Kybernetická bezpečnost v laboratorních provozech

M. Novotný

Již pátým rokem se některé veřejnoprávní subjekty musí řídit požadavky kladenými na jejich elektronické informační systémy Zákonem o kybernetické bezpečnosti č. 181/2014 Sb. Na poskytovatele zdravotní péče však tyto požadavky dopadly zásadním způsobem až s loňskou novelou zákona podnícenou směrnicí Evropské komise s názvem „Network Information Security“ [1)]. Na základě této novely vznikl Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), jehož úkolem je, mimo jiné, určit tzv. „provozovatele základní služby“. NÚKIB určil 16 zdravotnických zařízení, která splňují zákonná kritéria pro označení „provozovatel základní služby“.

Článek si klade za cíl stručně shrnout dopady výše zmíněných legislativních změn na provoz laboratorních informačních systémů těchto 16 vybraných poskytovatelů zdravotní péče.

[1)] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Teoretické či reálné (ne)bezpečí?

V éře informační společnosti není vždy snadné odlišit realitu od pouhých vizí a pravdu od marketingu. Strach bývá dobrý nástroj k dosažení zamýšlených cílů na úkor vystrašeného. V oblasti kybernetické bezpečnosti tomu není jinak, nicméně konkrétní sledování dokazují existenci konkrétních bezpečnostních incidentů, z nichž některé mají za následek reálné škody. Jeden mediálně zviditelněný příklad za všechny – útok nežádoucího kódu typu „ransomware“ na Britský národní zdravotní systém (NHS) v květnu 2017 způsobil škodu vyčíslenou na 92 mil £. [1]

Je evidentní, že i méně významní poskytovatelé zdravotních služeb trpí útoky vedenými z kybernetického prosotoru (nejčastěji z Internetu) proti jejich elektronickým informačním systémům. Podle našich zkušeností z posledních čtyř let jsou v ČR napadána spíše menší zdravotnická zařízení včetně laboratorních provozů. Shodou okolností podobná situace nastala letos v dubnu v jednom soukromém laboratorním řetězci, kde infiltrace typu ransomware zašifrovala virtuální server laboratorního informačního systému. Provoz několika laboratoří byl vážně ohrožen, odstranění následků útoku trvalo celý den. Ransomware je škodlivý kód, který šifruje data na přístupném souborovém systému včetně síťového – tedy působí i prostřednictvím lokální počítačové sítě. Za obnovení přístupu k takto znepřístupněným datům pak útočník požaduje platbu na anonymní účet.

Bez ohledu na výše řečené, legislativní požadavky kladené na poskytovatele základních služeb jsou celkem jednoznačné a ti ostatní se jimi mohou dobrovolně inspirovat. Naplnění legislativních požadavků na kybernetickou bezpečnost znamená zavedení řady opatření, která však lze z části financovat zejména v rámci evropských dotačních programů IROP.

Když laboratoř „nejede“...

V oblasti zdravotnictví byly jako poskytovatelé základní služby určeny všechny fakultní nemocnice (včetně ÚVN a s výjimkou Fakultní nemocnice u sv. Anny v Brně), Thomayerova nemocnice, Nemocnice Na Bulovce, Krajská zdravotní a.s., Krajská nemocnice Liberec, a.s., Nemocnice České Budějovice, a.s., Nemocnice Pardubického kraje, a.s. a Krajská nemocnice T. Bati, a.s. Jde o největší zdravotnická zařízení co do rozsahu a významu poskytovaných zdravotních služeb, tedy jejich určení je na první pohled logické. Proč ale zatěžovat laboratorní provoz obavami z kybernetických útoků? Odpověď je nasnadě: „Když nejede laboratoř, nemůžeme operovat.“ Tak přibližně zněla věta, kterou jsem jako mladý technik společnosti Stapro slyšel před více než 20 lety na svou adresu v jedné nemocnici, kde jsme řešili technickou havárii serveru, na němž byl provozován laboratorní informační systém. Protože poskytování základní služby se vztahuje na zdravotní péči jako celek, nelze ji dále dělit na jednotlivé odbornosti a dílčí informační systémy. I z pohledu laboratorního provozu je tedy třeba naplnit zákonem stanovené povinnosti, jež lze shrnout do těchto bodů:

- zavést a provádět bezpečnostní opatření
- vést o nich dokumentaci
- zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů
- detekovat kybernetické bezpečnostní události
- hlásit kybernetické bezpečnostní události NÚKIB

