PROBLEMATIKA KYBERNETICKÉ BEZPEČNOSTI V ŽELEZNIČNÍ DOPRAVĚ

THE ISSUE OF CYBER SECUTIRY IN RAIL TRANSPORT

Přemysl Šrámek[1]

Anotace: Tento článek se zabývá problematikou kybernetické bezpečnosti v železniční dopravě, a to především z pohledu manažera železniční infrastruktury. Je vysvětleno, proč je manažer železniční infrastruktury správcem kritické informační infrastruktury, jaká bezpečnostní opatření by měl dle platné legislativy zavést a jaké mohou být nalezeny nedostatky v implementaci této problematiky ze strany auditních orgánů.

Klíčová slova: bezpečnostní opatření, kybernetická bezpečnost, manažer železniční infrastruktury.

Summary: This article deals with the issue of cyber security in rail transport, especially the rail infrastructure manager point of view. It is explained, why the railway infrastructure manager is the critical information infrastructure administrator, which security measures should he apply and which imperfections there should be found in the implementation of this issue by auditors.

Key words: security measures, cyber security, rail infrastructure manager.

ÚVOD

Železniční doprava procházející překotným vývojem se dnes již vůbec neobejde bez počítačové podpory řízení jednotlivých procesů. Od tvorby jízdního řádu přes přidělování kapacity, řízení železničního provozu až po výpočet poplatku za užití železniční dopravní cesty jsou veškeré činnosti vedeny již standardně v elektronické podobě, a to prostřednictvím většího množství vzájemně provázaných systémů.

Tyto systémy je ale nezbytné kromě základní údržby a rozvoje také chránit před útoky zvenčí, neboť jejich selhání či omezení funkčnosti je značným rizikem s celosíťovým dopadem.

1. LEGISLATIVNÍ RÁMEC

1.1 Základní zákonná úprava

Problematika kybernetické bezpečnosti je v České republice ošetřena prostřednictvím zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění (ZKB) (1). Prováděcím předpisem k tomuto zákonu je vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti,

[1] Ing. Přemysl Šrámek, Ph.D., Univerzita Pardubice, Dopravní fakulta Jana Pernera, Katedra technologie a řízení dopravy, Studentská 95, 532 10 Pardubice, Tel.: +420 724 460 466, E-mail: premeksramek@centrum.cz

v platném znění (VKB) (2). Důležitým právním předpisem je též nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v platném znění (3).

1.2 Kritická informační infrastruktura

ZKB nabyl účinnosti 1. ledna 2015. Jeho hlavním cílem je ochrana kritické infrastruktury a informačních systémů, které jsou podstatné pro běh státu.

