlak a náročnost této profese ještě posílena.

Respondenti č. 1 a 2 se rozcházeli v pohledu na zájem útočníků. Zatímco respondent č. 1 uvedl, že je enormní zájem o data, druhý respondent odpověděl, že útočníkům jde nejvíce o peníze. Autorka se zde přiklání k názoru respondenta č. 2. Lze se domnívat, že žádat výkupné přímo od napadeného nemocničního zařízení je pro útočníky jednodušší a rychlejší způsob. Tento postup je však i silně nemorální a bezcitný, neboť v tomto prostředí jde každopádně o zdraví a životy pacientů, což ovšem paradoxně může být jedním z důvodů úspěšnosti zisku financí. Každopádně i zisk informací vede opět k finančnímu prospěchu, neboť se stávají předmětem obchodu na černém trhu.

K prevenci kybernetických útoků slouží zejména školení zaměstnanců a technická zařízení. Autorka se při výzkumu zaměřila zejména na zvyšování bezpečnostního povědomí u zaměstnanců a opět se zde přiklání k respondentovi č. 2. Zatímco u zdravotnického zařízení prvního respondenta probíhá školení v oblasti GDPR a kybernetické bezpečnosti výlučně prostřednictvím plošného e-learningu a pouze v případě nezbytnosti jsou u konkrétních specifických profesí prováděna individuální školení. Respondent č. 2 provádí školení kombinací e-learningového kurzu, e-mailů s aktuálními informacemi a osobními setkáními s menší skupinou zaměstnanců. Je zřejmé, že v nemocničním prostředí je prakticky nemožné uspořádat velké hromadné školení. Ovšem školení jednou ročně prostřednictvím e-learningového kurzu autorka, i z vlastní zkušenosti, považuje za nedostatečné. Takový kurz je vhodný důkazní prostředek o tom, že školení dle zákona skutečně bylo provedeno, ale po stránce nabytých informací je mnohdy zcela neúčinné. Za užitečný lze považovat přístup respondenta č. 2, který zaměstnancům v průběhu roku zasílá e-maily s aktuálními hrozbami a kampaněmi, a také se s nimi schází při osobních setkáních. Dovolím si říci, že tento přístup má na zaměstnance daleko lepší a hlubší dopad než pouhé školení prostřednictvím e-learningu. Zaměstnanci jsou při takovém kontaktu, byť i prostřednictvím e-mailu, daleko pevněji propojení s realitou a mohou si tak i lépe představit případné hrozby nebo si to, co jim je sdělováno v rámci této komunikace dokáží propojit se zkušenostmi v osobním životě.

Při prevenci plní také nezastupitelnou roli různá cvičení, při nichž se zkouší postupy při řešení případného kybernetického útoku. Tyto zkoušky také umožňují odhalit případná slabá místa a odstranit zjištěné nedostatky, aby během případného útoku fungovalo vše, jak má. V ne-

mocnicích probíhají dílčí cvičení, při nichž je zkoušena funkčnost různých dokumentů, plánů nebo prováděných záloh. Větší cvičení probíhají i s pomocí NÚKIB, a to jak na tuzemské, tak i mezinárodní půdě.

Vzhledem ke specifičnosti všech organizací i pouze v rámci sektoru zdravotnictví, není možné vytvořit univerzální postup chování při kybernetickém incidentu. Důležité je mít zavedená všechna zákonná opatření, personál s kvalitním bezpečnostním vědomím a funkční a prozkoušené plány a postupy pro případ napadení zařízení. Pokud k takové situaci skutečně dojde je klíčovým aspektem včasné zahájení komunikace s NÚKIB.

8 Kontrola a sankce

Jak bylo popsáno v předchozích kapitolách, zdravotnická zařízení jako celek, ale i jeho zaměstnanci, musí k zajištění informační a kybernetické bezpečnosti plnit celou řadu zákonných povinností. Při jejich naplňování je nezbytné vnímat povahu a důležitost nemocničního prostředí i citlivost údajů, se kterými se zde především pracuje.

V následující kapitole budou popsány správní sankce za přestupky, kterých se mohou povinné osoby dopustit, pokud řádně nesplní povinnosti, které jim jsou zákonem uloženy. Ohled při tom bude brán zejména na povinnosti dle nařízení GDPR a ZKB, které byly rozebrány v kapitolách 5 a 6.

Vhodné je také uvést, že sankce uložené dle nařízení GDPR a ZKB jsou na sobě nezávislé a současné uložení pokut podle obou předpisů za nesplnění povinností týkajících se jednoho incidentu nebude porušením zásady *„ne bis in idem“.*[255, 256] Sankce by se společně zohledňovaly pouze, pokud by jako celek byly pro povinný subjekt likvidační.[257]

8.1 Správní sankce dle nařízení GDPR

Přestupky v oblasti ochrany osobních údajů podle nařízení GDPR či českého ZZOÚ projednává ÚOOÚ, který také vybírá a vymáhá stanovené pokuty. K tomu dochází podle ZZOÚ a dále podle zákona č. 250/2016 Sb. a zákona č. 500/2004 Sb.[258] Přehled správních sankcí, které lze uložit v případě porušení některé ze stanovených povinností, obsahuje přímo aplikovatelné nařízení GDPR v čl. 83 a 84. Mimo tuto úpravu vyjmeno-

[255] Brauner, J. *Ohlašovací povinnost dle GDPR a zákona o kybernetické bezpečnosti.* 2021, závěrečná práce, Masarykova univerzita, Právnická fakulta, [vedoucí práce Polčák, Radim], s. 39.

[256] Např. v situaci, kdy incident založí ohlašovací povinnost vůči ÚOOÚ i NÚKIB, musí povinný subjekt provést obě hlášení. Neprovede-li je, hrozí mu sankce. (In: Brauner. *Ohlašovací povinnost dle GDPR a zákona o kybernetické bezpečnosti,* s. 39).

[257] Tamtéž.

[258] Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich a zákon č. 500/2004 Sb., správní řád.

vává adaptační ZZOÚ možné přestupky v ustanoveních § 61–64. Tuzemská úprava ovšem není komplexní a obsahuje tedy především úpravu přestupků spáchaných v oblastech upravených ZZOÚ.[259]

Sankce by měly být ukládány za jakékoliv porušení povinností stanovených nařízením GDPR, a to z důvodu posílení prosazování stanovených pravidel. Nemusí se však vždy jednat o správní pokutu. V méně závažných případech, nebo pokud by pokuta představovala pro fyzickou osobu nepřiměřenou zátěž, může být uloženo napomenutí. V jednotlivých případech také musí být přihlédnuto k přitěžujícím či polehčujícím faktorům, mezi něž patří například povaha, závažnost a doba trvání porušení, úmyslný charakter či snaha o zmírnění škody.[260] Pokud dojde na uložení pokuty, měla by být účinná a přiměřená, ale současně odrazující.[261]

Nařízení GDPR rozlišuje dvě skupiny správních pokut. Dle ÚOOÚ odráží toto rozdělní *„důležitost porušených povinností, kdy ve skupině s vyšší sazbou jsou povinnosti, u jejichž porušení je očekávána vyšší intenzita zásahu do práva na ochranu osobních údajů, které obecné nařízení zajišťuje."*[262]

První skupina, stanovená v čl. 83 odst. 4 nařízení GDPR, umožňuje uložení pokuty do výše 10 milionů eur, nebo do výše 2 % celosvětového ročního obratu, jedná-li se o podnik. Této výše správní pokuty může dosáhnout porušení téměř všech povinností uvedených dříve v této práci,[263] vyjma povinnosti dle čl. 5.

Nedodržení základních zásad v průběhu zpracování bude sankcionováno druhou skupinou, která ukládá až dvojnásobné sankce, tj. pokuty do výše 20 milionů eur, nebo do výše 4 % ročního obratu. V případě porušení více povinností u stejných nebo souvisejících operací zpracování, není možné tuto výši překročit.[264]

---

[259] Vlachová, B., Maisner, M. *Zákon o zpracování osobních údajů. 1. vydání.* Praha: C. H. Beck, 2019, s. 127.

[260] Recitál 148 preambule nařízení GDPR.

[261] Čl. 83 odst. 1 nařízení ZKB.

[262] Úřad pro ochranu osobních údajů. Základní příručka k ochraně údajů. Sankce, pokuty [online]. *uoou.cz.* [cit. 18. 10. 2023]. https://www.uoou.cz/11-sankce-pokuty/d-27287

[263] Viz kapitolu 4 Povinnosti dle nařízení GDPR.

[264] Čl. 83 odst. 3 nařízení GDPR.

8.2 Správní sankce dle ZKB

Směrnice NIS přenechala stanovení sankcí za porušení vnitrostátních předpisů přijatých podle unijní směrnice na členských státech. Určeny byly pouze požadavky na sankce, které dle čl. 21 musí být, stejně jako v případě sankcí dle nařízení GDPR, *„účinné, přiměřené a odrazující“.* Při jejich ukládání musí být zohledněna například povaha porušení, závažnost, úmysl či výše škod. V ZKB se této problematice věnuje ustanovení § 23–27.

Plnění stanovených povinností kontroluje NÚKIB v souladu se zákonem č. 255/2012 Sb.[265] Smyslem takové kontroly je především zjistit a zhodnotit stav kybernetické bezpečnosti u konkrétního subjektu a opravit případné nedostatky. V případě zjištění závažných nedostatků, pro které by systém mohl být ohrožen kybernetickým incidentem, může být i zakázáno používání takového systému či jeho části. K odstranění zjištěných mezer může být povinné osobě uloženo nápravné opatření.[266]

Nesplnění takto uloženého opatření stejně jako nesplnění jiných stanovených povinností je přestupkem, za který povinné osobě hrozí pokuta. Úprava je obsažena v ustanovení § 25 ZKB, jehož odst. 7 vyjmenovává přestupky správce a odst. 8 provozovatele informačního systému základní služby, odst. 9 se poté věnuje samotnému provozovateli základní služby.

Výše možných pokut je stanovena ve třech hranicích.[267] V případě správce a provozovatele informačního systému základní služby jsou sankce stanoveny ve stejných výších. V následujících odstavcích budou rozebrány výše pokut, které mohou být povinným osobám základní služby (tj. správci a provozovateli informačního systému základní služby a provozovateli základní služby) uloženy za nesplnění v práci rozebraných povinností.[268]

Nejnižší pokuty mohou být uloženy do 10 000 Kč, a to za nesplnění informační povinnosti ohledně kontaktních údajů či jejich změny. Tohoto přestupku se může dopustit každá z povinných osob.

---

[265] Zákon č. 255/2012 Sb., o kontrole (kontrolní řád).

[266] NÚKIB. FAQ. Kontrola plnění povinností podle zákona o kybernetické bezpečnosti [online]. *nukib.cz.* [cit. 19. 10. 2023]. https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka29

[267] § 25 odst. 14 ZKB.

