DOI: 10.35191/medsoft_2021_1_33_21_24

ZKUŠENOSTI Z IMPLEMENTACE KYBERNETICKÉHO ZÁKONA V NEMOCNICI

Jiří Knápek

Anotace

V našem článku se pokusíme přiblížit proces implementace požadavků Zákona o kybernetické bezpečnosti ve fakultní nemocnici. Jednotlivé kroky implementace, vytvořené dokumenty až po vytvořené výstupy. S nemocnicí jsme si prošli i metodickým auditem NUKIBu – Národního úřadu pro kybernetickou bezpečnost.

Klíčová slova

kybernetická bezpečnost, řízení rizik, řízení aktiv, metodiky, bezpečnostní politiky, zákon o kybernetické bezpečnosti, audit kybernetické bezpečnosti, řízení rizik, řízení aktiv, SW podpora

2 Úvod

V České republice byl přijat Zákon o kybernetické bezpečnosti (dále jen ZoKB) v roce 2014.

Vyhláškou č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby jsou určena Zdravotnická zařízení, která se musí řídit Zákonem. Podmínky vyhlášky se postupně zpřísňují a postupně zahrnují od největších nemocnic řízených přímo Ministerstvem zdravotnictví ČR i menší zařízení zřizovaná kraji a výjimečně i obcemi.

Větší část nemocnic se tak staly „povinnou" osobou dle ZoKB a postupně musí implementovat jednotlivé požadavky ZokB a jeho prováděcích vyhlášek.

2.1.1 Specifické podmínky nemocnice z pohledu kybernetické bezpečnosti

Areál nemocnice je extrémně rozsáhlý s velkým pohybem lidí (pacienti, jejich doprovod, studenti, dodavatelé apod.) Bezprostředně vedle areálu je konečná stanice metra a velký dopravní uzel MHD. To samozřejmě klade vysoké nároky na zajištění fyzické bezpečnosti, počítačové sítě v rámci areálu jsou velmi rozsáhlé s vysokými nároky na dostupnost.

Velký počet lůžek znamená samozřejmě i velký počet zaměstnanců. To se projevuje samozřejmě v počtu a charakteru licencí, procesů přidělování přístupových práv, vyšší jsou nároky na průběžné školení nových zaměstnanců.

Důležitým faktorem je i výzkum a vývoj, který klade na bezpečnost další požadavky.

3 Výchozí podmínky implementace zákona v podmínkách nemocnice

V čem je nemocnice jiná … Obecné problémy, které jsou typické pro zdravotnická zařízení.

Udržet nějak rozumně „perimetr fyzické bezpečnosti" je nemožné…

Nemocnici nelze obehnat ostnatým drátem, omezit výrazně pohyb osob. Pak by to nebyla nemocnice. Jakékoliv zpřísnění navíc narazí na další cíle nemocnice v oblasti vstřícnosti a přístupnosti pro pacienty a návštěvníky.

Situaci zkomplikuje i to, že většina nemocnic část rozsáhlého areálu pronajímá: ordinace, občerstvení. Speciálně fakultní nemocnice jsou nějakou formou „prorostlé" s akademickým světem.

Na druhou stranu jsou pracoviště, kde je nezbytné pohyb osob a fyzickou bezpečnost omezit ještě výrazněji: operační sály, laboratoře apod. Kde se s tím potkáme?

Vyhláška 82/2018 o kybernetické bezpečnosti

- § 10 Řízení provozu a komunikací
- § 17 Fyzická bezpečnost
- § 18 bezpečnost komunikačních sítí

Hodně lůžek = velký počet zaměstnanců, velká administrativa…

Lůžková péče je personálně velmi náročná a aktuální péče je ještě náročnější. Velké areály často historických budov potřebují zkušenou údržbu, pro personál i pacienty je potřeba zajistit stravu v několika dietních režimech a přidají se další „speciality": vytápění, prádelna, technické plyny…

Každá nemocnice se utápí v papírech, které často ani nesouvisejí s poskytováním zdravotní péče. Co z toho vyplývá?

