Metodika zabezpečení ICT infastruktury malých mezinárodních letišť v ČR

Doc. Ing. Vladimír Němec, Ph.D.

Prof. Ing. Róbert Lórencz, CSc.

Ing. Jiří Buček

Ing. Tomáš Zahradnický, Ph.D.

Tato publikace byla vytvořena v rámci řešení projektu MV ČR č. VG20132015130 - Využití nástrojů krizového řízení, rizikového inženýrství, systémového inženýrství a moderních technologií ke zvýšení ochrany před protiprávními činy na mezinárodních letištích v České republice (2013-2015, MV0/VG)

ČVUT v Praze, Fakulta dopravní

2015

1 Obsah

2 Úvod

Kybernetický prostor (kyberprostor) dnes představuje nedílnou součást lidské informační společnosti, která je dnes na informačních technologiích a jejich korektní funkci zcela závislá. Kyberprostor je neteritoriálním územím představujícím zdroj bezpečnostních hrozeb, jejichž materializace v podobě bezpečnostních incidentů mohou mít v až vážné ekonomické dopady s celostátní a výjimečně i globální působností. Lisabonský summit Organizace severoatlantické smlouvy (NATO) v roce 2010 určuje zajišťování kybernetické bezpečnosti jako jednu z klíčových výzev současné doby [1]. Kybernetické útoky jsou uvedeny jako jedna z šesti z bezpečnostních hrozeb v Bezpečnostní strategii České republiky z roku 2011 [2]. Bezpečností kyberprostoru se zabývá samostatná Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015 [3]. Od roku 2011 začíná budování české legislativy v oblasti kybernetické bezpečnosti.

Geneze legislativy kybernetické bezpečnosti v České republice počíná v roce 2011 usnesením vlády č. 781/2011 [4], ve kterém je stanoven gestorem problematiky kybernetické bezpečnosti a současně i národní autoritou pro tuto oblast Národní bezpečnostní úřad (NBÚ), je zřízena Rada pro kybernetickou bezpečnost. V roce 2012 připravuje NBÚ Strategii pro oblast kybernetické bezpečnosti na období 2012 - 2015 [3,6], která je schválena usnesením vlády č. 364/2012, a dále věcný záměr Zákona o kybernetické bezpečnosti (ZKB) [5], který je schválen usnesením vlády č. 382/2012. V roce 2013 se ZKB dostává do meziresortního připomínkového řízení a v témže roce je předložen vládě návrh ZKB, který je počátkem roku 2014 schválen. V polovině roku 2014 je zákon schválen Poslaneckou sněmovnou Parlamentu České republiky a o měsíc později i v Senátu Parlamentu České republiky. V srpnu roku 2014 zákon podepisuje prezident republiky Miloš Zeman. V témže měsíci vychází ZKB ve sbírce zákonů pod číslem 181/2014 a nabývá účinnosti dne 01.01.2015. Vedle ZKB vychází v roce 2014 nařízení vlády č. 315/2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, dále vyhláška č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Poslední vyhláškou je vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

2.1 Zákon o kybernetické bezpečnosti

Primárním cílem ZKB je zvýšit bezpečnost kyberprostoru, nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou při řešení kybernetických bezpečnostních incidentů a zavést do praxe soubor oprávnění a povinností [5]. Po vymezení předmětu úpravy a pojmů (§ 1-2), kterými je kybernetický prostor, kritická informační infrastruktura (KI, určující kritéria určena nařízením vlády č. 315/2014 jako příloha k nařízení vlády č. 432/2010 Sb.), bezpečnost informací, významný informační systém (VIS, určující kritéria definována vyhláškou č. 317/2014), správce informačního a komunikačního systému a významná síť, definuje zákon povinné subjekty (§ 3). Následuje výčet bezpečnostních, organizačních a technických opatření (§ 4-5) a informace o odkazu na zvláštní právní předpis stanovující obsah bezpečnostních, obsah a strukturu bezpečnostní dokumentace a rozsah bezpečnostních opatření pro orgány správce kritických informačních a komunikačních systémů a správce významných informačních systémů (§ 6). Následují definice pojmů kybernetická bezpečnostní událost a kybernetický bezpečnostní incident (§ 7) a způsoby jejich hlášení provozovateli národního CERT pracoviště anebo NBÚ (§ 8), opět s odkazem na prováděcí předpis (vyhláška č. 316/2014). Dále ZKB uvádí, že NBÚ vede evidenci kybernetických bezpečnostních incidentů (§ 9), mlčenlivosti (§ 10), vydávání opatření (§ 11) a varování (§ 12-15). Dále ZKB definuje pojem kontaktních údajů a způsob oznamování jejich změny (§ 16). Následuje zavedení Národního CERT pracoviště (§ 17), definice podmínek jeho provozovatele (§ 18) a náležitosti veřejnoprávní smlouvy (§ 19), která je s provozovatelem Národního CERT uzavírána. Následuje zavedení Vládního CERT (§ 20), kterým je NBÚ. Zákon dále uvádí definici kybernetického ne-