[268] Viz kapitolu 6 Povinnosti dle ZKB.

Maximálně možná pokuta může být uložena správci a provozovateli informačního systému základní služby, a to za nezavedení či neprovádění bezpečnostních opatření nebo nevedení bezpečnostní dokumentace o nich. Hranice této sankce je stanovena na 5 000 000 Kč.

Za nesplnění ostatních v práci rozebraných povinností je stanovena správní pokuta do výše 1 000 000 Kč. Tu je tedy možné uložit všem povinným osobám za nesplnění povinnosti uložené nápravným nařízením po provedené kontrole. Dále také za neohlášení kybernetického bezpečnostního incidentu NÚKIB a neinformování veřejnosti o incidentu v případě, kdy to je povinné osobě uloženo.[269] Provozovateli základní služby může být také uložena za neinformování o svém určení provozovatelem základní služby nebo za neohlášení významného dopadu incidentu na kontinuitu poskytování své služby. Správci a provozovateli informačního systému může být určena za nezohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele, nedetekování kybernetické bezpečnostní události nebo nesplnění povinností týkajících se reaktivních a ochranných opatření.

Nová směrnice NIS2 rozšiřuje kontrolní a donucovací prostředky a navyšuje správní pokuty, kdy stanoví nejnižší možnou úroveň horní hranice sazby pokut. Tyto hranice jsou stanoveny pro regulované organizace v kategorii „důležitý subjekt" na 7 milionů eur nebo 1,4 % ze světového obratu, podle toho, která z hodnot je vyšší. V kategorii „základní subjekt" je poté tato sazba navýšena na 10 milionů eur nebo 2 % ze světového obratu.[270]

V návrhu nového ZKB jsou zahrnuty také tzv. jiné správní tresty, mezi které patří pozastavení platnosti certifikace, o čemž může rozhodnout NÚKIB v případě neodstranění zjištěných nedostatků, a pozastavení výkonu řídící funkce. O druhém jmenovaném trestu bude moci dle návrhu ZKB rozhodnout pouze soud na návrh NÚKIB, a to v situaci, kdy se bude vrcholné vedení soustavně vyhýbat plnění zákonných povinností. Oba správní tresty bude možné uložit pouze poskytovatelům regulovaných služeb v režimu vyšších povinností, a to do doby odstranění zjištěných nedostatků, nejméně však na 6 měsíců.[271]

[269] Viz § 12 odst. 3 ZKB.

[270] Čl. 34 odst. 4 a 5 směrnice NIS2.

[271] NÚKIB. *Nová směrnice EU o kybernetické bezpečnosti „NIS2" a návrh nového zákona o kybernetické bezpečnosti.*

9 Závěr

Ochrana informací a zejména pak osobních údajů ve zdravotnictví je důležitá vzhledem ke specifické povaze prostředí, citlivosti údajů a důsledkům, které může jejich zneužití způsobit. S rozvojem informačních technologií vznikla i potřeba regulace informací, se kterými je manipulováno pomocí těchto prostředků. Respektive potřeba právní úpravy prostoru, do nějž se tyto informace stále častěji dostávají a kde je s nimi dále nakládáno. Dá se říci, že kybernetická bezpečnost a ochrana osobních údajů ve zdravotnictví jsou stále více propojené a musí společně fungovat. A v případě, kdy bude za primární formu vedení zdravotnické dokumentace ustanovena podoba elektronická, tak jak je nyní navrhováno v novele ZZS, bude toto spojení ještě posíleno.

K fungování bezpečnosti mimo jiné i pacientských dat je zapotřebí nejen plnění zákonem uložených povinností ze strany organizace, popřípadě jiných povinných osob, jako například správce či poskytovatele informačního systému. Rovněž je nutná součinnost a obezřetnost ze strany samotných zaměstnanců, kteří musí dodržovat určitá pravidla při práci s osobními údaji, počítači a dalšími prostředky a zařízeními.

K zajištění prevence kybernetické bezpečnosti stanovuje ZKB povinnost plnit určitá technická a organizační opatření. Pro zajištění ideální bezpečnosti pro konkrétní organizaci je nutné najít vhodný poměr prostředků těchto dvou typů opatření. Technická opatření bývají finančně nákladná, ale v situaci, kdy zaměstnanci nemají žádné povědomí o bezpečnosti, ztrácí význam.

Útočníci jsou každopádně neustále o krok vepředu a v rámci kybernetické bezpečnosti nejen ve zdravotnictví je a stále bude, co zlepšovat. I proto je důležité mít technická a organizační opatření nastavená tak, aby bylo riziko co nejvíce minimalizováno.

Mezi největší problémy kybernetické bezpečnosti ve zdravotnictví lze zařadit zejména nedostatek financí a odborníků. Jak bylo uvedeno, z rozpočtu nemocnic je IT oddělení určen jen zlomek, přičemž kybernetická bezpečnost je vedle provozu a dalšího jen jednou ze součástí. U odborníků na kybernetickou bezpečnost je jejich nedostatek obecným problémem. Tyto problémy se v současné době jen stěží vyřeší a lze se domnívat, že zatížením dalších povinných osob spíše vzrostou. Na druhou stranu je navýšení povinných osob v sektoru zdravotnictví snad nezbytnější než v jiných odvětvích.

Ve zdravotnictví vždy šlo, jde a půjde o zdraví osob a jejich životy, což je nejsilnější hodnota. Tomu je potřeba přizpůsobit dostupné technologie a ruku v ruce i jejich bezpečnost. A vzhledem k možnostem ve způsobech léčby, které nám moderní postupy umožňují, nelze tyto prostředky ignorovat.

Použité zdroje

Knihy a monografie

1. Buriánek, J. *Lékařské tajemství, zdravotnická dokumentace a související právní otázky.* Praha: Linde, 2005.
2. Doležal, T., Doležal, A. *Ochrana práv pacienta ve zdravotnictví.* Praha: Linde, 2007.
3. Fiala, O., Grepl, J., Lichnovský, O. *GDPR. Hmotné a procesní aspekty prakticky.* Praha: C. H. Beck, 2019.
4. Gibson, W. *Neuromancer.* Plzeň: Laser, 1998.
5. Graham, J., Howard, R., Olson, R. *Cyber Security Essentials.* Boca Raton: CRC Press, 2011.
6. Hendl, J. *Kvalitativní výzkum: základní teorie, metody a aplikace. Čtvrté, přepracované a rozšířené vydání.* Praha: Portál, 2016.
7. Husseini, F., Bartoň, M., Kokeš, M., Kopa, M. a kol. *Listina základních práv a svobod. Komentář. 1. vydání*. Praha: C. H. Beck, 2021.
8. Janečková, E. *GDPR. Praktická příručka implementace.* Praha: Wolters Kluwer, 2018.
9. Jirásek, P., Novák, L., Požár, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2012. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_V1_5_El.pdf
10. Kolouch, J., Bašta, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf
11. Lehto, M., Neittaanmäki, P., ed. Cyber Security. Critical Infrastructure Protection. Cham: Springer, 2022.
12. Mach, J. *Lékař a právo. Praktická příručka pro lékaře a zdravotníky.* Praha: Grada, 2010.
13. Mach, J., Buriánek, A., Záleská, D., Máca, M., Vráblová, B. *Zákon o zdravotních službách a podmínkách jejich poskytování. Zákon o specifických zdravotních službách. Praktický komentář.* Praha: Wolters Kluwer, 2018.
14. Maisner, M., Vlachová, B. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015.
15. Melotíková, P. *Osobní údaje v kontextu GDPR.* Praha: Leges, 2020.
16. Mišovič, J. *Kvalitativní výzkum se zaměřením na polostrukturovaný rozhovor.* Praha: SLON, 2019.

17. Navrátil, J. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018.
18. Polčák, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018.
19. Prudil, L. *Právo pro zdravotnické pracovníky*. Praha: Linde, 2014.
20. Smejkal, V., Sokol, T., Kodl, J. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Aleš Čeněk, 2019.
21. Sobek, T. Svoboda a soukromí. In: Šimíček, V. (ed.). *Právo na soukromí.* Brno: Masarykova univerzita, 2011.
22. Švaříček, R., Šeďová, K. *Kvalitativní výzkum v pedagogických vědách. Vydání druhé.* Praha: Portál, 2014.
23. Uherek, P. *Povinná mlčenlivost zdravotnických pracovníků: komplexní rozbor aktuální právní úpravy.* Praha: Grada, 2008.
24. Uřičař, M., Rámiš, V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021.
25. Vlachová, B., Maisner, M. *Zákon o zpracování osobních údajů. 1. vydání.* Praha: C. H. Beck, 2019.
26. Žůrek, J. *Praktický průvodce GDPR.* Olomouc: Anag, 2017.

Odborné články

1. Čermák, M. Jak identifikovat primární a podpůrná aktiva a zachytit závislost mezi nimi [online]. *cleverandsmart.cz.* 12. 3. 2016. [cit. 13. 10. 2023]. https://www.cleverandsmart.cz/jak-identifikovat-primarni-a-podpurna-aktiva-a-zachytit-zavislost-mezi-nimi/
2. Duračinská, Z. Co přináší nová směrnice EU o síťové a informační bezpečnosti? *IT Systems.* 2016, roč. 18, č. 10, s. 46–47. Dostupné z: https://www.systemonline.cz/it-security/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm
3. Chlebus, T., Dostál, J. Nový zákon o zpracování osobních údajů [online]. *epravo.cz.* 30. 5. 2019. [cit. 17. 3. 2023]. https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html
4. Kovář, D., Slavíková, K. Jak se (možná) změní vedení elektronické zdravotnické dokumentace? [online]. *havelpartners.blog.* 24. 3. 2023. [cit. 20. 6. 2023]. https://www.havelpartners.blog/jak-se-mozna-zmeni-vedeni-elektronicke-zdravotnicke-dokumentace

5. Lévy, P. Welcome to Virtuality. *Digital Creativity.* 1997, roč. 8, č. 1, s. 3–10. Dostupné z: https://www.tandfonline.com/doi/pdf/10.1080/09579139708567068?casa_token=FgCcxvDznQYAAAAA:3a-H-O2j2gPqHlcZz0jGl0zevfE-8uE8G9cbvGG5I3PqYnnzVxUl5JaQ1w2eXCIdMIE3z-Ccg9Ll
6. Mamrilla, F., Toman, Š. Kybernetická bezpečnost ve zdravotnictví [online]. *epravo.cz.* 9. 4. 2021. [cit. 8. 3. 2023]. https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html#_ftn3
7. Mareš, D., Crháková, E. Zákon o kybernetické bezpečnosti a jeho aktuální novelizace [online]. *epravo.cz.* 17. 8. 2017. [cit. 8. 3. 2023]. https://www.epravo.cz/top/clanky/zakon-o-kyberneticke-bezpecnosti-a-jeho-aktualni-novelizace-106268.html
8. Mašková, M., Kupcová, K. Zákon o elektronizaci zdravotnictví [online]. *epravo.cz.* 17. 5. 2022. [cit. 14. 10. 2023]. https://www.epravo.cz/top/clanky/zakon-o-elektronizaci-zdravotnictvi-114665.html
9. Smekal, H., Šipulová, K. Empirický právní výzkum. *Jurisprudence.* 2016, č. 6, s. 31–38.
10. Warren, S. D., Brandeis, L. D. The Right to Privacy. *Harvard Law Review.* 1890, roč. 4, č. 5. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Kvalifikační práce

1. Brauner, J. *Ohlašovací povinnost dle GDPR a zákona o kybernetické bezpečnosti.* 2021, závěrečná práce, Masarykova univerzita, Právnická fakulta, [vedoucí práce Polčák, Radim].
2. Harašta, J. *Právní aspekty kybernetické bezpečnosti ČR.* 2013, diplomová práce, Masarykova univerzita, Právnická fakulta, [vedoucí práce Polčák, Radim].