Velké množství zaměstnanců, které je potřeba pravidelně školit, velké množství různorodých dodavatelů, specializované aplikace, které přímo nesouvisejí s poskytování zdravotní péče, ale nemocnice bez nich nemůže fungovat.

Jedna relativně pozitivní věc zde je – při velkém počtu zaměstnanců je potřeba mít proces přidělování přístupových práv. Kde se s tím potkáme? Prakticky všude, ale asi nejvíce:

- § 8 Řízení dodavatelů
- § 9 Bezpečnost lidských zdrojů
- § 12 Řízení přístupu
- § 13 Akvizice, vývoj a údržba
- § 19 Správa a ověřování identit
- § 20 Řízení přístupových oprávnění

Věda, výzkum a moderní technika

Špičková pracoviště poskytují kvalitnější péči a samozřejmě to souvisí s prestiží daného zařízení. Je samozřejmě v zájmu vedení nemocnice i pacientů všechny tyto aktivity podporovat.

Z pohledu kybernetické bezpečnosti je to hromada starostí navíc. Výzkum je často spojen s mezinárodními registry – další prostupy do síťového perimetru.

S moderními technologiemi často souvisí i specializovaný software (např. speciální 3D zobrazování, analýzy dat). Takže už tak velký počet aplikací se ještě zvýší. Projekty jen výjimečně mají v rozpočtu kapitolu kybernetická bezpečnost.

Takzvané „modality" jsou tak jedním z nejcitlivějších a nejproblematičtějších oblastí ochrany dat v prostředí špičkových nemocnic.

„Povzdech" na konci kapitoly

Zákon a vyhláška tak nějak nepočítají se stavem, kdy většina nemocnic je příspěvkovými (rozpočtovými) organizacemi.

Peníze, peníze, peníze (v případě pražských nemocnic i nulový přístup k dotacím).

4 Postup implementace

Zadáním projektu bylo splnit v průběhu roku (zákonem stanovené lhůty) základní požadavky Zákona a vyhlášky o kybernetické bezpečnosti.

Rozhodně nebylo cílem splnit všechna technická opatření, protože to je ve stanovené lhůtě zcela nereálné. Tento přístup je plně v souladu se zákonem a vyhláškou.

4.1 Vstupní analýza

Na začátku projektu měl tým k dispozici dvě analýzy, které sice vznikly k zavádění GDPR, ale fakticky řešili kybernetickou bezpečnost z pohledu ISMS (obecnější norma než Zákon a vy-

DOI: 10.35191/medsoft_2021_1_33_21_24

hláška). Řada závěrů a doporučení v dokumentech byla nerealizovatelná, protože nezohlednila reálné podmínky nemocnice.

V rámci projektu se udělal trochu jiný typ analýzy. „Checklist" požadavků vyhlášky s odkazem na paragraf a odstavec a způsob a míra naplnění. Vznikl tak přehled, který nezapomíná na žádnou oblast.

4.2 Dokumenty a administrativa

4.2.1 Návrh bezpečnostních politik vyžadovaných vyhláškou

Po diskuzích s právníky a příslušnými odbory, byly základní bezpečnostní politiky přijaty ve formě „interních směrnic" tak aby dokument měl charakter řídícího dokumentu v rámci nemocnice – v souladu s jeho platnými normami.

Následně byl spuštěn řádný interní připomínkovací proces. Ten byl celkem zdlouhavý, komplikovaný, ale ve finále tyto dokumenty akceptovalo celé vedení nemocnice.

Dokumenty, které mají omezenou platnost, např. Metodika řízení aktiv a rizik byly vydány ve formě metodických pokynů apod.

Současně byly identifikovány navazující řídící dokumenty a v rámci nápravných opatření byly postupně aktualizovány.