bezpečí (§ 21), výkon státní správy (§ 22), kontrolu, nápravná opatření a správními delikty (§ 23-27). V závěru zákon zmocňuje Ministerstvo vnitra České republiky (MVČR) ke stanovení významných informačních systémů a jejich určujících kritérií ve zvláštní vyhlášce (vyhláška č. 317/2014 Sb.) a NBÚ ke stanovení obsahu a struktury bezpečnostní dokumentace (příloha č. 4 k vyhlášce č. 316/2014 Sb.), typů a kategorií kybernetických bezpečnostních incidentů a způsobu jejich hlášení (příloha č. 5 k vyhlášce č. 316/2014 Sb.), náležitosti oznámení o provedení reaktivního opatření (příloha č. 6 k vyhlášce č. 316/2014 Sb.) a oznámení kontaktních údajů (§ 28) (příloha č. 7 k vyhlášce č. 316/2014). Následují přechodná opatření, ve kterých vybrané orgány a osoby do 30 dnů od dne účinnosti ZKB oznámí své kontaktní údaje a do 1 roku začnou vykonávat zákonem určenou činnost, případně zavedou bezpečnostní opatření podle ZKB (§ 29-31). Další část upravuje výkon národního CERT do doby uzavření veřejnoprávní smlouvy (§ 32) a společná ustanovení (§ 33) omezující působnost zákona na vybrané informační a komunikační systémy. V části druhé zákon mění zákon o ochraně utajovaných skutečností a o bezpečnostní způsobilosti 412/2005 Sb. (§ 34), v části třetí ZKB mění zákon o elektronických komunikacích č. 127/2005 Sb. (§ 35), v části čtvrté mění zákon o svobodném přístupu k informacím č. 106/1999 Sb. (§ 36), v části páté zákon o provozování rozhlasového a televizního vysílání č. 231/2001 Sb. (§ 37) a v šesté části zavádí účinnosti ZKB od 01.01.2015 (§ 38).

2.2 Zákon o kybernetické bezpečnosti a letiště v České republice

Nařízení vlády č. 315/2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, nastavuje přílohu k nařízení vlády č. 432/2010 Sb., která určuje odvětvová kritéria pro určení prvku kritické infrastruktury. V části V., Doprava, oddíl C, Letecká doprava, uvádí kritéria pro letiště v odst. 1, a dále pro řízení letového provozu v odst. 2. takto:

V. DOPRAVA

...

C. Letecká doprava

C. 1 Letiště

Veřejné mezinárodní letiště způsobilé přijetí letu podle přístrojů, u kterého není možné leteckou obchodní dopravu zajistit alternativním letištěm nebo alternativní zajištění je příliš nákladné, nehospodárné nebo velmi těžko proveditelné.

Alternativním letištěm se rozumí veřejné mezinárodní letiště, které je schopno zajistit nejméně 80 % letecké obchodní dopravy letiště, pro které je určeno jako alternativní, je v čase 2 hodin dosažitelné jiným druhem dopravy, má dostatečnou kapacitu pohybových ploch a kapacitu terminálu, má stejnou nebo podobnou kategorii jako letiště, pro které je určeno jako alternativní, a je způsobilé přijmout let vykonaný podle přístrojů.

C. 2 Řízení letového provozu (ŘLP)

přibližovací služba řízení a letištní služba řízení letiště určeného jako kritická infrastruktura, nebo oblastní služba řízení poskytující letové provozní služby včetně řízení letového provozu ve vzdušném prostoru České republiky.

D. Vnitrozemská vodní doprava

...

[7]

Pražské letiště Václava Havla (kód ICAO LKPR) je největším veřejným mezinárodním letištěm způsobilým pro přijetí letu podle přístrojů v České republice. Proto toto letiště dosud neexistuje v České republice alternativní letiště, které by splňovalo podmínky alternativního letiště část C, odst. 1 bod a. přílohy k nařízení vlády č. 432/2010 Sb. Nebudeme-li se omezovat u alternativních letišť na letiště pouze v České republice a budeme-li uvažovat jako možná alternativní letiště také vybraná letiště ve státech bezprostředně sousedících s Českou republikou, dostáváme se do sporu s částí C, odst. 1 bod b. přílohy k nařízení vlády č. 432/2010 Sb., protože tato letiště nejsou dosažitelná jiným druhem dopravy v čase do 2 hodin. Letiště Václava Havla tedy nemá alternativní letiště, splňuje odvětvová kritéria pro určení prvku kritické infrastruktury, je její součástí, a je povinným subjektem podle ZKB. Ostatní mezinárodní letiště v České republice schopná přijmutí letu podle přístrojů, která pro účely této metodiky budeme nazývat *malými letišti*, nejsou prvky kritické infrastruktury, protože jejich obchodní dopravu lze zajistit alternativními letišti — z pražského letiště Václava Havla je v čase do 2 hodin dosažitelné kterékoliv letiště od západního cípu České republiky až po letiště Brno-Tuřany (kód ICAO LKTB) včetně, ze kterého je opět v čase do 2 hodin dosažitelné kterékoliv malé letiště na východním cípu České republiky. ZKB ani k němu přidružená nařízení vlády č. 315/2014 Sb., příloha k vyhlášce č. 432/2010 Sb. a vyhlášky č. 316/2014 a č. 317/2014 Sb. se na malá letiště ani na jimi spravované informační a komunikační infrastrukturu a informační a komunikační systémy nevztahují.

Definice. Jako *malé letiště* budeme uvažovat takové veřejné mezinárodní letiště, které není součástí kritické infrastruktury, a které je způsobilé přijmout let vykonaný podle přístrojů.

3 Cíl metodiky

Přestože malá letiště nejsou prvky KI, s prvky KI mají interakce, které mohou být zdrojem hrozeb. Tyto interakce mohou být jednosměrné směrem od KI k letišti, od letiště ke KI, anebo mohou probíhat obousměrně a mohou být hmotné prostřednictvím fyzických objektů, anebo nehmotné, ve formě komunikace po komunikačním kanálu (metalické vedení, elektromagnetické spektrum, přenos dokumentů po flash discích, ...). Interakce mohou být zdrojem přímého anebo indukovaného ohrožení jak letiště, ze kterého interakce vychází (zdrojové letiště), tak i letiště, na které přichází (cílové letiště), kterým mohou být i letiště tvořící součást KI, a mohou tak tvořit vstupní bránu pro ohrožení letišť v KI. Tato metodika si vytyčuje za cíl se interakcí malých letišť s prvky KI zabývat a poukázat na potenciálně zranitelná místa.