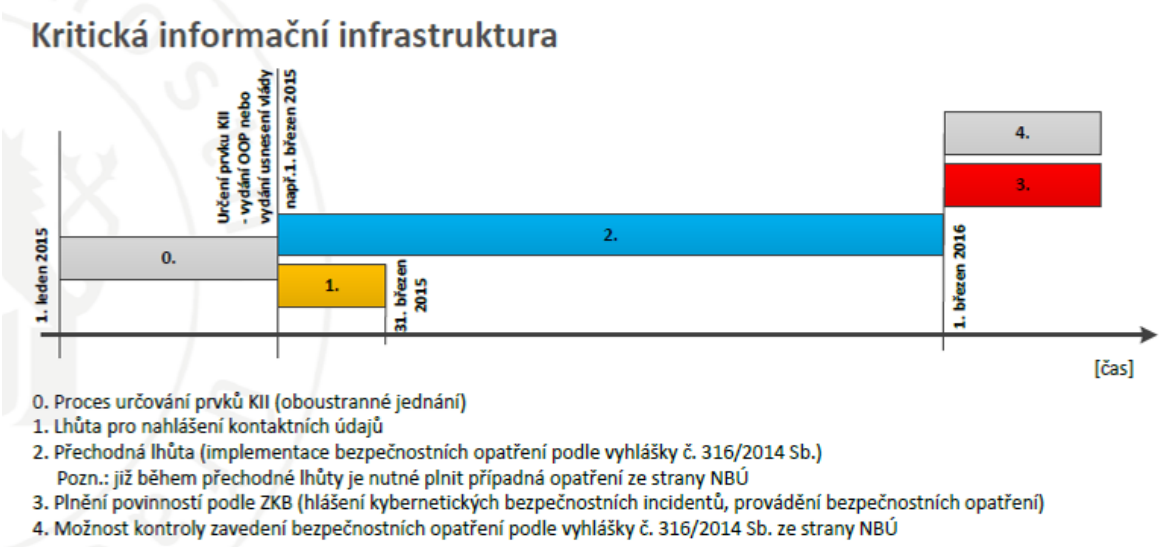
Kritickou informační infrastrukturu (KII) určuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v platném znění. Proces určování, resp. posuzování, zda systémy naplňují stanovená kritéria, probíhá ve spolupráci s daným správcem systémů s využitím analýz dopadu incidentů a dalších podkladů. Samotný akt určení potom probíhá dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), v platném znění, a závisí na povaze subjektů – organizační složky státu jsou určeny na návrh NÚKIB usnesením vlády, ostatní subjekty pak opatřením obecné povahy vydaným NÚKIB. Obecně se jedná o takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb, zdraví nebo ekonomiku.

Aby byl informační systém určen jako KII, musí splňovat určitá kritéria stanovená legislativou. Jsou to průřezová kritéria určující míru závažnosti důsledků narušení těchto systémů a dále kritéria odvětvová, která vymezují pouze některé klíčové oblasti, které jsou pro stát, resp. pro zajištění jeho společenských a hospodářských funkcí, důležité. Z každé skupiny kritérií musí systém splnit alespoň jedno (4).

Manažer železniční infrastruktury coby její celosíťový provozovatel naplňuje v případě kompletního zastavení železničního provozu v řádu hodin a více minimálně 2 ze 3 průřezových kritérií dle § 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v platném znění. Konkrétně je naplněno hledisko ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu a hledisko dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob. Odvětvová kritéria jsou posléze uvedena v příloze č. 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v platném znění, kde je železniční doprava uvedena jako odvětvové kritérium V. B. Informační systémy manažera železniční infrastruktury tak splňují kritéria stanovená legislativou a jsou nepochybně KII.

2. BEZPEČNOSTNÍ OPATŘENÍ PODLE ZKB

Národní centrum kybernetické bezpečnosti (NCKB), resp. NÚKIB určí opatřením obecné povahy informační a komunikační systémy manažera železniční infrastruktury jako prvky KII na území České republiky. Nabytím účinnosti tohoto opatření začínají pro manažera železniční infrastruktury plynout přechodné lhůty k provádění povinností podle ZKB, mimo jiné i přechodná roční lhůta, více na Obr. 1.



Zdroj: NCKB, úprava autor

Obr. 1 – Lhůty a přechodná období

Dle § 30 ZKB je manažer železniční infrastruktury coby správce a provozovatel KII povinen nahlásit kontaktní údaje do 30 dnů od nabytí účinnosti opatření obecné povahy, které určilo jeho informační či komunikační systém jako KII. Jeden rok od nabytí účinnosti opatření obecné povahy poté běží přechodná lhůta pro implementaci bezpečnostních opatření dle VKB a splnění všech povinností dle ZKB.

Dle ZKB jsou bezpečnostní opatření členěna do dvou základních skupin, a to na organizační a technická opatření. Specifikace jednotlivých opatření jsou dále rozvedeny prováděcím předpisem – VKB.

2.1 Organizační opatření

Organizačními opatřeními se zabývá VKB, část druhá, hlava I. Jednotlivá opatření jsou zde uváděna v pořadí dle jednotlivých paragrafů VKB (5).