Judikatura

1. Nález Ústavního soudu ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99.
2. Nález Ústavního soudu ze dne 20. 12. 2016, sp. zn. Pl. ÚS 3/14.
3. Rozsudek Nejvyššího soudu ze dne 30. 8. 2011, č. j. 25 Cdo 3562/2009.

4. Rozsudek Soudního dvora EU ze dne 30. 5. 2013 ve věci C-342/12.
5. *S. a Marper proti Spojenému království,* rozsudek Evropského soudu pro lidská práva, 4. 12. 2008, č. stížnosti 30562/04 a 30566/04.

Internetové zdroje

1. Article 29 Data Protection Working Party. Guidelines on Data Protection Officers (‚DPOs'). WP 243 rev. 01 [online]. *commission.europa.eu.* 30. 10. 2017. [cit. 10. 6. 2023]. https://ec.europa.eu/newsroom/article29/items/612048/en
2. Article 29 Data Protection Working Party. Guidelines on Personal data breach notification under Regulation 2016/679. WP 250 rev. 01 [online]. *commission.europa.eu.* 20. 8. 2018. [cit. 10. 6. 2023]. https://ec.europa.eu/newsroom/article29/items/612052/en
3. Fakultní nemocnice v Motole v číslech [online]. *FN Motol.* [cit. 8. 3. 2023]. https://www.fnmotol.cz/o-nas/historie-a-soucasnost/fakultni-nemocnice-v-motole-v-cislech/
4. Jak implementovat v ambulantní sféře Nařízení Evropského parlamentu a Rady 2016/679 [online]. *uzis.cz.* 31. 3. 2018. [cit. 10. 6. 2023]. https://www.uzis.cz/res/file/gdpr/jak-implementovat-gdpr-v-ambulantni-sfere.pdf
5. Jelínková, B. Hippokratova přísada: Jak se slavný slib lékařů měnil a co vlastně dnes slibují? [online]. *stoplusjednicka.cz.* 2. 11. 2021. [cit. 9. 6. 2023]. https://www.stoplusjednicka.cz/hippokratova-prisaha-jak-se-slavny-slib-lekaru-menil-co-vlastne-dnes-slibuji
6. NÚKIB. FAQ. Kontrola plnění povinností podle zákona o kybernetické bezpečnosti [online]. *nukib.cz.* [cit. 19. 10. 2023]. https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka29
7. NÚKIB. Informace o institutu základní služby [online]. *nukib.cz.* 22. 12. 2022. [cit. 8. 3. 2023]. https://www.nukib.cz/download/publikace/podpurne_materialy/Informace-o-institutu-zakladni-sluzby_v1.5.pdf
8. NÚKIB. Nová směrnice EU o kybernetické bezpečnosti „NIS2" a návrh nového zákona o kybernetické bezpečnosti [online]. *osveta.nukib.cz.* [cit. 16. 3. 2023]. https://osveta.nukib.cz/mod/page/view.php?id=2582
9. NÚKIB. Odůvodnění zákona o kybernetické bezpečnosti [online]. *osveta.nukib.cz.* Verze 1.0 platná k 25. 1. 2023. [cit. 15. 3. 2023].

https://osveta.nukib.cz/pluginfile.php/82880/mod_resource/content/1/1b_Oduvodneni_Zakon-o-kyberneticke-bezpecnosti.pdf
10. NÚKIB. Rada Evropské unie přijala znění nové směrnice NIS2 [online]. *nukib.cz.* 15. 12. 2022. [cit. 17. 3. 2023]. https://www.nukib.cz/cs/infoservis/aktuality/1923-rada-evropske-unie-prijala-zneni-nove-smernice-nis2/
11. Obecné nařízení o ochraně osobních údajů (GDPR) [online]. *uoou.cz.* [cit. 27. 9. 2022]. https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938
12. Oubělický, R. Směrnice NIS2 a ochrana osobních údajů: Souvislosti a dopady na GDPR [online]. *kybez.cz.* 14. 7. 2023. [cit. 21. 10. 2023]. https://kybez.cz/smernice-nis2-a-ochrana-osobnich-udaju-souvislosti-a-dopady-na-gdpr/
13. Parlament ČR, Poslanecká sněmovna. Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva [online]. *psp.cz.* 10. 1. 2014. [cit. 11. 6. 2023]. https://www.psp.cz/sqw/text/orig2.sqw?idd=90888
14. Parlament ČR, Poslanecká sněmovna. Vládní návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. …/2017 Sb., a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Důvodová zpráva [online]. *psp.cz.* 23. 11. 2016. [cit. 11. 6. 2023]. https://www.psp.cz/sqw/text/orig2.sqw?idd=120106
15. Pender-Bey, G. The Parkerian Hexad: The CIA Triad Model Expanded [online]. Lewis University. [cit. 21. 10. 2022]. http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf
16. RSA Conference. RSA Conference 2012 Keynote – Combating Threats in the Cyber World – Robert S. Mueller, III [online]. *youtube.com.* 2. 3. 2012, 19:47–20:04. [cit. 31. 10. 2022]. https://www.youtube.com/watch?v=MGMOW7nLGvY
17. Sedlák, J. NATO posouvá kybernetikou ochranu mezi priority a na nejvyšší úroveň [online]. *E15.cz.* 5. 9. 2014. [cit. 3. 10. 2022]. https://www.e15.cz/magazin/nato-posouva-kybernetickou-ochranu-mezi-priority-a-na-nejvyssi-uroven-1116140
18. Slávik, M. Útočníci jsou vynalézaví, obyčejný antivirus už k ochraně dat nestačí [online]. *HN.cz.* 18. 7. 2017. [cit. 11. 10. 2022]. https://partner.hn.cz/c1-65803020-utocnici-jsou-vynalezavi-obycejny-antivirus-uz-k-ochrane-dat-nestaci

19. Sněmovní tisk 81/0. Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Důvodová zpráva. [online]. *Poslanecká sněmovna ČR*. [cit. 11. 10. 2022]. https://www.psp.cz/sqw/text/orig2.sqw?idd=90888
20. Úřad pro ochranu osobních údajů. Nové přístupy a povinnosti [online]. *uoou.cz.* [cit. 10. 6. 2023]. https://www.uoou.cz/2-nove-pristupy-a-povinnosti/d-27268/p1=4744
21. Úřad pro ochranu osobních údajů. Obecné nařízení o ochraně osobních údajů (GDPR) [online]. *uoou.cz.* [cit. 27. 9. 2022]. https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr/ds-3938/p1=3938
22. Úřad pro ochranu osobních údajů. Základní příručka k ochraně údajů [online]. *uoou.cz.* [cit. 18. 10. 2023]. https://www.uoou.cz/11-sankce-pokuty/d-27287
23. Úřad vlády ČR. Důvodová zpráva k Návrhu zákona, kterým se mění zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, a zákon č. 325/2021 Sb., o elektronizaci zdravotnictví [online]. *odok.cz.* 8. 6. 2023. [cit. 20. 6. 2023]. https://odok.cz/portal/veklep/material/KORNCMACTGI2/
24. Úřad vlády ČR. Návrh zákona o kybernetické bezpečnosti. Návrh prováděcích právních předpisů [online]. *odok.cz.* Datum autorizace 19. 6. 2023. [cit. 26. 8. 2023]. https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/
25. Úřad vlády ČR. Návrh zákona, kterým se mění zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, a zákon č. 325/2021 Sb., o elektronizaci zdravotnictví [online]. *odok.cz.* Datum autorizace 20. 12. 2022. [cit. 20. 6. 2023]. https://odok.cz/portal/veklep/material/KORNCMACTGI2/
26. Ústav zdravotnických informací a statistiky ČR. Osobní údaje vedené v registrech a systémech ÚZIS ČR [online]. *uzis.cz.* [cit. 9. 6. 2023]. https://www.uzis.cz/index.php?pg=o-nas--ochrana-osobnich-udaju--osobni-udaje-v-registrech-a-systemech
27. Výroční zpráva 2021 [online]. *Nemocnice Blansko.* [cit. 15. 3. 2023]. https://www.nemobk.cz/download/vyrocni-zprava-2021/
28. World Health Organization. Basic Documents, 49th edition [online]. *who.int.* 2020. [cit. 9. 6. 2023]. https://apps.who.int/gb/bd/pdf files/BD_49th-en.pdf

Příloha A Základní okruhy otázek pro poskytovatele

V seznamech níže jsou uvedeny otázky, které byly použity při rozhovorech s respondenty. Tyto otázky byly dle potřeby rozšířeny o další otázky, či zúženy. Taktéž odpovědi jsou v mnoha případech velmi rozsáhlé tím způsobem, že obsahují i odpovědi na další otázky či jiná specifika kybernetické bezpečnosti v praxi. Otázky jsou zde rozděleny na skupinu, která byla položena zástupcům zdravotnických zařízení (respondent č. 1 a 2) a otázky položené zástupci NÚKIB (respondent č. 3). V samotném textu diplomové práce je část pro zdravotnická zařízení rozdělena na další dvě poloviny.