Aby bylo možné určit potenciální vstupní brány pro útok, je nutno postupovat buď i) směrem od možných interakčních kanálů k informačním a komunikačním systémům letištní infrastruktury (metoda shora dolů, angl. top-down), anebo ii) postupovat směrem od systémů letištní infrastruktury vzhůru ke komunikačním kanálům a pro ně dále hledat hrozby pomocí některé ze standardních metodik (metoda zdola nahoru, angl. bottom-up). Pro účely této metodiky budou třídy a kanály interakce definovány podle standardní metodiky pro bezpečnostní testování OSSTMM verze 3 [8], která dělí možné interakce do tří tříd, které pak dělí na jednotlivé komunikační kanály. Dělení interakcí na třídy a kanály je zobrazeno v Tab. 1.

Třída	Kanál	Popis
Fyzická bezpečnost (PHYSSEC)	Lidský	Zahrnuje lidský element komunikace, přičemž interakce jsou buď fyzické anebo psychologické.
	Fyzikální	Fyzikální testování bezpečnosti, kde kanál je fyzikální neelektrické podstaty. Zahrnuje hmatatelný element bezpečnosti, kde interakce vyžaduje použití fyzické síly anebo přenosu energie k manipulaci.
Spektrální bezpečnost (SPECSEC)	Bezdrátový	Zahrnuje veškeré elektronické komunikace, signály a emanace, které se odehrávají ve známém elektromagnetickém spektru. Toto zahrnuje elektronické komunikace (ELSEC), signály (SIGSEC) a emanace zařízení nepropojených kabelem (EMSEC).
Komunikační bezpečnost (COMSEC)	Telekomunikační[1]	Zahrnuje telekomunikační sítě, digitální i analogové, kde interakce probíhají pomocí zavedených telefonních anebo telefonním podobných síťových linkách.
	Datový	Zahrnuje všechny elektronické systémy a datové sítě, kde interakce probíhá po zavedených kabelových a drátových síťových linkách.

Tabulka 1. Interakční třídy a kanály podle metodiky OSSTMM [8].

Prvky letištní informační a komunikační infrastruktury vzájemně interagují. Tyto interakce probíhají vždy po jednom z výše uvedených kanálů. Vzhledem k tomu, že interakce mohou být předmětem ohrožení, je nutné se zabý-

[1] V rámci této metodiky nebudeme uvažovat telekomunikační kanál separátně, ale jako případnou podmnožinu kanálu datového.

vat všemi potenciálními možnostmi, jak by k takovému ohrožení mohlo dojít a určit zdroje hrozeb. K hledání zdrojů hrozeb je vhodná metodika STRIDE.

3.1 Metodika STRIDE

K odhalení možných hrozeb po jednotlivých kanálech bude uvažováno klasifikační schéma STRIDE [9], které klasifikuje možné hrozby do 6 různých tříd:

- podvržení identity (angl. Spoofing),
- manipulace s daty (angl. Tampering),
- popíratelnost (angl. Repudiation),
- únik informací (angl. Information Disclosure),
- odepření služby (angl. Denial-of-Service) a
- zvýšení oprávnění (angl. Elevation of Privilege).

Na kanál je třeba pohlížet jako na objekt, který může být předmětem útoku patřícího do každé z šesti tříd metodiky STRIDE. Je tedy nutné se ptát, jakým způsobem by mohlo dojít k podvržení identity (S) interagujících stran během interakce těch kterých informačních a komunikačních prvků. Dále je-li možné provést během interakce její ovlivnění prostřednictvím manipulace s daty anebo objekty, které jsou předmětem interakce (T). Je také nutné se ptát, může-li jedna, druhá, či obě strany popřít, že danou interakci začaly provádět (R), může-li dojít, případně za jakých okolností, k nevyžádanému úniku dat (I). Nakonec je nezbytné se ptát, za jakých okolností může dojít k odepření dané interakce jednou či druhou stranou (D) a není-li možné získat neoprávněnou úroveň přístupu (E).

3.2 Klasifikace ohrožení z hlediska lokality kybernetického ohrožení

Ohrožení kybernetické bezpečnosti lze klasifikovat podle rozsahu možného dopadu vzhledem k prvkům kritické infrastruktury. Může nastat jeden ze tří případů. Bezpečnostní incident vyvolaný uvažovaným ohrožením může mít dopad, jehož rozsah je lokální, tj. zasáhne jen IS letiště, kde incident vznikl. Takové ohrožení označíme jako **lokální**. Vzhledem k tomu, že malé mezinárodní letiště není prvkem kritické infrastruktury, lokální ohrožení nemá žádný dopad na informační systémy patřící do kritické infrastruktury.

Druhý typ ohrožení je takzvané **indukované**, nepřímé ohrožení. Jeho uvažovaný dopad může zasáhnout informační systém patřící do kritické infrastruktury nepřímo, jako následek narušení bezpečnosti lokálního letiště. Jako indukované považujeme ohrožení, které pochází z narušení lokálního IS a má dopad na informační systém patřící do KI. KI na toto narušení reaguje, avšak neexistuje komunikační kanál, kterým by mohl reagovat zpět směrem k útočníkovi. Takovéto narušení bývá často zapříčiněno útoky typu manipulace s daty, při kterých z lokálního IS odejdou směrem do KI pozměněná data. KI na tuto situaci reaguje buď tak, že data nepřijme např. díky chybě v nich, anebo je přijme jako platná, se všemi důsledky, které z takových pozměněných dat vyplývají.