- Systém řízení bezpečnosti informací – zavedení systému řízení bezpečnosti informací (SŘBI) lze chápat jako všeobecné bezpečnostní opatření, odkazující tím pádem i na jiná opatření (např. řízení rizik, stanovení a udržování bezpečnostních politik). Pro KII je nezbytné též zajistit audit kybernetické bezpečnosti s roční periodou, monitoring a vyhodnocování účinnosti bezpečnostních opatření a politik stejně jako stanovení rozsahu SŘBI a řízení provozu a zdrojů.

- Řízení rizik – v rámci tohoto opatření je nutné zavést metodiku pro identifikaci a hodnocení aktiv a rizik včetně požadavků na hodnocení důležitosti aktiv a zároveň zvažování hrozeb a zranitelností při hodnocení rizik. Výčet bodů pro hodnocení rizik a doporučené stupnice pro hodnocení jsou uvedeny v přílohách č. 1 a 2 VKB. Pro KII je nezbytné hodnotit všechna aktiva a s nimi související rizika (hrozby a zranitelnosti). Výstupem je poté několik provázaných dokumentů, z nichž dokumentem výchozím je zpráva o hodnocení aktiv a rizik. Na ni je dále navázáno prohlášení o aplikovatelnosti a plán zvládání rizik. Minimální požadavky na obsah těchto dokumentů jsou uvedeny ve VKB s tím, že je možné naplňovat toto opatření i jiným způsobem, než je přímo uvedeno ve VKB, ale pouze za předpokladu zajištění stejné či vyšší bezpečnosti. Nejdůležitější je ale toto opatření vnímat jako kontinuální neukončený proces.
- Bezpečnostní politika – toto opatření implikuje stanovení bezpečnostních politik taxativně pokrývajících oblasti uvedené ve VKB. Důležitá zde je především relevantnost a úplnost politik pro daného správce a prvek KII.
- Organizační bezpečnost – toto opatření předpokládá zavedení výboru pro řízení kybernetické bezpečnosti a zřízení jednotlivých bezpečnostních rolí včetně vymezení jejich práv a povinností. Pro KII se jedná o bezpečnostní role manažer, architekt, auditor kybernetické bezpečnosti a garant aktiva. Jednotlivé bezpečnostní role musí prokázat svou odbornost a doložit příslušnou praxi dle VKB.
- Stanovení bezpečnostních požadavků na dodavatele – s dodavateli je třeba zajistit řízení bezpečnosti informací neboli seznámit dodavatele s relevantními bezpečnostními požadavky (včetně stanovených bezpečnostních politik) a toto zanést do příslušných smluv jako ustanovení o bezpečnosti informací. Problematické se v případě manažera železniční infrastruktury toto jeví pro dlouhodobé smlouvy a pro dodavatele soutěžené ve výběrovém řízení. Správce KII musí navíc pravidelně hodnotit rizika spojená s dodávkou a smluvně stanovit úroveň poskytovaných služeb (SLA).
- Řízení aktiv – v tomto opatření je dále rozvíjena problematika identifikace a hodnocení aktiv zmíněná již v požadavcích na řízení rizik. Manažer železniční infrastruktury jako správce a provozovatel KII je povinen aktiva identifikovat, určit garanty odpovědné za jejich správu a rozvoj a provádět hodnocení aktiv z hlediska jejich důvěrnosti, dostupnosti a integrity. To je povinen vykonávat i pro podpůrná aktiva s určením jejich vazby na aktiva primární.
- Bezpečnost lidských zdrojů – v kontextu celé organizace je nezbytné zpracovat plán rozvoje bezpečnostního povědomí, který má zahrnovat formu, rozsah a obsah školení napříč všemi rolemi, včetně role uživatelské. Kromě zpracování plánu musí být tento též prokazatelně vykonáván a monitorován stejně jako příslušné bezpečnostní politiky.
- Řízení provozu a komunikací – pro systémy KII je nezbytné zajistit jejich integritu, stabilitu a bezpečnost provozu. V prvé řadě je nutné stanovit provozní pravidla a postupy, poté monitorovat provoz a detekovat kybernetické bezpečnostní události, výstupy pravidelně hodnotit a pravidelně vytvářet zálohy včetně prověření jejich funkčnosti. Správce KII musí též stanovit práva a povinnosti jednotlivých rolí, postupy pro spuštění