4.2.2 Analýza aktiv a rizik

Obě analýzy probíhaly na základě již dříve schválené metodiky „Metodika analýzy a řízení rizik" a „Metodika identifikace a správy aktiv".

Pro analýzu primárních aktiv byl zvolen přístup workshopu s garanty. Garantům primárních aktiv bylo třeba i detailně vysvětlit jejich roli a všechny souvislosti.

Pro podpůrná aktiva byl zvolen trochu jiný přístup zahrnující sérii schůzek s garanty podpůrných aktiv, administrátory, případně jinými technickými pracovníky. Na tuto analýzu navázala i analýza rizik.

Problém, na který narazí v rámci analýzy každý, je, jak správně zvolit typová (agregovaná) podpůrná aktiva. Je samozřejmě nereálné evidovat i sebemenší komponentu, na druhou stranu příliš velká agregace může skrýt některá slabá místa.

Specifickým problémem každé nemocnice jsou tzv „modality" (digitální diagnostická zařízení používaná ve zdravotnictví). Jeho správu zajišťuje odborné lékařské pracoviště, je zde velká role dodavatele a od ICT infrastruktury se připojuje jen jedním bodem.

4.2.3 Plán zvládání rizik a prohlášení o aplikovatelnosti

Na základě výše uvedeného, byl zpracován plán zvládání rizik.

Plán zohlednil několik zdrojů.

- Již dříve navržená opatření (např. vycházející ze zavádění GDPR), která byla aktualizována, a nově byly stanoveny priority s ohledem na analýzu rizik.
- Již realizované projekty nebo projektové záměry.
- Nová opatření, která se soustředila více na organizační a administrativní oblast.
- Technická opatření, která mají za cíl připravit realizační projekty na vyhlášku předepsaná technická opatření.

Protože zákon a vyhláška vycházejí z normy ISO 27000, je prohlášení fakticky nejdůležitějším dokumentem v oblasti kybernetické bezpečnosti.

4.3 Interní audit KB

S určitým zpožděním byl proveden první interní audit dle interní metodiky auditu kybernetické bezpečnosti, tak jak jej požaduje vyhláška.

Audit použil obdobný „checklist" jako vstupní analýza a zmapoval aktuální stav realizace. Co je realizováno, a v jakých oblastech jsou ještě rezervy.

Další audity se již zaměřují na jednotlivé oblasti bezpečnosti, přidělování přístupových práv, práci administrátorů apod.

4.4 Evidence v systému TAS

Aktiva a rizika je samozřejmě v souladu s požadavky zákona a vyhlášky potřeba evidovat „auditovatelným" způsobem. Nemocnice již od začátku věděla, že evidence s pomocí MS Excel má svoje úskalí a proto zvolila evidenci v systému „TAS".

Základní výhoda systému je v následujících oblastech:

Každé evidované aktivum, riziko, nápravné opatření apod. má svoji kartu, která umožní přehledně evidovat všechny náležitosti, změny (auditní stopa).

Je zachována vnitřní logika mezi aktivy, riziky a nápravnými opatřeními (vztah rizika k aktivu, hrozbě a zranitelnosti, vzájemné vazby mezi aktivy, vazba mezi rizikem a nápravným opatřením apod.). Tyto závislosti je již prakticky nemožné postihnout evidencí na úrovni MS Excelu.

Výstupem ze systému jsou:

Uživatelsky definovatelné reporty do MS Excel, tj. lze on-line vygenerovat aktuální přehled (katalog) aktiv, rizik, nápravných opatření.

Standardní tiskové výstupy do přehledových záznamů – ty se prakticky uplatňují především u primárních aktiv, kdy je pro garanta snadnější orientace v přehledné kartě, kde má všechny potřebné informace o aktivu než „vyfiltrovaná" excelová tabulka s desítkami sloupců.

5 Závěr

Aby bylo možné splnit požadavky zákona, musí být splněno několik základních předpokladů.

Podpora managementu – toto je naprosto zásadní předpoklad a bez jeho podpory nelze administrativní a organizační opatření prosadit.