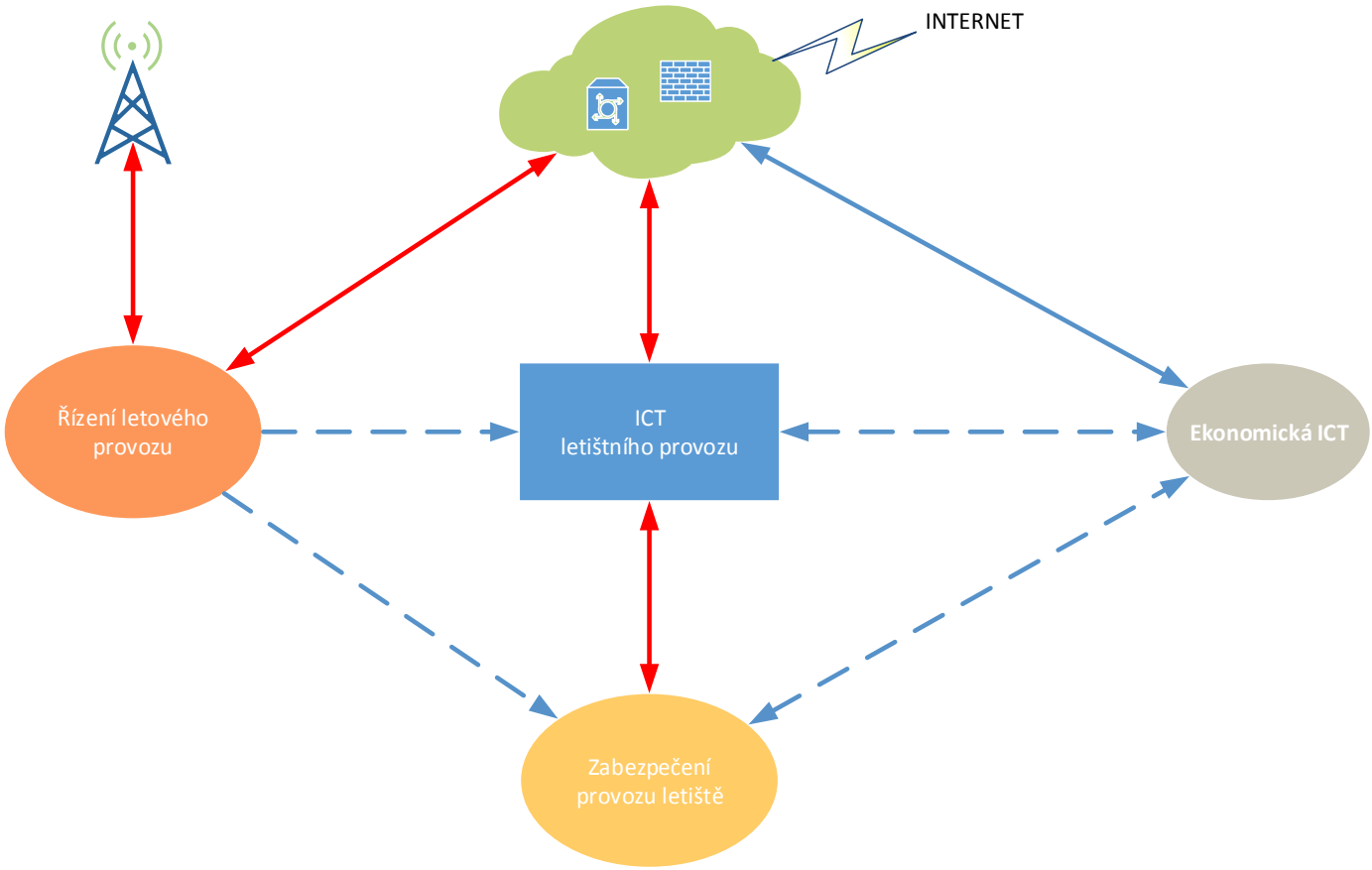
Třetí typ ohrožení kybernetické bezpečnosti je ohrožení **s přímým dopadem na KI** - lokální ICT infrastruktura je přímým prostředníkem incidentu IS KI. Jako přímé považujeme narušení, které pochází z lokálního IS, a tento využívá jako prostředek k narušení informačního systému KI, kde vyvolá incident informační bezpečnosti s příslušným dopadem v rámci KI. Nutným předpokladem je existence přímého datového komunikačního kanálu, který se dostane pod kontrolu útočníka.

4 Komponenty ICT infrastruktury malých mezinárodních letišť v ČR

Malá mezinárodní letiště nepatří podle definice uvedené v zákoně o Kybernetické bezpečnosti […] do tzv. Kritické Infrastruktury (KI). Tato kapitola se zabývá rozborem a prozkoumáním ICT infrastruktury a jejích základních součástí malých mezinárodních letišť v ČR a to z hlediska jejich bezpečnosti a odolnosti vůči kyber-útokům. Výsledkem této analýzy bude určení potenciálních bezpečnostních rizik ICT infrastruktury a to jednak z hlediska jak lokálního ohrožení, tak zejména z hlediska průniků útoků vedených z ICT struktury malých letišť do vnějších ICT systémů, které můžou již patřit do kritické infrastruktury. V takových případech útoků do kritické infrastruktury vedených prostřednictvím ICT infrastruktury malých letišť je velmi důležité v co největší míře určit kritické aplikace a metodiky, které toto umožňují.

Podrobnější popis propojení a funkčnosti informačních systémů letiště je uveden ve výzkumné zprávě *VG20132015130 - Analýza propojení a funkčnosti informačních systémů letiště (viz příloha 1)*.