A.1 Zdravotnická zařízení

1. Co musí Vaše zdravotnické zařízení splnit v oblasti kybernetické bezpečnosti? Co považujete za slabiny kybernetické bezpečnosti ve zdravotnictví?
2. Co podle Vašeho názoru patří mezi nejdůležitější zákonné požadavky?
3. Kdo se v nemocnici stará o IT? Má nemocnice interní oddělení nebo využívá služeb dodavatelských firem (tzv. outsourcing)?
4. Úprava NIS2. Je podle Vašeho názoru nutná? Měla dle Vás přijít dřív? Změní se pro Vaše zdravotnické zařízení něco zásadního?
5. Na co se útočníci v současné době nejčastěji zaměřují (krádež dat či paralyzace nemocnice)?
6. Která kybernetická hrozba je v současné době nejběžnější?
7. Jak ve Vašem zdravotnickém zařízení probíhá prevence kybernetických útoků? Jak probíhá školení zaměstnanců (např. prostřednictvím e-learningu či osobními školními)?
8. Jaké první kroky musí nemocnice učinit po útoku? Existuje nějaký interní předpis? Jsou nějakým způsobem prováděny zkoušky takové situace?
9. Na co se dle Vašeho názoru budou útočníci v budoucnosti zaměřovat? Co považujete za příchozí hrozby?

A.2 NÚKIB

1. Jak poskytovatelé zdravotních služeb přistupují k plnění zákonných povinností v oblasti kybernetické bezpečnosti? Co je v tomto ohledu největším problémem?
2. Jak je na tom české zdravotnictví po stránce kybernetické a informační bezpečnosti ve srovnání s jinými evropskými státy?
3. Úprava NIS2. Je změna nutná? Měla přijít dříve?
4. Změní se s novým ZKB pro stávající povinné subjekty něco zásadního?
5. Máte odhad na kolik nových povinných osob ze sektoru zdravotnictví se nový ZKB bude vztahovat (v režimu základních i důležitých subjektů)? Nebudou povinnosti pro nové subjekty příliš zatěžující?
6. Jak NÚKIB přistupuje k prevenci kybernetických hrozeb? Liší se nějak prevence v oblasti zdravotnictví od prevence v jiných oblastech?
7. Jak probíhají kybernetická cvičení? Jak často se provádějí?
8. Jak probíhá součinnost NÚKIB s napadenou nemocnicí při řešení kybernetického útoku a při řešení jeho následků?

Příloha B **Rozhovory s respondenty**

B.1 Rozhovor s respondentem č. 1

První rozhovor byl veden se zástupci zdravotnického zařízení. V případě potřeby a pro přehlednost odpovědí jsou tito zástupci u některých otázek označeni jako „respondent č. 1A“ a „respondent č. 1B“ (viz Tab. 1: Přehled respondentů).

1. **Můžete zhodnotit kvalitu kybernetické bezpečnosti ve Vašem zdravotnickém zařízení? Jak na tom podle Vás jste ve srovnání s ostatními nemocnicemi?**

My pod ZKB spadáme od roku 2021, kdy jsme splnili stanovená kritéria a NÚKIB nás jmenoval za provozovatele základní služby. Museli jsme splnit požadavky zákona a vyhlášky, na což byl rok. Začali jsme implementovat nějaké věci, vybrali jsme dodavatele ISMS a tento projekt právě běží. Oproti ostatním nemocnicím, které byly stanoveny od roku 2015, máme skluz.

Vše závisí na technologiích a lidech. Nemocnice mají podstavy zaměstnanců v IT a i technologicky jsou o něco pozadu, protože investice jsou vysoké. Nemocnice, které mají řádově stovky milionů rozpočet, tak na IT z toho jde jen zlomek.

Takže my jsme ve stavu, kdy implementujeme ISMS, řešíme procesně incidenty, které zde vznikají. Řeší se to s NÚKIB, kterému se to hlásí. To u nás nějakým způsobem funguje. Máme zde Výbor pro kybernetickou bezpečnost, který řídí kybernetickou bezpečnost na bázi procesních věcí. Je zde pozice manažera a architekta kybernetické bezpečnosti. Připravujeme se na interní audit, bude jmenovaný člověk na interní audit, jehož povinností bude v intervalu 1–2 roky kontrolovat plnění různých směrnice.

Myslím si, že na tom nejsme špatně, ale máme před sebou ještě dlouhou cestu. Nyní máme zažádáno o dotaci v hodnotě 50 milionů Kč, která nám pomůže zlepšit technickou bezpečnost (tj. technologie). Jsme na dobré cestě, ale uvidí se.

2. Co musí Vaše zdravotnické zařízení splnit v oblasti kybernetické bezpečnosti? Co považujete za slabiny kybernetické bezpečnosti ve zdravotnictví? Co podle Vašeho názoru patří mezi nejdůležitější zákonné požadavky?

Respondent č. 1A

Musíme minimálně naplnit zákon. Musíme mít ty věci organizačně, tzn. potřebné dokumenty, musí být nasazené a všechny procesy musí nějakým způsobem fungovat.

V podstatě každá věc je důležitá. Nyní se řeší dodavatelský řetězec, abychom měli podchycené a prověřené významné dodavatele. To si myslím, že je hodně komplikovaná věc, protože my k dodavatelům mnohdy nevidíme a nevíme, jak fungují. Většinou se při výběrových řízeních podepisuje čestné prohlášení, že daný dodavatel něco splňuje. Jinak je nejsme schopni prověřit a nemáme na to ani mechanismy.

Respondent č. 1B

Když se vypisuje veřejná zakázka, tak zadavatel může do velké míry nadefinovat různé podmínky. Věci, které nejsou v jeho silách zkontrolovat, proto to čestné prohlášení. Je to takové vykrývání zodpovědnosti, kdy uchazeč prohlašuje, že zadavatelem stanovené podmínky, splňuje.

Respondent č. 1A

Dále v celé kybernetické bezpečnosti je složitá evidence aktiv. V našem případě je to tak, že aktivem je vše, kde jsou zjednodušeně např. pacientská data. Vedle toho existují podpůrná aktiva, což jsou technologie, kterými se to nějakým způsobem zpracovává. Procesně je velmi složité podchytit všechny systémy ve vztahu, že patří do základní služby.

K tomu je nutné za každý systém určit garanta aktiva, který za něj zodpovídá. Nezodpovídá po technologické stránce, ale musí vědět, jaká data systém obsahuje a jakým způsobem se tam dostávají. To může probíhat buď automaticky, nebo manuálně.

V organizaci je těžké najít nějakého garanta, který by si vzal tu zodpovědnost na sebe. Většinou jsou jimi manažeři z nejvyšší úrovně.

Respondent č. 1B

Zde je průnik do GDPR. Jednou ze základních povinností každého správce je vést tzv. záznamy o činnostech zpracování, což de facto je evidence procesu zpracování, tam kde jsou osobní údaje.

Ono se to poměrně často vykrývá s těmi informačními systémy. Ne vždy, protože ne vše je zpracováváno v elektronické podobě. Typicky

zdravotnická dokumentace, pokud již nepřešla do digitalizace, tak se zatím primárně vede v listinné podobě.

Záznamy o činnostech, co záznam to nějaká činnost zpracování a celé to vede k systému. A dostáváme k odpovědnosti. Kolega říká, že je garant za aktivum, ale když se to překlopí do té mojí agendy, tak každé pracoviště má mít přehled o procesech zpracování, které na tom daném pracovišti jsou. Když se zavede nějaký nový systém, tak by to mělo být doplněno, měla by se provést analýza rizik, každého toho procesu i podle GDPR. Abychom na 100 % plnili to, co plnit máme i podle GDPR. Upřímně jsme na tom tak, že plníme, co plnit máme, ale stále jsou mety, kam je potřeba to vylepšovat. A proto se dělají audity i v této oblasti.

Respondent č. 1A

U těch aktiv se ještě musí zhodnotit integrita, důvěryhodnost a dostupnost. Takže každé aktivum je ohodnoceno nějakou škálou. Existuje k tomu metodika.

S garanty aktiv se potom ty systémy musí projít, a musí se stanovit, jak dlouho mohou být mimo provoz. Například i kolik dat se může ztratit v rámci havárky, aby je bylo možné doplnit, nebo se o ně přijde úplně. Pro garanty je nepředstavitelné, aby došlo k něčemu takovému, ale dochází k tomu. Musí být nastaveno kolik dní či hodin mohou být bez dat nebo systémů, a zda vůbec jsou schopni překlenout takový výpadek.

Úplně dám triviální příklad. V nemocnici je kuchyně, která vaří pro pacienty a zaměstnance. Kdyby vypadly systémy, v nichž se eviduje, jaká jídla se mají vařit, objednávkový systém surovin atd., tak by to byli schopni jiným způsobem naplánovat na den dopředu. Ale těžko by už připravovali jídelníčky na týden. Muselo by se přejít do nouzového režimu.

Respondent č. 1B

Představte si, co by se stalo ve zdravotnickém provozu, kdyby přestaly fungovat nemocniční informační systémy. Máte pacienty na sále, laboratoře, čeká se na výsledky a často na tom závisí život pacienta. Je to extrémní, proto asi systém základní služby, protože bez toho to vlastně nejde.

Od našeho IT oddělení vím, že kybernetickým útokům nemocnice čelí prakticky stále. Systémy musí být nastavené tak, že útoky automaticky kontinuálně odvracejí. Není to tak, že jednou za čas přijde útok.

Respondent č. 1A

Ono se čeká na objevení nějaké zranitelnosti, která zde je, ale ještě se o ní neví. Pak záleží na rychlosti reakce a schopnosti napravit chybu.

Respondent č. 1B

Slabý článek je lidský faktor, zaměstnanci, proto je důležitá edukace. Pod tlakem, který v nemocnici nepochybně je, mohou udělat nějakou chybu. Proto se klade důraz na školení, aby se to riziko minimalizovalo, protože zcela tomu zabránit je asi nemožné.

Doplním kolegu ještě, kdyby došlo k nějakému kybernetickému incidentu, tak on má opět přesah zpátky do GDPR, a to ve chvíli, kdy by šlo o pacientská nebo zaměstnanecká data. Ve chvíli, kdy jsou dotčeny osobní údaje, tak jako pověřenec musím podle GDPR vyhodnotit, na kolik to potencionálně zasahuje do práv subjektů a musí se to do 72 hodin hlásit na ÚOOÚ. A v případě, že by šlo o nějaký velký plošný útok, tak to musíte zveřejnit prostřednictvím tiskového mluvčího či zveřejněním na webových stránkách, popř. když je subjektů míň, ale je to závažné, tak se budou informovat adresně. Předpisy jsou docela striktní.

Respondent č. 1A

Ne vždy je kybernetický útok tak rozsáhlý, ale média a lidi z toho mohou udělat obrovskou bublinu. Proto je důležitá komunikace nemocnice vůči veřejnosti – aby byly včas sděleny korektní informace. Jinak to začne žít svým životem.

Respondent č. 1B

Tohle se metodicky, a myslím si, že docela dobře, snaží vést NÚKIB. NÚKIB se snaží být tím metodickým vůdcem, jak tyto incidenty řešit.

Respondent č. 1A

Ještě jednu věc zmíním. Když se v nemocnici něco takového stane, nemusí to být nijak velké, tak se v podstatě nemocnice musí odstavit. Potom nastává otázka, co s pacienty a vzniká velké riziko, že se jim může něco stát.