restartu a ukončení chodu systémů po selhání, vytvořit komunikační matice pro nestandardní stavy a striktně oddělit vývojové, testovací a produkční prostředí.

- Řízení přístupu a bezpečné chování uživatelů – je nezbytné stanovit základní principy řízení přístupů a přidělování přístupových oprávnění (jednoznačný identifikátor pro každého uživatele), včetně jasných pravidel pro přidělování privilegovaných účtů. Jsou řešeny i přístupy a bezpečné používání mobilních zařízení.
- Akvizice, vývoj a údržba – je nutné zavést bezpečnostní opatření související se změnami zabezpečovaných systémů (zanesení do změnových projektů).
- Zvládání kybernetických bezpečnostních událostí a incidentů – je nezbytné zajistit detekci, oznamování, vedení evidence, vyhodnocování a následnou analýzu kybernetických bezpečnostních událostí a incidentů s cílem zdokonalení implementovaných opatření či nasazení opatření nových.
- Řízení kontinuity činností – na základě stanovení minimální úrovně poskytovaných služeb pro provoz, užívání a řízení dotčených systémů mají být připraveny plány zabezpečující obnovení této úrovně služeb včetně stanovení doby na obnovu chodu. Také je nutné definovat práva, povinnosti a odpovědnost zainteresovaných osob.
- Kontrola a audit – jedná se o posouzení souladu zavedených bezpečnostních opatření s právními, vnitřními a jinými relevantními předpisy, případně jinými smluvními závazky. Výstupy z pravidelné kontroly dodržování stanovených bezpečnostních politik jsou brány v potaz při aktualizaci plánu rozvoje bezpečnostního povědomí a analýzy rizik. Zároveň je za tímto účelem požadováno i provádění testů zranitelností technických prostředků (5).

2.2 Technická opatření

Technickými opatřeními se zabývá VKB, část druhá, hlava II. Jednotlivá opatření jsou zde uváděna v pořadí dle jednotlivých paragrafů VKB (6).

- Fyzická bezpečnost – v rámci tohoto opatření je nezbytné přijmout pravidla a postupy vedoucí k zamezení neoprávněného vstupu do vymezených prostor, v nichž jsou umístěna nebo zpracovávána aktiva. Dále je také nezbytné definovat pravidla zamezující neoprávněným zásahům, poškození či krádeži těchto aktiv.
- Nástroj pro ochranu integrity komunikačních sítí – jedná se o zajištění řízení bezpečného přístupu do sítě a její segmentaci včetně zřízení demilitarizované zóny. U vzdálených přístupů musí být komunikace šifrována kryptografickými prostředky. V neposlední řadě je též požadováno odstranění přenášených dat v nevalidním formátu.
- Nástroj pro ověřování identity uživatelů – toto nařízení přikazuje správci KII používat nástroj pro ověření identity uživatelů a administrátorů s požadavky na komplexnost a délku hesla. Je také zamezeno používat dříve používaná hesla a měnit heslo častěji než jedenkrát za 24 hodin. Po určité době nečinnosti je vyžadováno opětovné ověření identity uživatele. Přístupy je také možné realizovat i jinak než heslem, ale pouze se stejnou nebo vyšší úrovní zabezpečení.
- Nástroj pro řízení přístupových oprávnění – je nezbytné řídit oprávnění na úrovni jednotlivých aplikací, dat (zápis, čtení) a změn přístupových oprávnění. Manažer

železniční infrastruktury jako správce KII je povinen zaznamenávat použití příslušných přístupových oprávnění.