Základní architektura informační infrastruktury malých mezinárodních letišť je zobrazena na Obrázku 1. Tvoří ji základní bloky: ICT letového provozu, Řízení letového provozu, Zabezpečení provozu letišť Ekonomická ICT infrastruktura a Komunikace. Jednotlivé bloky jsou propojený prostřednictvím datových a kontrolních toků, tak jak je to znázorněné na obrázku. Červenou barvou jsou znázorněné řídící toky a modrou datové. Z hlediska analýzy bezpečnostních rizik je tento způsob zobrazení důležitý. Komunikace s vnějším prostředím je zabezpečeno dvěma způsoby. Je to jednak prostřednictvím komunikačního kanálu Řízení letového provozu a jednak prostřednictvím Internetu připojeného k jednotce Centrální komunikace.



Obrázek 1. Architektura informační infrastruktury malých mezinárodních letišť.

4.1 Řízení letového provozu

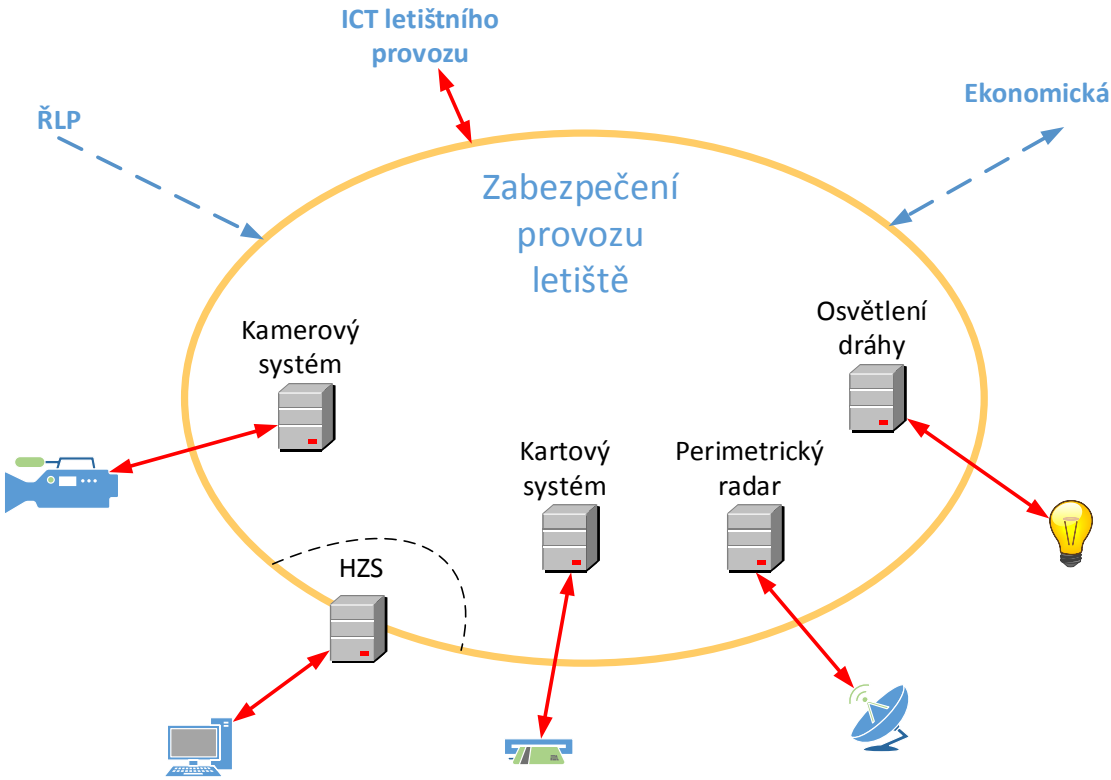
Řízení letového provozu je samostatnou a nezávislou části informační infrastruktury. Je napojena na letištní systémy za účelem výměny specifických informací. Z letiště do ŘLP se předávají informace o pohybu vozidel po vyhrazené letištní ploše, naopak letiště dostává informace o přesných polohách letadel. Z hlediska kybernetické bezpečnosti jde o oddělený systém, jehož interakce se systémy letiště je omezena. Ochrana před kybernetickými útoky spočívá ve filtrování dat tak, aby byly propuštěny jen specifické stavové informace.

4.2 Ekonomická ICT infrastruktura

Ekonomická část ICT infrastruktury je ICT infrastruktura podporující ekonomické aspekty provozních procesů letiště včetně lidských zdrojů. Není přímo napojena na provoz letiště a neměla by při dodržování obecných bezpečnostních doporučení představovat bránu pro kybernetické útoky.

4.3 Zabezpečení provozu letiště

Zabezpečení provozu letiště komunikuje s ICT letového provozu, Ekonomickou ICT a ŘLP. Do Zabezpečení provozu letiště patří tyto systémy: Perimetrický radar, HZS (pokud není od letiště zcela oddělen) a Kartový systém.



Obrázek 2. Komponenty ICT infrastruktury provozu letišť.

4.4 ICT letištního provozu

ICT infrastruktura letištního provozu zahrnuje tyto komponenty: Deprature Control System (DCS), Flight Information Display System (FIDS-E-VIDS), Common User Airport System (CUS) a Airport Operational Database (AODB).

Obrázek 3. Komponenty ICT infrastruktury letištního provozu.

4.4.1 Systém DCS

je systém určený pro odbavování a zahrnuje tyto moduly:

- Weight and Balance (W&B) system – systém na vyvážení letadla
- Check-In/Boarding System – kontrolní systém pro odbavování cestujících, využívaný data z letových plánů a aktuálních rezervací
- Baggage Handling System (BHS) – kontrolní systém logistiky zavazadel
- Baggage Reconciliation System (BRS) – systém rekonciliace zavazadel
- Flight Plan Management System (FPMS) – systém letových plánů, je zdrojem dat pro další systémy DCS a může být připojen k FIDS

4.4.2 Systém CUS

se skládá z:

- Common Use Terminal Equipment (CUTE)
- Common Use Self Service using Kiosks (CUSS)

Tyto systémy slouží pro propojení na databáze elektronických letenek s možností flexibilního odbavení různými způsoby. Je využíváno všemi leteckými společnostmi a handlingovými agenty. CUTE je využíváno různými uživa-

teli a propojuje různé počítačové terminály, displeje a tiskárny. CUSS je určeno pro společné využívání samoobslužných check-in přepážek různými dopravci.