Když všechno, co tady děláme, funguje jak má, tak je to v pořádku. Ta činnost musí být kontinuálně vykonávána. Taktéž se neustále musíme v různých věcech zlepšovat a sledovat trendy. Kybernetické hrozby jsou neustále vepředu a objevují se nové.

Respondent č. 1B

Nasazování nových technologií na vychytávání hrozeb je do velké míry i otázkou peněz. Třeba se ví, co by bylo potřeba, ale je nutné do toho zainvestovat.

Respondent č. 1A

Jedno z měřítek je i personální zajištění IT procentuálně vůči velikosti organizace. My se pohybujeme pod 1 % počtem zaměstnanců v IT, ale v bankovnictví je to mezi 7–9 %. Potom je rozdíl kolik lidí, energie

a úsilí se do toho dá. Navíc v nemocnici primárně zajišťují provoz, jehož součástí je i kybernetická bezpečnost.

Klíčovou věcí je, že by určitá znalost neměla stát na jednom člověku. Je jeden člověk, který dělá klíčovou roli, má nějakou znalost, kterou nikdo jiný nemá. Třeba v oblasti medicíny bych řekl, že to je vykryté. Dlouhodobě tady je více lékařů s jednou specializací, RTG přístroj nebo CT není jedno, takže když jedno selže, dá se to nahradit. Ale v IT tomu tak není.

3. Kdo se v nemocnici stará o IT? Má nemocnice interní oddělení nebo využívá služeb dodavatelských firem (tzv. outsourcing)?

My máme interní tým, ale v tom jsme v naprosté menšině. Většina nemocnic systémy outsourcuje, mají to řešené dodavateli.

My máme některé věci outsourcované ve smyslu servisu. To znamená, že v případě nějaké havárky nebo nějaké opravy přijede servisní organizace. Třeba pro výměnu akumulátorů v UPS zařízení nebo pro servis diesel agregátu je společnost, která tento servis provádí.

Outsourcing má své důvody z třeba ekonomického hlediska. Nevýhodou je závislost na jiných firmách v případě mimořádných situací.

4. Úprava NIS2. Je podle Vašeho názoru nutná? Měla dle Vás přijít dřív? Změní se pro Vaše zdravotnické zařízení něco zásadního?

Respondent č. 1A

Já si myslím, že NIS2 neměla vzniknout jako skok, ale mělo to být plynule. Podle mě to způsobí zase takovou vlnu, kterou způsobilo GDPR. Bude se muset změnit dokumentace a procesy v organizacích, komerční sféra na to zareaguje různými typy kampaní, kdy budou nabízet různá řešení. Budou to chtít monetizovat stejně jako GDPR. GDPR trochu posloužilo ke strašení organizací, že budou velké pokuty, když něco nesplní nebo když si nekoupí nějaký evidenční systém, a nakonec to tak nebylo. NIS2 k tomu také spěje.

Pro nás to bude znamenat, že se nová úprava bude vztahovat na celou organizaci. Teď je jen na základní službu a vše kolem ní, ale na některé systémy, které nemají dopad do základní služby, není kladen takový důraz. NIS2 bude brát jen celou organizaci. Vznikne administrativa, další směrnice, a to si myslím, že už bude problém. My máme přes 700

různých směrnic. Není v lidských možnostech si to pamatovat. Samozřejmě směrnice jsou pro určité oblasti a zaměstnanci znají jen ty, které se jich dotýkají, ale myslím si, že už to je trochu kontraproduktivní.

Respondent č. 1B

Tady si dovolím uvést trochu jiný pohled na věc. Já si nemyslím, že GDPR, NIS a podobné předpisy, které přichází zejména z EU, jsou nějakým způsobem v principu špatně. Možná je chyba v tom, že konkrétně GDPR je v podstatě geniální předpis, ale je strašně obsáhlý a problém byl v jeho obecnosti, která je však nutná. Někdo třeba vůbec nepochopil jeho klíčové poselství, které stanovovalo, co se má zařídit, ale nebyla určena cesta, jak se k tomu má dospět. Někdo ten předpis nepochopil vůbec, další si to vyložil nějak a pak se ty názory střetávaly.

Za mě všechny tyto předpisy přišly pozdě, GDPR i NIS2. Pak je problém jejich přenos do legislativ členských států. Zákonodárci v některých členských státech nevyužili toho, co jim ty směrnice nabízí nebo to, co měli dávno udělat, aby byla ČR konkurenceschopná ve vztahu k jiným státům, tak to neudělali. Když necháte členským státům prostor, tak si zákonodárci u různých věcí řeknou, že se s tím praxe nějak popere. Pak se člověk nediví, když nikdo neví, jak co má fungovat.

5. Která kybernetická hrozba je v současné době nejběžnější?

Nejčastější jsou phishingové útoky. Ty umožňují rychle kompromitovat obrovské množství e-mailových schránek, protože organizace typu nemocnice mají tisíce zaměstnanců (my máme přes 3000). A vždy se může stát, že tam minimálně jednoho člověka nachytají.

Podle nějaké starší statistiky, když vyhodnocovali útoky v USA, jak se staly a kdo byl strůjcem, to většinou byli lidi, kteří pracovali ve směnách. Takoví zaměstnanci mají obrovskou vytíženost a mezi tím jim přijde nějaký e-mail, který vypadá, že mají jen něco někde vyplnit. Tak rychle vyplní svoje přístupové údaje, odešlou a pracují dál. Tím může dojít ke zneužití e-mailové schránky.

Ransomwary, to už je opravdu obrovský průšvih, když je ransomware uvnitř organizace a už koná, šifruje data, vytvoří back door, dochází k úniku dat. To už je fatální kybernetický útok, který vede k ochromení IT a v podstatě i celé instituce. U nás se to nestalo, ale jsou případy (Bohunice, Benešov, Ostrava), kdy se tato věc stala. Mohlo by to mít takový dopad, že už data nikdy neobnoví. To potom vyřeší čas a zákonné lhůty pro skartaci dokumentů.

6. Na co se útočníci v současné době nejčastěji zaměřují (krádež dat či paralyzace nemocnice)?

Respondent č. 1A

V současné době je enormní zájem o data, se kterými se obchoduje. Ve Finsku se stalo, že byla napadena psychiatrická klinika a hackeři vydírali pacienty. Nabízeli jim, že jejich diagnóza nebude nikde zveřejněna, ale musí jim zaplatit v bitcoinech. Může to poškodit renomé nemocnice i pacienty. Takže je zájem o pacientská data.

Respondent č. 1B

Dopady totiž nejsou jen finanční nebo konkrétní, že útok např. může někoho ohrozit na životě, ale vznikají i právní dopady. Někomu je třeba způsobena újma a může se legitimně domáhat náhrad.

V neposlední řadě je to i poškození dobrého jména nemocnice, renomé. Nemocnice není nenahraditelná, ale vše stojí na důvěře. Pacienti chodí do nemocnice v dobré víře, že se jim zde pomůže, že se jim tam nemůže nic stát.

Respondent č. 1A

Snahou nás všech je, aby dopady na pacienty byly co nejmenší. Zdravotní personál, aby dělal, co má dělat. A našim úkolem je, aby systémy fungovaly, protože prostředí v nemocnici je rizikovější. Pracuje se zde se zdravím lidí, s léky, se zdravotními výkony, jsou zde zdravotní přístroje, které něco dávkují, rentgeny. Prostředí s vyšší rizikovostí zde je.

Respondent č. 1B

Nemocnice je ještě specifická v tom, že kdokoliv bez ohledu na své společenské postavení se zde může ocitnout. Dotýká se to skutečně všech. V tom je to citlivé.

Respondent č. 1A

Ještě k těm útokům, ve všech nemocnicích se nejvíce obávají sofistikovaného kybernetického útoku, který změní data – integritu a důvěrnost dat. To může nastat, jak v evidenčních systémech, tak v medicínských přístrojích. Jsou známy případy např. dávkování do infuzních pump, že se začne dávkovat větší množství nebo rychleji, a to ohrožuje pacienta na životě. U nás se to nestalo, ale viděl jsem článek, jak je možné ovládat infuzní pumpu tím způsobem, že navenek ukazuje správné hodnoty, ale dávkuje třeba dvakrát rychleji. Nebo může dojít ke změně pacientských dat a potom se může zvolit špatná medikace.

To je ten sofistikovaný útok. Špatně se odhaluje, protože se projeví třeba až sekundárně na pacientech. Je to asi nejhorší na odhalení a může to mít fatální dopad.

7. Jak ve Vašem zdravotnickém zařízení probíhá prevence kybernetických útoků? Jak probíhá školení zaměstnanců (např. prostřednictvím e-learningu či osobními školními)?

Respondent č. 1A

Co se týče organizačních opatření, probíhá školení prostřednictvím e-learningu. Noví zaměstnanci jsou při nástupu seznámeni, čím vším musí projít, co vše se musí naučit a splnit. E-learningy máme na GDPR i na kybernetickou bezpečnost. Dále to pak jsou i nějaká osobní školení související se zaměřením zaměstnanců.

Respondent č. 1B

Já jsem osobně školila výzkumníky pracující s daty. I lékaři s nimi sice pracují, ale u lékaře je hlavní náplní práce poskytování zdravotních služeb. Výzkumníci ta data potřebují z nějakého místa vzít a dále s nimi pracovat. Takže jsem dělala onsite školení zaměřené na zdravotníky a výzkumníky, ale jinak máme ten plošný e-learning.

Respondent č. 1A

Já dělal školení biomedicínských inženýrů. To jsou zaměstnanci, kteří obsluhují zdravotní techniku, která dnes vesměs má charakter IT zařízení. Ta zařízení s něčím komunikují a sbírají nějaké informace, a to od operačních sálů až po ambulance. Jsou tedy více do IT, ale ještě stále zaměřeni na medicínskou diagnostiku. Tito zaměstnanci se tedy musí edukovat zvlášť, protože ta zdravotní technika je specifická.

K těm phishingovým útokům, které by řídila nemocnice. V současné době žádné nejsou. Historicky se dělaly. Ale nyní tím, jak neustále nějaké probíhají, tak jsou zaměstnanci trénovaní skutečnýma.

8. Jaké první kroky musí nemocnice učinit po útoku? Existuje nějaký interní předpis? Jsou nějakým způsobem prováděny zkoušky takové situace?

V nemocnici je Odbor bezpečnosti a krizového řízení, který má na starost všechny stavy, kdy nemocnici hrozí nějaký kolaps. Je na to směrnice, která všechno řídí. Říká, jak aktivovat nějakou nouzovou situaci, označuje shromaždiště pacientů a pokračuje až po kybernetickou

bezpečnost, resp. provoz IT systémů, včetně toho, který systém se musí zprovoznit jako první, který jako poslední apod. To je pro celé krizové řízení.