Bezpečnostní opatření se dělí na dvě velké skupiny:

a) Organizační opatření
b) Technická opatření

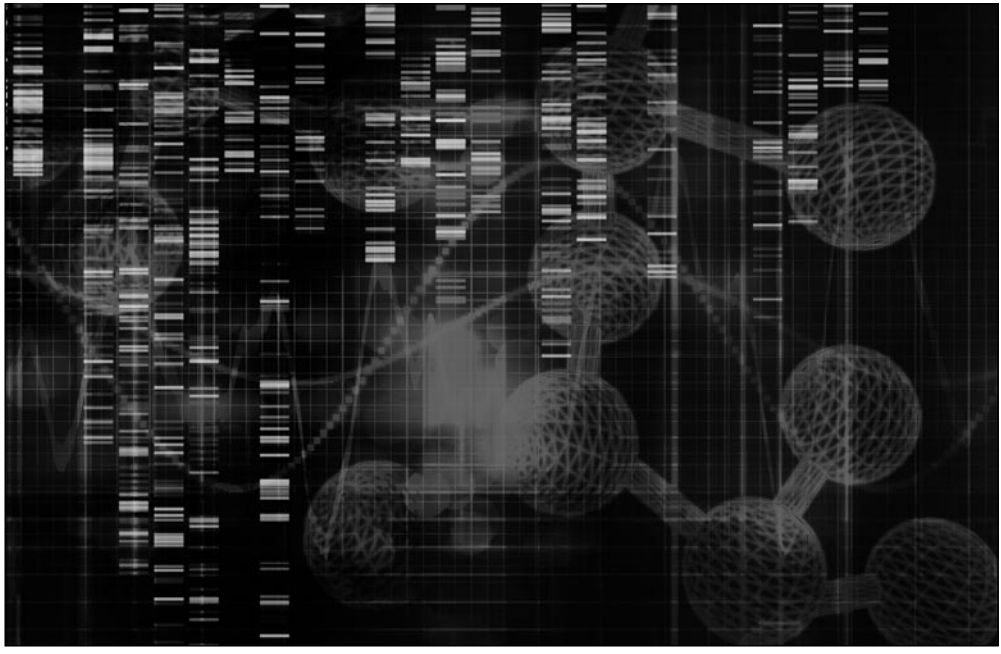
Zatímco organizační opatření jsou plně v rukou provozovatele resp. správce informačních systémů (nejčastěji samotného zdravotnického zařízení), technická opatření se týkají i dodávek informačních technologií včetně laboratorních informačních systémů. O konkrétních opatřeních pojednává velmi podrobně prováděcí předpis k Zákonu o kybernetické bezpečnosti [2].

Vyhláška o kybernetické bezpečnosti - síto na informační systémy

Původní prováděcí předpis k Zákonu o kybernetické bezpečnosti byl v létě 2018 nahrazen novou vyhláškou [2], která velmi systematicky zpracovává požadavky na zajištění informační bezpečnosti a disponuje řadou užitečných informací, takže na ni lze pohlížet jako na metodickou příručku zavádění systému řízení informační bezpečnosti. S vědomím, že laboratorní informační systém FONS Openlims společnosti Stapro s.r.o. je nasazen v 11 z 16 zdravotnických zařízení, na něž přímo dopadají ustanovení a požadavky Zákona o kybernetické bezpečnosti, jsme přistoupili k analýze potřebných změn jak ve vlastním aplikačním programovém vybavení, tak i v doporučeném způsobu jeho implementace do prostředí laboratorního provozu. Konkrétně jsme se zaměřili na bezpečnostní opatření, které musí informační systémy (IS) naplňovat, a položili jsme si otázky shrnuté v následující tabulce:

Předpisy:	Vyhláška 82/2018 Sb., § 19 Správa a ověřování identit
(2) a)	Je vynuceno ověření identity (autentizace) uživatelů, administrátorů a služeb před zahájením aktivit v IS?
(2) b)	Je možné řízení počtu možných neúspěšných pokusů o přihlášení?
(2) c)	Jak je zajištěna odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití?
(2) d)	Jsou autentizační údaje ukládány ve formě odolné proti offline útokům (odcizení úložiště identit a následné prolomení)?
(2) e)	Jak je zajištěno opětovné ověření identity po určené době nečinnosti?
(2) f)	Jak je zajištěno dodržení důvěrnosti autentizačních údajů při obnově přístupu po určité době nečinnosti?
(2) g)	Jak je zajištěna centralizovaná správa identit?
(3)	Je umožněna vícefaktorová autentizace?
(4)	Pokud není umožněna vícefaktorová autentizace, je umožněna autentizace pomocí kryptografických klíčů?
(5) a), b), c), e)	Jak je možné vynutit pravidla tvorby hesla k uživatelskému účtu ? (min. délka, max. délka množina znaků a jejich kombinace, permutace znaků, triviální kombinace, slova...)
(5) d), e), f)	Jak je možné vynutit pravidla změny hesla k uživatelskému účtu ? (min. a max. doba, jedinečnost hesla v historii)
(6) a)	Je možné vynutit bezodkladnou změnu výchozího (default) hesla po jeho prvním použití?
(6) a)	Lze zajistit bezodkladné zneplatnění hesla sloužící k obnovení přístupu po prvním použití tohoto hesla nebo uplynutím nejvýše 60 minut od jeho vytvoření? (situace, kdy byl původní přístup ztracen díky zablokování účtu, zapomenutí hesla apod.)
Předpisy:	Vyhláška 82/2018 Sb., § 20 Řízení přístupových oprávnění
b)	Existuje centralizovaný nástroj pro řízení přístupových oprávnění ke čtení dat, zápis dat a změnu oprávnění?
Předpisy:	Vyhláška 82/2018 Sb., § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

(2) b)	Označte seznamem číslic, které údaje o aktivitách v IS se zaznamenávají do logu: 1. datum a čas včetně specifikace časového pásma, 2. typ činnosti, 3. identifikaci technického aktiva, které činnost zaznamenalo (např. jméno serveru), 4. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, 5. jednoznačnou síťovou identifikaci zařízení původce a 6. úspěšnost nebo neúspěšnost činnosti.
(2) d)	Označte seznamem číslic, které aktivity/stavy v IS se zaznamenávají do logu: 1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, 2. činností provedených administrátory, 3. úspěšné i neúspěšné manipulace s účty, oprávněními a právy, 4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, 5. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, 6. zahájení a ukončení činností technických aktiv, 7. kritická i chybová hlášení technických aktiv, 8. přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí (logů).
(2) c)	Jak je zajištěna ochrana logovaných informací proti neoprávněnému čtení či modifikaci?
(3)	Lze uchovat logové záznamy po dobu min. 18 měsíců?
Předpisy:	Vyhláška 82/2018 Sb., § 25 Aplikační bezpečnost
(1)	Obsahuje-li IS webové služby nebo webové aplikace, byly provedeny testy zranitelností dle OWASP v aktuální verzi?
Předpisy:	Vyhláška 82/2018 Sb., § 26 Kryptografické prostředky
a)	Jaké IS používá kryptografické algoritmy a jaké délky kryptografických klíčů? K čemu je používá?
b)	Umožňuje používaný systém správy klíčů a certifikátů audit své činnosti? Jak?



Na základě odpovědí na uvedené otázky byly upraveny některé funkční vlastnosti FONS Openlims tak, aby bylo tento systém možné provozovat ve shodě s platnou legislativou. Řady potřebných vlastností bylo dosaženo integrací FONS Openlims s adresářovou službou MS Active Directory, která je dnes ve velkých zdravotnických zařízeních často využívána jak pro správu elektronických identit a přístupů ke zdrojům IS, tak pro správu klientských stanic a jejich operačního prostředí. To se týká například i možnosti používat čipové karty pro autentizaci uživatelů a logování událostí souvisejících s autentizací uživatelů k IS.

Shrnutí

Aktuální situace v oblasti kybernetické bezpečnosti neposkytuje důvod k velkému klidu či dokonce přehlížení potřeby chránit důležité elektronické informační systémy. Legální provoz informačních systémů poskytovatelů základní služby předpokládá naplnění organizačních a technických opatření daných zákonem, jež je potřeba respektovat již při výběru a implementaci vlastního aplikačního programového vybavení laboratorních provozů.

Zásadní roli na poli kybernetické bezpečnosti rovněž hrají partnerské vztahy mezi dodavateli laboratorních informačních systémů a jejich provozovateli. Ta se projeví zejména v prevenci slabých míst informačního systému již při jeho implementaci ale také v okamžiku nežádoucího bezpečnostního incidentu, kdy je potřeba jednat rychle a pokud možno bezchybně.

Společnost Stapro s.r.o. jako dodavatel IS pro zdravotnictví dlouhodobě monitoruje reálný stav vývoje kybernetických hrozeb, sbírá zkušenosti s jejich řešením a ve spolupráci se specializovanými partnery testuje, zabezpečuje a implementuje své aplikace u poskytovatelů zdravotních služeb dle obecně uznávaných metodik a platné legislativy.

Prameny:

[1] https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs.

[2] Vyhláška č. 82/2018 Sb.,o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)