4.4.3 FIDS - E-VIDS Flight Information Display System

FIDS je informační systém pro zobrazování informací o příletech a odletech, výdeji zavazadel a dalších informací pro cestující na informačních tabulích. Většina informací je přijímána od centrálních letištních systémů – AODB, FPMS a DCS. V případě synchronizace na jiné databáze může být FIDS bránou pro útok.

4.4.4 AODB Airport Operational Database

Databáze AODB obsahuje všechny informace nutné pro provoz letiště. AODB je centrální databází, na kterou jsou připojeny ostatní systémy (DCS, FIDS, CUS) a která je propojena mimo letiště přes systém předávání zpráv (SITA).

5 Analýza kybernetických hrozeb ICT infrastruktury malých mezinárodních letišť v ČR

V následující části textu rozebereme propojení jednotlivých komponent ICT infastruktury malých mezinárodních letišť s prvky kritické infrastruktury, a dále analyzujeme kybernetická ohrožení podle metodiky STRIDE s uvažováním informačních kanálů podle metodiky OSSTMM.

5.1 Analýza zabezpečení provozu letiště

V této části textu budeme rozebírat kybernetické ohrožení zabezpečení provozu letiště, do kterého patří Hasičský záchranný systém, kartový přístupový systém, perimetrický radar, osvětlení přistávací dráhy a kamerový systém.

Tabulka 2 obsahuje charakterizaci vzájemného propojení jednotlivých komponent zabezpečení provozu letiště s vnějšími systémy, a dále klasifikaci ohrožení ve vztahu ke kritické infrastruktuře. Ve sloupcích ohrožení jsou uvedeny jednotlivé typy možných ohrožení, s případným dopadem na kritickou infrastrukturu.

	Propojení na jiný systém (lokální/vnější)	**Přímé lokální ohrožení**	**Indukované ohrožení KI**	**Propojení na KI**	**Poznámka**
HZS	ICT letového provozu a ŘLP Internet	Falešný poplach, potlačení poplachu	Falešný poplach bez vlivu na KI	Přes IZS ČR	Připojení k IZS
Kartový systém	Ekonomická – personální ICT	Prolomení karty/kopírování, napadení řídicího systému – neautorizovaný vstup	Přes systémy v místnostech s autentizaci/autorizaci pomocí karet, ne přímé	Přes systémy v místnostech s autentizaci/autorizaci pomocí karet, ne přímé	Podceňována bezpečnost
Perimetrický radar	Bezpečnostní dispečink	Falešný poplach/maskování			
Osvětlení přistávací dráhy	ŘLP	Prostřednictví kyberútoku přes řídicí systém (AMS) vyřadí se z provozu			
Kamerový systém	Bezpečnostní dispečink	Maskování/vyřazení z provozu	Přes systémy v místnostech, které hlídá kamer. systém	Přes systémy v místnostech, které hlídá kamer. systém	

Tabulka 2. Typy komunikaci mezi jednotlivými komponenty zabezpečení provozu letiště s vnějšími systémy.

Tabulka 3 obsahuje klasifikaci ohrožení jednotlivých komponent zabezpečení provozu letiště podle metodiky STRIDE. Jednotlivé buňky obsahují charakterizaci příslušného ohrožení, a ve zkratce uvádějí, prostřednictvím kterých kanálů (podle OSSTMM, viz tab. 1).

Typ ohrožení Komponenta	Podvržení identity (S)	Manipulace s daty (T)	Popíratelnost (R)	Únik inf. (I)	Odepření služby (D)	Zvýšení oprávnění (E)
HZS	Ano přístup L, F, D	Ano Poplach, falešné vyhlášení nebo zamlčení L, B, T, D	Ne	Ano Únik strategických dat L, B, T, D	Ano Zahlcení komunikačních linek B, T, D	Ano Přístup L, D
Kartový systém	Ano přístup L, F, B, D	Ano Falšování informací o vstupu F, L, B, D	Ano Popření informaci o vstupu B, D	Ano Osobní data, monitorování pohybu osob L, B, D	Ano Zahlcení systému, znemožnění funkce přístupového systému F, B, D	Ano přístup L, B, D
Perimetr. radar	Ne	Ano Utajení narušení perimetru a falešné narušení perimetru L, B, D	Ne	Ano Monitoring pohybu, získaní charakteristiky radaru L, B, D	Ano Zablokovaní komunikace s centrálou. Narušení základní funkce. F, B, D	Ne
Osvětlení přistávací dráhy	Ne	Ano F, D	Ne	Ne	Ano Blokace řídícího zařízeni D	Ne
Kamerový systém	Ano L, B, D	Ano L, F, B, D	Ne	Ano L, B, D	Ano B, D	Ne

Tabulka 3. Třídy kybernetických ohrožení metodiky STRIDE pro jednotlivé komponenty Zabezpečení provozu letiště

5.1.1 Hasičský záchranný systém (HZS)

HZS může být součástí ICT infrastruktury provozu letišť. Pokud je HZS zcela oddělen, nemusí se na něj tato metodika vztahovat. V dalším textu se tato metodika zabývá situací, kdy ICT systému HZS je součástí ICT infrastruktury letiště. ICT infrastruktura provozu letišť zahrnuje kromě HZS také kartový přístupový systém, systém perimetrického radaru, systém osvětlení přistávací a vzletové dráhy, a kamerový systém. HZS je propojeno na ICT letového provozu, ŘLP, a také do Internetu. Narušení informačního systému HZS může mít za následek především přímé lokální ohrožení, např. formou falešného poplachu. Narušení IS může být formou podvržení identity, manipulace s daty, úniku informací, odepření služby a zvýšení oprávnění. Narušení může být pomocí kanálů vypsaných v tabulce 3**.** Podvržení identity umožní útočníkovi vstup do systému HZS např. s použitím přístupových údajů oprávněného zaměstnance přečtených z papírku na monitoru. Manipulace s daty může mít za následek vyhlášení falešného nebo naopak potlačení skutečného poplachu. Odepření služby může nastat formou zahlcení serveru pro zpracování údajů z čidel, případně zahlcení komunikačních linek směrem k ICT letiště nebo IZS. Zvýšení oprávnění může způsobit provedení akce (např. odvolání poplachu) neoprávněným uživatelem.