Přímo pro kybernetickou bezpečnost, která je podřízena krizovému řízení, existuje Výbor pro kybernetickou bezpečnost, ve kterém jsou nominovaní lidi, kterých se to přímo dotýká.

Nějaká cvičení probíhají jedenkrát ročně, ale jsou to dílčí. Zatím jsem tady nezažil nějaké velké cvičení, ale dělají se průběžně. Také se zkouší i např. evakuační plány.

9. Na co se dle Vašeho názoru budou útočníci v budoucnosti zaměřovat? Co považujete za příchozí hrozby?

Nové hrozby přináší umělá inteligence a její aplikace v kybernetických útocích. Pokud se frameworky umělé inteligence začnou aplikovat v kybernetických útocích, tak tam je riziko. A asi to přijde. Umělá inteligence bude dělat útoky nějakého typu a umělá inteligence je bude analyzovat a bude dělat opatření. Směřuje to víc a víc k automatizaci, stejně jako Průmysl4, kdy se automatizuje výroba v továrnách. Směřuje to i k automatizovaným útokům, které už v podstatě probíhají a k automatizované obraně, protože reakční doby jsou krátké a půl hodina už je dlouhá doba.

B.2 Rozhovor s respondentem č. 2

Druhý rozhovor byl veden jako první se zástupcem zdravotnického zařízení.

1. Co musí Vaše zdravotnické zařízení splnit v oblasti kybernetické bezpečnosti? Co považujete za slabiny kybernetické bezpečnosti ve zdravotnictví?

Nemocnice má dle zákona, respektive vyhlášky plnit určitá organizační a určitá technická opatření.

Na technická opatření existují firewally a zabezpečení systému obecně. K tomu potřebujete odborníky na IT (lidskou sílu) a finance. Obojího je nedostatek.

Jakmile spadnete do kategorie povinných osob dle ZKB a NÚKIB vás určí, máte rok na naplnění požadavků zákona. Existují sice nějaké dotace, ovšem ne vždy se podaří danou dotaci získat, nebo ty dotační programy trvají déle, než potřebujete. Je to složité.

Troufnu si říct, že 10 z 10 přednášejících na kterékoliv konferenci zmíní, že je nedostatek lidí (a to je obecný problém, odborníků na kybernetickou bezpečnost je nedostatek) a nedostatek financí.

U organizačních opatření se naráží na rezistenci zdravotnického personálu, jehož hlavním úkolem je zachraňovat životy, ne se věnovat kybernetické bezpečnosti. Ovšem i tak se kybernetické bezpečnosti nemohou vyhnout, a musí být obezřetní zejména při procházení mailů.

V případě osob, které své e-mailové schránky příliš nenavštěvují, toto riziko paradoxně stoupá. Takové osoby totiž svůj e-mail jednou za čas navštíví, aby rychle prošli doručené zprávy, a jejich obezřetnost v takových případech klesá.

Toto jsou největší úskalí kybernetické bezpečnosti v nemocnicích. Paradoxně k tomu, aby se problematika kybernetické bezpečnosti v nemocnicích začala vnímat, pomohly útoky, co proběhly v nedávné době – v Brně Bohunicích, Ostravě a Benešově.

V současné době nejsme bez počítače schopni udělat téměř nic a stačí opravdu málo, aby došlo k nějakému incidentu. Můžeme mít sebelepší technické zabezpečení, ale vždycky může projít ten jeden e-mail, na který může někdo kliknout. A v tu chvíli nastává problém.

Stejně jako byl nejdřív meč a až poté štít, tak i hackeři jsou vždy o něco napřed. Oni nejprve vymýšlí útok, na který se až následně vymýšlí obrana. Poté záleží na IT, manažerovi kybernetické bezpečnosti a architektovi kybernetické bezpečnosti, jak dokáží poskládat bezpečnost, aby se to riziko, které nelze vyloučit, co nejvíce minimalizovalo.

2. Co podle Vašeho názoru patří mezi nejdůležitější zákonné požadavky?

V zákoně musíte dodržovat všechny požadavky. Nemám úplně rád, když se někdo rozhodne nastavit jen něco, aby se „vlk nažral a koza zůstala celá“. Zkrátka máme zákon, ve kterém jsou určité paragrafy, které je nezbytné plnit.

Za mě lze za základní považovat ty technické požadavky. Aby bylo technické zabezpečení, firewally, aktuální systémy. Dá se říct, že to je

trošku jednodušší, protože se nebojuje se zdravotnickým personálem, který samozřejmě má úplně jiné starosti než, že si mají přečíst školení.

Samozřejmě i to školení je důležité a dělat se musí ze zákona. Ovšem já nejsem zastánce toho, že se kybernetická bezpečnost musí řešit, protože to určuje zákon. Chci, aby to bylo bráno tak, že kybernetickou bezpečnost řešíme, protože chceme a ne protože musíme. A chceme ji řešit, protože chceme zdravotní péči poskytovat stále. Tudíž se musíme chránit, aby nám nevypadly systémy a nenastal výpadek poskytování základní služby. Přestat poskytovat péči by byl velký problém.

Samozřejmě i organizační opatření na zaměstnance, považuji za důležitý požadavek. Myslím si však, že k tomu nelze pouze vytvořit e-learning, který každý vyplní. To je ve finále dobrý důkaz pro NÚKIB. Samotnou edukaci, osobní setkání či e-maily s novinkami to však nenahradí. Když takto upozorním na nové phishingové kampaně, tak si to zaměstnanci mohou propojit i se soukromým životem a začnou být více pozorní.

Úplně rozdělit to asi nelze, ale ano, nějaké pořadí by asi šlo vyspecifikovat. Nejdůležitější je udělat si systém řízení bezpečnosti informací (ISMS) a určit garanty jednotlivých aktiv. Aktivy rozumíme různé oblasti, třeba servery, nebo technické vybavení genetické laboratoře atd., u nichž musí být určen garant, který označí všechny prvky, které je nutné chránit. Dále je nezbytné udělat analýzu rizik, která spočívá ve stanovení, jaká musí být dostupnost, například zmíněné genetické laboratoře, po útoku. Maximálně může být např. 24 hodinový výpadek. Tudíž se musí stanovit, jak se do 24 hodin po útoku obnoví provoz. Tohle je základ, kterým se začíná. Určíte si garanty, veškeré aktiva (primární a podpůrná/technická), na která se potom udělá analýza rizik.

Dalším příkladem může být například situace, kdy onemocní celý personál. Nedostatek personálu je určité riziko. A my musíme popsat, jak toto riziko budeme řešit, zda máme smlouvu s nějakou nemocnicí, do které bychom převáželi pacienty, zda přijdou pomoci nějací lékaři apod.

Pro případ havárie serverů jsou dělány pravidelné zálohy. Víme však, že výpadek můžeme mít maximálně 24 hodin. Musíme mít nastavené postupy a zajištěné kapacity (lidské zdroje), aby bylo možné servery do 24 hodin obnovit. Takto se to musí prolnout celou nemocnicí, nejrůznějšími situacemi.

Největší základem pro odborníka na kyberbezpečnost je naučit se, jak nemocnice funguje, což je to nejnáročnější. Nemůžete zabezpečovat něco, co neznáte. Personál z IT musí přesně vědět, co který server dělá.

Nemohou jen takaktualizovat servery, které hlídají nějaká zařízení u pacientů. Na všechno toto se musí myslet. Je to odlišné od jiných prostředí např. úřadů, protože na nemocnici závisí lidské životy.

Za mě je zkrátka z toho zákona důležité všechno. Samozřejmě to ale nejde všechno nastavit zároveň, je to potřeba dělat postupně. Dle mého názoru je potřeba, nejprve vše zabezpečit technicky, což uživatele moc nezatěžuje, protože se to někde nastaví na serveru, nainstalují se antiviry a podobně. A potom zaměstnance začít trápit těmi organizačními složkami. Školit je, jak se chovat k počítači, že nemají nechávat spuštěné počítače, otevřené kanceláře, vysvětlit jim pravidlo čistého stolu, nenechávat citlivé údaje, např. zprávy pacientů, jen tak ležet na stole. Je potřeba ty informace zabezpečit.

3. Kdo se v nemocnici stará o IT? Má nemocnice interní oddělení nebo využívá služeb dodavatelských firem (tzv. outsourcing)?

Vždy musí existovat nějaké interní IT. Minimálně alespoň jeden IT technik, který pomáhá s každodenními situacemi v nemocnici. Například když lékaři přestane fungovat počítač, musí být někdo, kdo půjde zjistit, co se stalo. Vždy zkrátka je nějaké IT oddělení.

Pokud se nezvládá, tak se třeba o nějakou část IT starají dodavatelé (síťoví specialisti apod.).

Nedokážu obecně říct kolik to je procentuálně, jaká je ta vyváženost interního IT vs. externí dodavatelé. Každá nemocnice to má jinak. Je rozdíl, pokud se jedná o kliniku o 500 zaměstnancích a fakultní nemocnici, kde jsou zaměstnány řádově tisíce zaměstnanců.

Takže samozřejmě jsou využívání i externí dodavatelé, se kterými musí být uzavřené patřičné smlouvy. Ovšem v každé nemocnici musí být nějaký IT tým, nebo minimálně alespoň jeden IT technik, který je fyzicky přítomen a řeší aktuální problémy.

4. Úprava NIS2. Je podle Vašeho názoru nutná? Měla dle Vás přijít dřív? Změní se pro Vaše zdravotnické zařízení něco zásadního?

Nutná je. Na druhou stranu tím, jakým způsobem je současný zákon o kybernetické bezpečnosti udělaný, tak pro nás jako nemocnici to s novou úpravou nebude tak rapidní změna. Velký zásah to však bude pro ty, kteří kybernetickou bezpečnost nikdy neřešili a budou dle nového zákona

nově povinni plnit požadavky nového zákona o kybernetické bezpečnosti.

K té druhé otázce. Na evropskou úroveň obecně a narovnání podmínek pro zajišťování kyberbezpečnosti napříč státy EU to mohlo přijít dřív. Co beru za velké plus, je článek o zodpovědnosti vedení, který nyní chyběl, a rapidně se zvýší sankce. Takže bude tlak na řešení kybernetické bezpečnosti na úrovni vedení nemocnic. U nás je naštěstí kybernetická bezpečnost na úrovni vedení vnímána a je jí přikládána vysoká důležitost. Jen chybí ty peníze.

5. Na co se útočníci v současné době nejčastěji zaměřují (krádež dat či paralyzace nemocnice)?

Záleží útok od útoku. Dá se říct, že není pravidlem, že se útočí na nemocnice. Jsou známé situace, kdy byla zašifrována dětská nemocnice. Hackeři poté zjistili, kam se dostali, odšifrovali ji a omluvili se. Zkrátka měli nějaký etický kodex.