Odborné a realistické vedení kybernetické bezpečnosti. Manažer kybernetické bezpečnosti musí samozřejmě rozumět kybernetické bezpečnosti a ICT, ale jsou také věci, které nesmí…

- Nesmí být interně ve střetu zájmů, kumulaci řady funkcí vylučuje i samotná vyhláška 82/2018, ale přesto tato ustanovení nebývají vždy dodržována.
- Nesmí fungovat jako „stínový" manažer ICT a zasahovat mu do kompetencí. Vymýšlet koncepce, projekty. To je z části role architekta.
- Nesmí přeceňovat technická opatření, která sama od sebe bezpečnost zcela nezajistí. (To je pro bývalé ICT administrátory vnitřně poměrně velký rozpor).
- Nesmí mít odpor k administrativě, protože značná část souvisí s administrativou, interními předpisy, analýzami.
- Nesmí se nechat odradit určitou nepopularitou své pozice, která bude vyplývat z kontroly dodržování interních směrnic a postupů.

Vedení ICT a odborný ICT pracovníci

90% práce není o zázračných projektech typu „když si koupíte toto řešení, máte vše vyřešeno…". Je to především o každodenní důsledné práci administrátorů a jejich odbornosti.

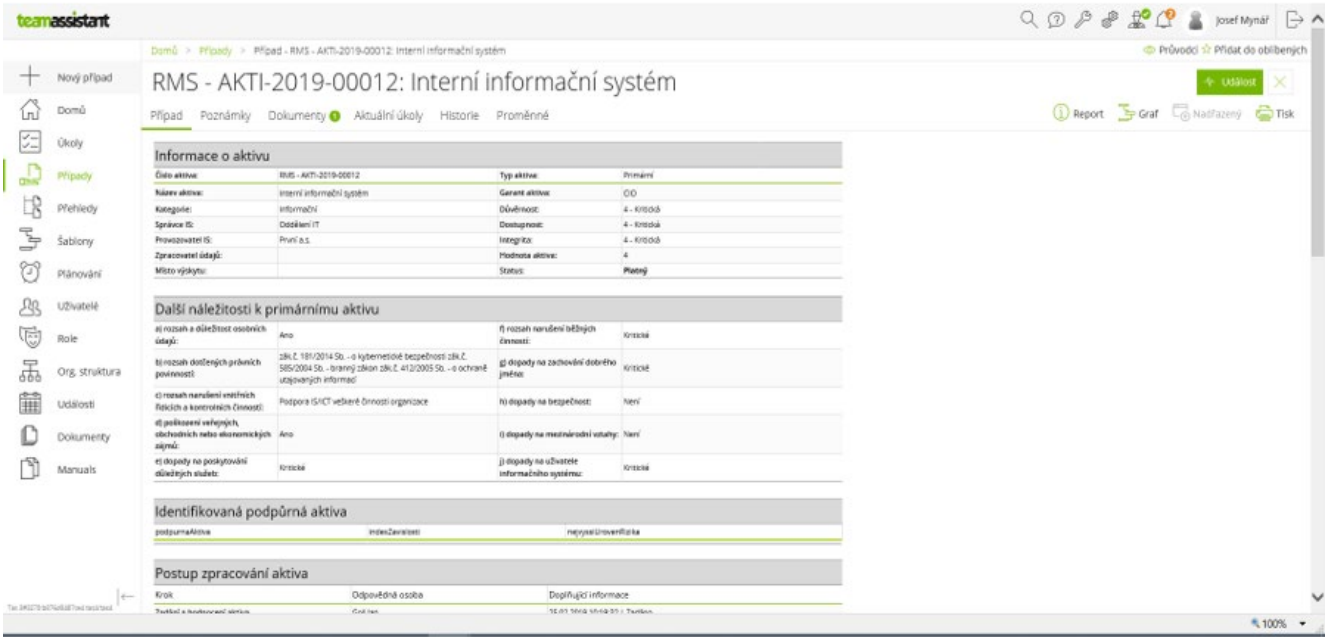
DOI: 10.35191/medsoft_2021_1_33_21_24

Základní ICT infrastruktura

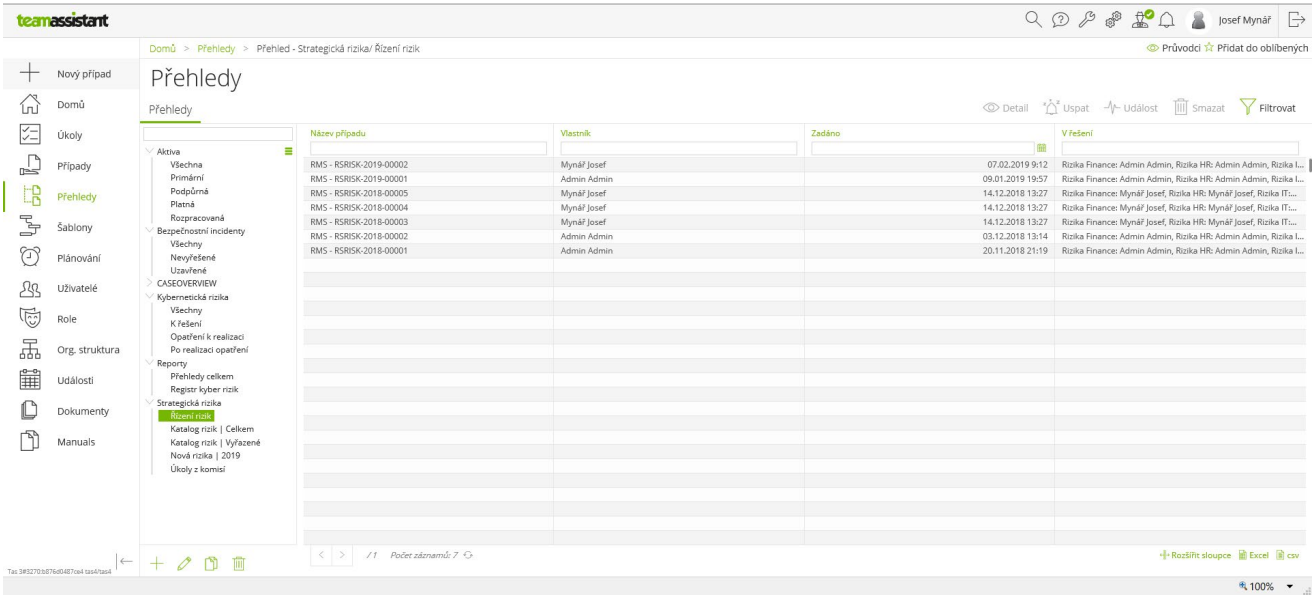
ICT technologie mají své zákonitosti, a pokud nejsou pevné základy, nelze zlepšovat ani oblast kybernetické bezpečnosti. Hlavním problémem je často nedostatek odborných pracovníků a příspěvková organizace se platově například s bankami a pojišťovnami nemůže srovnávat.