- Nástroj pro ochranu před škodlivým kódem – cílem tohoto opatření je zajištění ochrany komunikace mezi vnitřní a vnější sítí, ochrana serverů, sdílených datových úložišť a pracovních stanic. Daný nástroj je nutné pravidelně aktualizovat a kontrolovat jeho výstupy.
- Nástroj pro zaznamenávání činnosti KII, jejích uživatelů a administrátorů – u systému jsou zaznamenávány provozní, konfigurační a bezpečnostní činnosti. U uživatelů a administrátorů poté jejich přihlášení a odhlášení, u administrátorů všechny činnosti (změny nastavení oprávnění, snaha o činnosti nad rámec přidělených oprávnění atd.). Tímto nástrojem získaná data, obsahující minimálně identifikaci uživatele a jeho stroje, činnost a její výsledek, je nezbytné chránit proti smazání či přepsání. Technické aktivum zaznamenávající tuto činnost musí být též jednoznačně identifikováno, a to s uvedením přesného data a času (synchronizace jednotného systémového času). Manažer železniční infrastruktury musí záznamy získané tímto nástrojem uchovat minimálně 3 měsíce.
- Nástroj pro detekci kybernetických bezpečnostních událostí – tento nástroj slouží k ověření, kontrole a případnému zablokování komunikace (primárně mezi vnitřní a vnější sítí, nicméně pro KII i v rámci vnitřní sítě).
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí – tento nástroj zajišťuje integrovaný sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí, poskytuje sadu reportů pro jednotlivé bezpečnostní role a je schopný včasného varování. Pravidla pro automatické varování je ale nutné neustále aktualizovat a zdokonalovat.
- Aplikační bezpečnost – manažer železniční infrastruktury je povinen před uvedením aplikací dostupných z vnější sítě do provozu či v případě jejich zásadních změn provést bezpečnostní testování stejně jako zajistit jejich trvalou ochranu (před neoprávněnou změnou, popřením informací či kompromitací). Je nezbytné stejně chránit též příslušné transakce (nedokončení, špatné směrování, neautorizované opakování apod.).
- Kryptografické prostředky – je třeba nasadit dostatečné kryptografické prostředky zajišťující ochranu důvěrnosti a integrity předávaných či ukládaných dat s jednoznačnou identifikací jejich původce. Manažer železniční infrastruktury musí stanovit a provozovat systém správy klíčů včetně jeho náležitostí (generování, distribuce, archivace, ničení atd.). VKB definuje seznam odolných kryptografických algoritmů, ale bohužel pouze k datu poslední novelizace VKB.
- Nástroj pro zajišťování úrovně dostupnosti – tento nástroj musí splňovat potřeby řízení kontinuity činností, zajistit odolnost vůči kybernetickým útokům cílícím na snížení jeho dostupnosti a zajistit záložní řešení (redundantní infrastruktura či smluvní zajištění v definovaném časovém intervalu).
- Bezpečnost průmyslových a řídicích systémů – z hlediska manažera železniční infrastruktury se jedná především o informační systémy podílející se svou činností na řízení železničního provozu. Toto opatření je již částečně součástí předcházejících

opatření, nicméně je zde nezbytné omezit fyzický přístup k síti a zařízením a mít vypracovány plány pro obnovení chodu těchto systémů (6).

2.3 Nejčastější nedostatky

V této kapitole jsou uvedeny nejčastější nedostatky implementace problematiky kybernetické bezpečnosti identifikované auditory kybernetické bezpečnosti napříč různými organizacemi (7).