Musíte si uvědomit, že je to virus. Je to jako v tramvaji, tam si taky virus nevybírá, na koho skočí. Například ty e-maily, to nerozesílá člověk na konkrétní místa. To dělá robot, který ty e-maily rozesílá náhodně na různé adresy. Potom někdo někde klikne na odkaz s virem a hackerovi přijde zpráva, že se někam dostal. Mluvím teď o jedné z milionu možností. Potom tam může nainstalovat nějakého červa, kterým to bude monitorovat, bude si to tam procházet a bude zjišťovat, kam všude se dostane. To může trvat třeba i rok.

Je známá situace, kdy našli virus až po třech letech. Ten virus ale pořád spal a až s nějakými aktualizacemi ho nalezli. Zpětně zjistili, že tam byl hodně dlouho. V této situaci pravděpodobně hacker zapomněl, že ho tam dal.

Když už si ten virus najde všechny slabiny a zjistí, co všechno může provést, tak potom to třeba může zašifrovat nebo udělat nějaký útok. Může například ukrást údaje, poslat vzorek na vedení a požadovat výkupné. Nebo to může zašifrovat. To znamená, že zčernají obrazovky a pro odšifrování bude nutné zadat kód. V takových případech bývá opět nutné zaplatit výkupné.

Rozhodnutí, zda bude výkupné poskytnuto, závisí na vedení. Můžete zaplatit a hackeři mohou požadovat další peníze. To už je otázka, jak moc to pro vás spěchá. Policie obecně říká, že se platit nemá.

Když máte dobré zálohy, které máte offline, takže se nemohly nakazit, tak nemusíte platit. Týden sice nebudete fungovat, ale budete obnovovat zálohy. Samozřejmě je potřeba, před samotnou obnovou, zálohy zkontrolovat, jestli jsou skutečně v pořádku a nejsou také zavirované.

To vše souvisí s již zmíněným Plánem kontinuity činností. Nemocnice, respektive všichni garanti aktiv, které mohou být potencionálně napadnutelné, musí vědět, co mají dělat.

6. Co bývá nejčastějším cílem útočníků?

To záleží na typu viru. Ale nemyslím si, že by hackeři cílili na paralyzaci nemocnice, to už by muselo být opravdu hodně cílené.

Nejvíc chtějí peníze. A je pravda, že ty nejlíp dostanou, když nemocnici paralyzují, když jim tam něco zašifrují.

V případě kdy ukradnou data, tak nemocnice může stále fungovat. Nemá to tedy takovou váhu pro rychlé získání peněz.

Kdybych měl uvažovat jako hacker, chtěl peníze a nezajímali by mě životy lidí, tak bych se zaměřil na paralyzaci nemocnice. Takovou situaci totiž musí vedení rychle vyřešit, a prvním a nejrychlejším řešením ve chvíli paniky je zaslání peněžního obnosu za účelem rychlého obnovení provozu.

7. Která kybernetická hrozba je v současné době nejběžnější?

Phisingové kampaně chodí v podstatě neustále. Objevují se nové viry, např. FBI v nedávné době informovala o hojném využívání přihlašování přes vzdálenou plochu. Ale to jsou spíš takové technické věci. Bohužel už jsou i známé situace, kdy se začalo využívat umělé inteligence k vytvoření takového viru, který dokáže obejít i ty lepší způsoby zabezpečení.

Na uživatelské úrovni to jsou stále phishingové kampaně. Bohužel jsou již tak sofistikované a i čeština je téměř dokonalá, že i běžný uživatel e-mailu musí přemýšlet, zda nějakou zprávu, například z banky, opravdu čeká nebo se jedná o spam.

8. Jak ve Vašem zdravotnickém zařízení probíhá prevence kybernetických útoků?

V případě uživatelů je nejdůležitější edukace. Taktéž můžete dělat penetrační testy, kdy si sami vytvoříte podvodné maily a děláte si statistiku, kdo kliknul. Poté případně můžete zintenzivnit školení.

V případě technických zařízení je nezbytné udržovat aktuální všechna aktiva, servery, stanice. To jsou ty záplaty na díry, kterými může vniknout virus. Když se nějaká taková díra objeví, tak většinou rychle vyjdou aktualizace, které je potřeba co nejrychleji v daném prostředí rozšířit.

Dále je potřeba dělat zálohy a kontrolovat je, aby byly funkční. Zálohy je třeba kontrolovat, jestliže jejich nefunkčnost zjistíte až v případě nějakého problému, tak je pozdě. To je v podstatě taky prevence, taková ta aktivní, kdy k tomu aktivně přistupujete a něco děláte.

9. Jak probíhá školení zaměstnanců (např. prostřednictvím e-learningu či osobními školními)?

V nemocničním prostředí je složité všechny zaměstnance hromadně proškolit. Dá se říct nereálné. Školení probíhá zejména kombinací e-learningu, posílání e-mailů a osobních setkání.

V e-mailu je potřeba vždy shrnout nejaktuálnější hrozby, jaké kampaně v dané době začaly chodit, jak může škodlivá zpráva vypadat. Při osobních schůzkách je potřeba vysvětlit aktuální hrozby nabídnou pomoc v případě pochybností ohledně nějakého mailu apod.

Myslím, že je dobré zejména to osobní setkání. Když si s těmi lidmi povídáte osobě, tak jim toho, podle mě, v hlavě zůstane mnohem víc než z e-learningu. Propojí se jim to třeba i s osobním životem a není to jen o tom, že si rychle něco přečtou.

10. Co se děje, když je nemocnice napadená?

V prvé řadě musí být nemocnice připravena na útok. Musí se testovat funkčnost záloh serverů. Zkrátka je potřeba být na to připravený technicky. Pokud je vše dobře nastavené, tak když je napadnut jeden počítač, tak to nemusí znamenat, že bude ochromena celá nemocnice. Mělo by to být segmentované, takže bude ovládnuta třeba určitá část.

Dále by měl být sestavený Plán kontinuity činností. To znamená, že každý ví, co má dělat. Na tento plán poté navazují havarijní plány. Plán kontinuity činností říká, co budeme dělat, když něco nebude fungovat. A havarijní plán pak řeší, jak to obnovit, jak se dostat do původního stavu. Poté se řeší, jak moc zpátky se požadujete dostat (jestli vám stačí zálohy staré měsíc, nebo potřebujete týdenní zálohy), a jak rychle se požadované zvládne obnovit.

Tohle je hezké na papíře, ale samozřejmě ta realita může být jiná.

11. Jaké první kroky musí nemocnice učinit po útoku? Existuje nějaký interní předpis? Jsou nějakým způsobem prováděny zkoušky takové situace?

O tom hovoří ten Plán kontinuity činnosti, který stanoví, co dělat, když je útok. Na ten navazuje Havarijní plán, jehož obsahem je postup jak vše obnovit.

Tyto plány by se měly pravidelně testovat a zkoušet. K takové zkoušce není potřeba reálný výpadek. Stačí si jednou za čas sednout, představit si situaci, že jsou ochromena určitá oddělení a začít říkat postup, co by se dělo, kdyby taková situace skutečně nastala.

V Izraeli mají jednou ročně cvičení, kdy evakuují pacienty z šesti tisícové nemocnice. To se v České republice nezkouší, nebo nevím o nemocnici, která by toto zkoušela. Pravidelně tam také školí ochranku, která ví, co dělat s útočníkem se zbraní. Izrael je permanentně ve válce, i proto je v rámci kybernetických útoků opravdu na špičkové úrovni.

Důležité je mít nachystané všechny plány a pravidelně si je zkoušet. V podstatě, když si ty plány zkoušíte, tak je i vylepšujete. Můžete tak přijít na to, co by v reálně situaci nemuselo fungovat. Tohle se všechno musí dělat, bohužel z časových důvodů se to kolikrát vůbec nedělá a řeší se to, až když problém nastane, a to je pozdě.

12. Na co se dle Vašeho názoru budou útočníci v budoucnosti zaměřovat? Co považujete za příchozí hrozby?

Stále jim půjde o jedno a to samé, pokud to nebudou samozřejmě politicky a mezinárodně cílené útoky, tak se budou zaměřovat na peníze. Nejjednodušší to je nemocnic, protože tam jde o životy.

Ale jak jsem říkal, nemusí to být vůbec cílený útok. Může to být situace, že jsou někde náhodně rozesílány e-maily, na který klikne zaměstnanec nemocnice. Ten hacker neřeší, jestli je v nemocnici nebo ne. V první řádě ho zajímá, jak moc velké to je, kolik může získat peněz, a pak už třeba zjistí, že to je nemocnice, třeba nemocnice, co má nějaké obraty a tak to zkusí a buď mu to projde, nebo neprojde.

Jinak nikdo neví, co bude v budoucnu.

B.3 Rozhovor s respondentem č. 3

Poslední z rozhovorů byl veden se zástupcem NÚKIB.

1. **Jak poskytovatelé zdravotních služeb přistupují k plnění zákonných povinností v oblasti kybernetické bezpečnosti? Co je v tomto ohledu největším problémem?**

Kybernetická bezpečnost je nikdy nekončící proces. Jejímu zajišťování je tak potřeba dlouhodobý a systematický přístup. Platí to ať už po stránce technologického zabezpečení nebo osvěty, v tomto případě zaměstnanců zdravotnických zařízení. Jsou to totiž stále především lidé, jejichž chyba umožňuje úspěšný kybernetický incident. Obecně vzato je tedy problémem absence systematického přístupu, o jehož důvodech lze dlouze spekulovat. Mezi nejčastější příčiny lze ale určitě zařadit nedostatečné financování, obecně platný nedostatek odborníků a nedostatečné bezpečnostní povědomí (proškolení) zaměstnanců.

Sektor zdravotnictví pracuje s citlivými daty nás všech a také proto je v ČR jedním z nejčastějších cílů kybernetických útoků (z pohledu sektorů, které spadají pod ZKB). Sofistikovanost těchto útoků se navíc zvyšuje. Zástupci zdravotnického sektoru si to začínají uvědomovat stále více a kybernetické zabezpečení jejich zařízení se zlepšuje. Obecně je však právě ve zdravotnictví stále opravdu velký prostor pro zlepšení. Vliv na to bude mít také nový zákon o kybernetické bezpečnosti, který obsahuje mj. evropskou bezpečnostní směrnici, tzv. NIS2. Ta zásadně rozšiřuje počet subjektů, které budou spadat pod regulaci zákona. V případě zdravotnictví se bavíme o navýšení z nynějších 44 subjektů na přibližně 1100. Tyto subjekty budou muset nově mít např. jistý bezpečnostní standard a dodržovat další povinnosti nařízené zákonem.

2. Jak je na tom české zdravotnictví po stránce kybernetické a informační bezpečnosti ve srovnání s jinými evropskými státy?