Vztah HZS ke kritické infrastruktuře je dán především napojením na celostátní integrovaný záchranný systém ČR, jinak nemá žádný přímý nebo zprostředkovaný vliv na KI.

Vzhledem k předchozí analýze plynou pro zabezpečení ICT HZS před kybernetickými útoky následující doporučení. Pro omezení hrozby podvržení identity je třeba důsledně chránit uživatelské přístupové údaje v souladu

s nasazenou bezpečnostní politikou. Typickým příkladem nedodržování bezpečnostní politiky je heslo napsané na papírek (na monitoru, klávesnici apod.). Další příklad je slabé heslo atd. Útokem na sociální vrstvě může být sdělení hesla po telefonu osobě vydávající se za administrátora, zadání hesla do podvodné webové stránky, která je součástí tzv. phishingu.

Před hrozbou manipulace s daty je třeba se bránit pomocí mechanizmů zajištění integrity založených na digitálních podpisech nebo tzv. MAC kódu. Dále je potřeba dodržovat pravidla validace vstupních dat a minimálního nutného oprávnění.

Před hrozbou úniku informací je nutná ochrana kryptografickými prostředky (šifrování) za předpokladu dodržování bezpečnostní politiky.

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních služeb, řízením přístupu, filtrováním dat. Dále je potřeba zajistit fyzickou ochranu.

Před hrozbou zvýšení oprávnění je třeba se chránit dodržováním bezpečnostní politiky. Dodavatel systému musí dodržovat tzv. best practices při návrhu a implementaci systému.

5.1.2 Perimetrický radar

Perimetrický radar je součástí ICT infrastruktury provozu letišť. Perimetrický radar je propojen na bezpečnostní dispečink. Narušení systému perimetrického radaru může mít za následek přímé lokální ohrožení bezpečnosti letiště. Narušení IS může být provedeno zejména formou manipulace s daty poskytovanými systémem perimetrického radaru bezpečnostnímu dispečinku. Tato manipulace může způsobit, že narušitel nebude prostřednictvím perimetrického radaru detekován (jeho přítomnost bude manipulací s daty před systémem radaru anebo před jeho operátorem maskována), anebo může dále vykazovat falešný zdroj narušení perimetru letiště. Z IS perimetrického radaru anebo jeho počítačové sítě může dále dojít k úniku informací o polohách objektů v rámci perimetru. Manipulací s daty v síti perimetrického radaru a jejich nahromaděním může dojít až k jejímu zahlcení, což může mít za důsledek odepření služby vedoucí k vyřazení perimetrického radaru z provozu a přímé ohrožení bezpečnosti letiště.

IS perimetrického radaru nemá žádné přímé propojení do kritické infrastruktury. Tímto tedy nemá žádný přímý nebo zprostředkovaný vliv na KI.

Vzhledem k předchozí analýze plynou pro zabezpečení ICT perimetrického radaru před kybernetickými útoky následující doporučení.

Před hrozbou manipulace s daty je vhodné se bránit pomocí důsledného oddělení (i fyzického) datové sítě perimetrického radaru od ostatní počítačové sítě letiště. Je vhodné uvažovat o využití datových diod, které mohou komunikaci mezi sítí radaru a běžnou sítí letiště ještě posílit. Výstup ze sítě perimetrického radaru je nanejvýš vhodné zabezpečit pomocí mechanizmů zajištění integrity založených např. na tzv. MAC kódu. Kabely datové sítě perimetrického radaru je třeba fyzicky chránit před jejich napadením.

Před hrozbou úniku informací je nutná ochrana kryptografickými prostředky (šifrování) za předpokladu dodržování bezpečnostní politiky.

Před hrozbou odepření služby je nutno se bránit důsledným oddělením sítě perimetrického radaru od běžné sítě letiště. Bude-li výstup z radaru jednosměrný a bude-li síť oddělena, bude značně obtížně provést útok typu DoS z vnější (běžné) počítačové sítě. Jako možnou příčinu DoS v síti perimetrického radaru spatřujeme zejména poškození datových cest perimetrického radaru anebo jeho zarušení na spektrální úrovni. Tyto významné výpadky funkce

musejí být detekovány obsluhou bezpečnostního dispečinku a ostraha letiště má pro takové případy připraveny příslušné postupy.

5.1.3 Osvětlení přistávací dráhy

Osvětlení přistávací dráhy je propojeno na IS AMS (a tím zprostředkovaně také na bezpečnostní dispečink a ŘLP). Narušení systému osvětlení dráhy může mít za následek přímé lokální ohrožení bezpečnosti letiště manipulací s daty systému osvětlení, fyzickým poškozením světel, anebo znepřístupněním ovládání systému světel.

IS ovládání osvětlení přistávací dráhy nemá žádné přímé propojení do kritické infrastruktury. Tímto tedy nemá žádný přímý nebo zprostředkovaný vliv na KI.