- Nedostatečná podpora oblasti kybernetické bezpečnosti ze strany vedení organizace – velmi často nemá manažer kybernetické bezpečnosti dostatečné kompetence a pravomoci pro výkon jeho role, tudíž není schopen prosadit příslušná bezpečnostní opatření. V oblasti kybernetické bezpečnosti také mohou chybět zdroje (lidské, finanční, technologické).
- Nevhodné zařazení v organizační struktuře – manažeři a auditoři kybernetické bezpečnosti nesmí být z důvodu zajištění nezávislosti a nestrannosti zařazeni v sekcích, jejichž činnost upravují či auditují.
- Nedostatek specialistů – může vést k nevhodnému slučování bezpečnostních rolí, kdy např. jeden zaměstnanec vykonává roli manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a bezpečnostního analytika.
- Nedostatky v bezpečnostní dokumentaci – v některých organizacích se objevují neschválené, tím pádem neplatné bezpečnostní politiky. Dalším problémem je neaktuálnost dokumentace a chybějící metodiky (např. chybějící metodika k analýze rizik – nelze opakovat jednotný postup).
- Rozvoj bezpečnostního povědomí v oblasti kybernetické bezpečnosti – v případě nedostatečného či zcela chybějícího pravidelného zvyšování bezpečnostního povědomí zaměstnanců je velmi pravděpodobné, že zaměstnanci budou jako nejslabší bezpečnostní článek využiti ke kompromitaci firmy.
- Řízení dodavatelů – s dodavateli systémů nejsou často smluvně ošetřeny bezpečnostní požadavky (zákaznický audit, exit strategie, hlášení kybernetických bezpečnostních incidentů apod.).
- Řízení aktiv a rizik – klasifikace aktiv bývá často nedostatečná či neúplná či úplně chybí. Plány zvládání rizik je možné označit v mnoha případech za nevyhovující z důvodu chybějící návaznosti bezpečnostních opatření na rizika, z důvodů chybějících termínů realizace bezpečnostních opatření apod.

ZÁVĚR

Manažer železniční infrastruktury je dle ZKB jednoznačně správcem KII s tím, že některé jeho systémy spadají do kategorie průmyslových a řídicích systémů. Je tedy povinen systémy zabezpečit v rámci kybernetické bezpečnosti tak, jak je popsáno v ZKB a VKB.

Při implementaci bezpečnostních opatření je ale nezbytné uvažovat racionálně a implementovat jen opatření relevantní k zabezpečovaným systémům. Zároveň by přijímaná bezpečnostní opatření měla vždy vycházet z výsledků analýzy rizik tak, aby vynaložené náklady byly přiměřené přínosu zabezpečení určených systémů KII. V případě

nedostačujících zdrojů je poté vhodné postupovat dle kritičnosti a priorit a ihned nerealizovaná opatření zahrnout do plánu zvládání rizik.

POUŽITÁ LITERATURA

(1) *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění* [online]. c2017 [cit. 2017-12-27]. Dostupné z <http://www. portal.gov.cz/app/zakony/>.
(2) *Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti* [online]. c2017 [cit. 2017-12-27]. Dostupné z <http://www. portal.gov.cz/app/zakony/>.
(3) *Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury* [online]. c2017 [cit. 2017-12-27]. Dostupné z <http://www. portal.gov.cz/app/zakony/>.
(4) KUČÍNSKÝ, A. Zákon o kybernetické bezpečnosti a směrnice NIS. *Interní auditor*, 2016, roč. 20, č. 3, s. 2-4, ISSN 1213-8274.
(5) KINTR, L. Bezpečnostní opatření podle zákona o kybernetické bezpečnosti – 1. část – organizační opatření. *Interní auditor,* 2016, roč. 20, č. 4, s. 5-8, ISSN 1213-8274.
(6) KINTR, L. Bezpečnostní opatření podle zákona o kybernetické bezpečnosti – 2. část – technická opatření. *Interní auditor*, 2017, roč. 21, č. 2, s. 30-34, ISSN 1213-8274.
(7) RYBÁKOVÁ, A. Audit a auditor kybernetické bezpečnosti. *Interní auditor*, 2017, roč. 21, č. 4, s. 12-16, ISSN 1213-8274.