Takováto porovnání se spíše neprovádí a když už ano, je otázka nakolik relevantní jsou jejich výstupy. Důvodem je mj. rozdílný přístup k hodnocení v jednotlivých zemích, na národní úrovni v jednotlivých institucích. Značně problematické je také specifikovat měřitelná kritéria. V neposlední řadě nelze opomíjet ani objektivní fakt, že každá organizace je do značné míry unikátní ekosystém.

3. Úprava NIS2. Je změna nutná? Měla přijít dříve?

NIS2 není revolucí, ale evolucí. S ohledem na povahu nové směrnice se jedná o stěžejní krok k zajištění kybernetické bezpečnosti EU a jejího obyvatelstva v dynamicky se proměňujícím a vyvíjejícím se bezpečnostním a geopolitickém prostředí, v němž hraje kyberprostor a kybernetická bezpečnost obzvlášť důležitou roli. Česká republika se aktivně podílela na vzniku této směrnice. Naší velkou výhodou pak je kvalitně zpracovaný aktuálně platný zákon o kybernetické bezpečnosti, neboť velká část změn prezentovaných v NIS2 je v souladu se systematikou aktuálně platné české regulace.

Přijetím NIS2 dochází zejména k prohloubení a rozšíření již existujícího legislativního rámce, původní Směrnice Evropského parlamentu a Rady EU, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, tzv. směrnici NIS.

Ale abych odpověděl, ano změna je nutná – nelze nereflektovat kontinuálně probíhající technologický vývoj. O správném načasování lze dlouze polemizovat, uvedu ale, že „novelizace“ směrnice přišla po přibližně 6 letech. Pokud chceme racionálně zhodnotit efekt takového předpisu, potřebujeme na to dostatečně dlouhou dobu. A 6 let je s přihlédnutím k transpozičním lhůtám z mého pohledu téměř minimum.

4. Změní se s novým ZKB pro stávající povinné subjekty něco zásadního?

Pro subjekty, které již spadají pod aktuálně platný ZKB a tudíž se musí věnovat své kyberbezpečnosti, se nic zásadního měnit nebude.

Zásadní změnou bude navýšení počtu regulovaných subjektů. Z nynějších 400 to bude více než 6000 subjektů, které budou muset řešit svou

kybernetickou bezpečnost. Česká republika se však díky tomu stane bezpečnější zemí.

Novinkou v regulaci bude také mechanismus na prověřování bezpečnosti dodavatelských řetězců, který dá státu nástroj pro řízení strategických závislostí na dodavatelích ICT pro ty pro stát nejdůležitější systémy – tento mechanismus se bude nicméně týkat pouze cca 150 nejkritičtějších subjektů.

V kontextu řady změn i zájmu odborné veřejnosti o dané téma spustil NÚKIB webové stránky nis2.nukib.cz, jejichž cílem je podávat přehledné a ucelené základní informace o tom, co nová směrnice přináší. Bližší požadavky směrnice NIS2 pak lze najít zde: NIS2: 01 - Obecné informace o směrnici NIS2 (nukib.cz).

5. Máte odhad na kolik nových povinných osob ze sektoru zdravotnictví se nový ZKB bude vztahovat (v režimu základních i důležitých subjektů)? Nebudou povinnosti pro nové subjekty příliš zatěžující?

Pokud jde o celkový počet povinných osob ze sektoru zdravotnictví, předpokládáme nárůst na cca 1100 subjektů (viz odpověď na otázku č. 1). Finální rozdělení do dvou režimů je stále proměnlivé. Pokud jde o tu zátěž, musíme brát ohledem na to, s jak citlivými daty se ve zdravotnictví pracuje a jak postupuje digitalizace tohoto sektoru. Je logické, že s tím ruku v ruce musí jít také bezpečnost. Pro toho, kdo věnuje otázce bezpečnosti zdravotnických dat (tedy velmi citlivých informací o nás občanech) dostatečnou pozornost již dnes, nebudou nové povinnosti zátěží.

6. Jak NÚKIB přistupuje k prevenci kybernetických hrozeb? Liší se nějak prevence v oblasti zdravotnictví od prevence v jiných oblastech?

Aktivit a činností, které NÚKIB dělá v oblasti prevence a s tím spojené osvěty je opravdu velké množství. NÚKIB se mj. činnosti průběžně věnuje dění v kyberprostoru a veškeré podněty průběžně vyhodnocuje. V případě, že je to potřeba a je objevena, zjištěna nějaká hrozba, vydává NÚKIB upozornění, varování nebo nějakou formu opatření. Nejčastěji se jedná třeba upozornění na nějakou zranitelnost. Všechny takové hrozby a zranitelnosti lze nalézt na našich webových stránkách.

Když mluvíme o prevenci nelze nezmínit osvětové a vzdělávací činnosti napříč všemi sektory, spolupráci s národními a mezinárodními organizacemi, pořádání a účasti na kybernetických cvičeních, výzkumu a vývoji v oblasti kyberbezpečnosti a dalším. Můžeme zmínit například veškeré profily NÚKIB na sociálních sítích (IG, Twitter, Facebook, LinkedIn) a instagramový účet @petr.vytrzny. Stěžejní pak je náš vzdělávací portál osveta.nukib.cz, kde naleznete volně dostupnou řadu e-learningových kurzů pro veřejnost i specifické cílové skupiny. Mimo to se dále zapojujeme do řady vzdělávacích akcí, kurzů a přednášek po celé České republice.

NÚKIB se snaží být partnerem pro všechny regulované a v rámci kapacit dělat maxim možného. V současnosti se náš přístup k prevenci ve zdravotnictví neliší od jiných sektorů, je ale na místě zmínit, že po sérii mediálně známých incidentů z let 2019 a 2020 jsme zdravotnickým zařízením v následujících 2 letech věnovali abnormální pozornost po všech stránkách. Z preventivních kroků stojí rozhodně za zmínku 2 běhy tabletop cvičení HealthCzech, audity a následná metodická pomoc v 16 největších nemocnicích, velké množství workshopů a seminářů, e-learning upravený pro potřeby zdravotnického personálu, osvětovou výtahovou kampaň v rámci Festivalu bezpečného internetu, v technické oblasti jsme nabídli průběžné skenování zranitelností a penetrační testy nebo jsme např. vydali jsme veřejně dostupný minimální bezpečnostní standard (dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf (gov.cz)), ten jsme se snažili, bohužel marně, zapracovat také do příslušné legislativy o poskytování zdravotní péče. Dále jsme ve spolupráci s Ministerstvem zdravotnictví vydali doporučení ke snížení kybernetických hrozeb pro zdravotnická zařízení, které se vztahuje na útoky typu DDoS a ransomware. Doporučení obsahuje preventivní kroky, jak incidentům předejít, a jak se zachovat, pokud už útok probíhá.

Pokud jde o konkrétní rady, jak se chovat při kybernetickém incidentu, je třeba brát na vědomí jedinečnost jednotlivých organizací. Proto nelze vytvořit univerzální postup pro všechny, a to ani pro všechny subjekty v sektoru zdravotnictví. Mají různé systémy, sítě a s tím se pojí odlišná rizika. Obecně proto doporučujeme mít připravený vlastní plán, který bude tvořen organizaci na míru a bude obsahovat postupy, jak v případě napadení jednat. Samozřejmě je třeba případný incident nahlásit buď na Vládní CERT, pod který spadají regulované subjekty, nebo na Národní CERT.

7. Jak probíhají kybernetická cvičení? Jak často se provádějí?

Cvičení hrají nezastupitelnou roli při zajišťování kybernetické bezpečnosti České republiky. Umožňují věrně simulovat rozličné typy krizových situací a slouží k prověření různých plánů a postupů, kterými disponují konkrétní organizace. Jde tak o jedinečnou možnost zjistit slabá místa v nastavených postupech a napravit tyto nedostatky v době, kdy na to ještě máme čas. Tedy ne v krizi samotné.

Průběh a zaměření cvičení je odvozeno od toho, komu je určeno a jaké požadavky jsou na něj kladeny. Více informací o druzích cvičení lze najít zde: https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/typy-cviceni/.

Četnost cvičení nelze plošně určit. Jsou cvičení, která se opakují každý rok a z opačné strany také cvičení, která se odehrají pouze jednou. Cvičení je celá řada, lze je členit dle různých kritérií na technická a netechnická, procesní, komunikační, sektorová, národní a mezinárodní nebo ta námi organizovaná a ta, do kterých se zapojíme pouze jako účastník.

Např. v roce 2022 se NÚKIB zapojil různým způsobem (ať už jako cvičící, spoluorganizátor nebo organizátor) celkem do 10 cvičení. Některá byla mezinárodní (Locked Shields – role cvičících i spoluorganizátorů, Cyber Coalition), jiná se odehrávala pouze u nás, např. námi organizované sektorové cvičení Health Czech zaměřené přímo na zdravotnictví. (Popis akce i její průběh je k dispozici zde: Národní úřad pro kybernetickou a informační bezpečnost - Zástupci zdravotnických zařízení si na cvičení Health Czech vyzkoušeli, jak reagovat na kybernetické útoky (nukib.cz).).

8. Jak probíhá součinnost NÚKIB s napadenou nemocnicí při řešení kybernetického útoku a při řešení jeho následků?

Řešení bezpečnostních incidentů patří mezi stěžejní činnosti vládního CERT, který je integrován ve struktuře NÚKIB. Při nahlášení takové události naši odborníci pomáhají IT specialistům napadených organizací po technické stránce a poskytují rady pro další preventivní opatření. Snažíme se vždy poskytnout maximální možnou součinnost a pomoci obětem minimalizovat škody způsobené daným incidentem.

Tým CERT je schopen v rámci řešení incidentu poskytnou celou řadu služeb od analýzy síťových dat a logů až po obecné konzultace postupů. Vzhledem k navázané rozsáhlé spolupráci napříč různými institucemi lze poskytnout pomoc při zprostředkování kontaktů jak s českými bezpečnostními týmy, tak se zahraničními partnery při řešení bezpečnostních incidentů s mezinárodním přesahem.

Ve vážných případech, pak náš tým vyráží přímo do zasažené nemocnice (nebo obecně instituce), kde je po nezbytně potřebnou dobu součástí týmu řešícího incident. Náš primární cíl je minimalizovat škody a negativní dopady (např. nedostupnost služby). Nabízených služeb je celá řada a situace od situace např. i dle zájmu zasažené organizace jsou poskytovány. Úplný přehled nabízených služeb je na našem webu: Národní úřad pro kybernetickou a informační bezpečnost - Poskytované služby (nukib.cz).

O hlášeních incidentů a následné reakci lze více zjistit zde: Národní úřad pro kybernetickou a informační bezpečnost - Hlášení incidentů (nukib.cz). Zcela klíčovým aspektem je včasné zahájení komunikace, nahlášení incidentu či podezřelých událostí.