A naposledy to, co souvisí se vším výše uvedeným

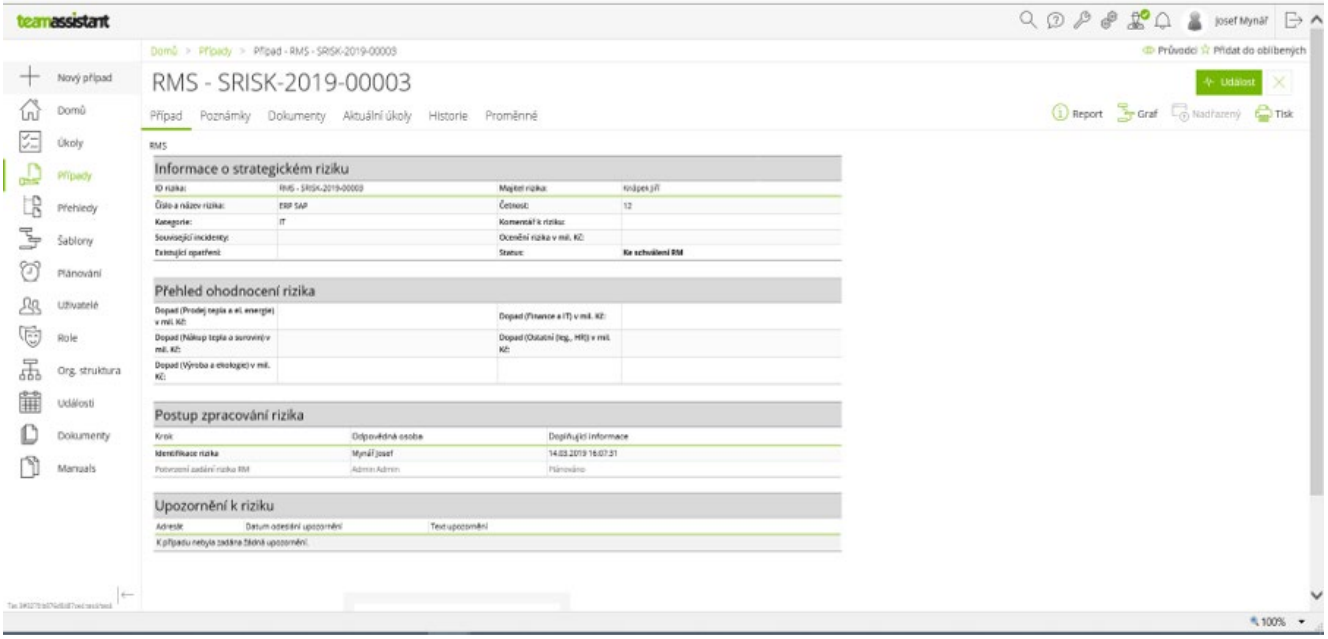
Důsledná analýza rizik a realizace nápravných opatření (rozvojové projekty) na jejich základě. Nepřipravené projekty, stejně jako v jiných oblastech, končí neúspěchem.



Obrázek 1 – Karta aktivita



Obrázek 2 – Titulní obrazovka aplikace TAS KYBEZ – přehled SW úloh pokrývající kybernetický zákon.



Obrázek 3 – Karta rizika

Použité zdroje

[1.] Zákon č. 181 /2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, Vyhláška č. 82/2018 Sb.

Jiří Knápek – manažer realizace společnosti Netia® s.r.o.

Působí na pozici manažera realizace projektů ve společnosti NETIA®, společnost je dodavatelem SW a služeb s orientací na projektové řízení, řízení rizik, interních auditů, implementaci požadavků kybernetické bezpečnosti a řešení GDPR/Data Protection Officer.

Společnost NETIA® se zaměřuje především na tyto oblasti:

- Projektové řízení – SW Oracle – Primavera – dodávka licencí, školení a implementace, podpora BIM;
- Řešení pokrytí Zákona o kybernetické bezpečnosti;
- Řízení rizik a interních auditů – SW Risk manager tool – dodávky licencí, školení, implementace – cloudové řešení;
- GDPR/Data Protection Officer – konzultace a zastupování firem a úřadů;
- Oborová řešení pro řízení rizik – zdravotnictví, strojírenství, veřejná správa;
- Řízení rizik – tvorba metodik a směrnic;

Pracovníci společnosti NETIA® s.r.o. mají rozsáhlé zkušenosti z mnohaletého působení v IT a realizace projektů v České a Slovenské republice.

www.netia.cz

Kontakt

Jiří Knápek
Netia®®s.r.o., Hliníky 259, 679 72 Kunštát
Mob: +420 730 827 844
e-mail: *knapek@netia-it.cz*
http://www.netia.cz