Doporučení pro zajištění kybernetické bezpečnosti IS ovládání osvětlení přistávací dráhy je jeho důsledné oddělení od běžných systémů letiště a fyzické zabezpečení komunikačních kabelů.

Vzhledem k předchozí analýze plynou pro zabezpečení IS ovládání osvětlení přistávací dráhy před kybernetickými útoky následující doporučení.

Před hrozbou manipulace s daty je vhodné se bránit pomocí důsledného oddělení (i fyzického) datové sítě ovládání osvětlení dráhy od ostatní počítačové sítě letiště. Kabely datové sítě osvětlení dráhy je třeba fyzicky chránit před jejich napadením.

Před hrozbou odepření služby je nutno se bránit důsledným oddělením sítě osvětlení od běžné sítě letiště. Jako možnou příčinu DoS v síti spatřujeme zejména poškození datových cest anebo fyzické poškození osvětlení. Tyto významné výpadky funkce musejí být detekovány obsluhou provozního a bezpečnostního dispečinku a provoz i ostraha letiště mají pro takové případy připraveny příslušné postupy.

5.1.4 Kamerový systém

Kamerový systém je propojen s bezpečnostním dispečinkem. Narušení kamerového systému může mít za následek přímé lokální ohrožení bezpečnosti letiště. Jako narušení uvažujeme vyřazení z provozu, ovlivnění funkčnosti částí kamerového systému anebo únik informací.

Podvržení identity může nastat v důsledku zneužití uživatelských přístupových údajů oprávněného zaměstnance. Pokud je kamerový systém je připojen k LAN, připadá v úvahu podvržení identity po bezdrátovém i datovém kanálu.

Manipulace s daty může být provedena lidským zásahem, tj. zásahem oprávněného (i neoprávněného) uživatele, například na bezpečnostním dispečinku, anebo v serverovně kamerového systému. Co se týče fyzického zásahu do kamerového systému, ten může nastat fyzickým přerušením datových linek. Kamerový systém je připojen k LAN, proto připadá v úvahu možnost manipulace s přenášeným obrazem kamerového systému či dalšími daty tohoto sytému při přenosu dat po metalické anebo bezdrátové síti.

Únik informací z kamerového systému může nastat prostřednictvím obsluhy v bezpečnostním dispečinku nebo obsluhy kamerového systému anebo odposlechem audiovizuálního signálu buď po metalické síti, po které se jeho data přenáší, nebo bezdrátové síti je-li propojena s LAN. Další možnosti je odposlech signálu přímo z kamery, je-li bezdrátová.

Odepření služby může nastat v případě, bude-li zahlcená metalická síť, po které je přenášen audiovizuální signál. Zahlcení může nastat rovněž v případě, je-li LAN propojená s bezdrátovou sítí – zdroj může být u ní. Kamerový systém je též možné zahltit zarušením kamerového signálu.

Kamerový systém nemá žádné přímé propojení do kritické infrastruktury. Tímto tedy nemá žádný přímý nebo zprostředkovaný vliv na KI.

Vzhledem k předchozí analýze plynou pro zabezpečení kamerového systému před kybernetickými útoky následující doporučení.

Pro omezení hrozby podvržení identity je třeba důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou.

Před hrozbou manipulace s daty, úniku informací a odmítnutí služby je nutno se chránit pomocí důsledného oddělení od běžných systémů letiště a fyzického zabezpečení komunikačních kabelů. Dále je vhodné nepoužívat bezdrátové připojení kamer.

Před hrozbou úniku informací lidským kanálem je nutno bránit se důsledným dodržováním bezpečnostní politiky a omezením okruhu oprávněných osob.

5.1.5 Kartový přístupový systém

Kartový přístupový systém může být různou měrou propojen s ekonomickým informačním systémem (personální část). Narušení kartového systému může mít za následek přímé lokální ohrožení bezpečnosti letiště. Jako možná narušení uvažujeme podvržení identity, manipulaci s daty, popíratelnost, únik informací, odmítnutí služby a zvýšení oprávnění.

Podvržení identity může nastat v důsledku útoků na sociální vrstvě, odcizení karty, odposlechu a opakování komunikace, přepojování komunikace nebo klonování karty. Podvržení identity je možné jak lidským, tak i fyzikálním, bezdrátovým a datovým kanálem (kartový přístupový systém je obvykle řešen pomocí technologie bezkontaktních karet).

Manipulace s daty může být provedena fyzickým připojením na řídicí a stavové signály elektronických zámků přístupového systému, případně útokem na řídicí počítač. Přístupový systém je připojen k LAN, proto připadá v úvahu možnost manipulace s databází osob a oprávnění přístupu, jakož i se záznamy vstupů prostřednictvím metalické popřípadě bezdrátové sítě.

Popíratelnost se týká případů, kdy osoba popře, že vstoupila do oblasti chráněné přístupovým systémem, a následkem zranitelnosti systému jí tento vstup není možno prokázat. Zranitelností mohou být v tomto případě nedostatečné záznamy o vstupech (logy), které neunesou forenzní zkoumání. Dále se může jednat o zranitelnou technologii čipových karet, kdy je možno demonstrovat podvržení identity a tím zpochybnit záznam o vstupu konkrétní osoby.

Únik informací z kartového přístupového systému může nastat čtením osobních informací z karty, případně informací z databáze držitelů karet. V úvahu připadá bezdrátový a datový kanál.

Odepření služby může nastat vlivem fyzického narušení funkce systému, dále zahlcením snímače elektromagnetickým polem nebo po datové síti, případně zahlcení řídicích počítačů nebo centrálního serveru.

Zvýšení oprávnění může nastat v případě modifikace karty útočníkem, který zneužije zranitelnost čipové karty. Útočník modifikuje kartu s cílem získat oprávnění k přístupu, na který nemá nárok. V úvahu připadá užití bezdrátového kanálu.

Kartový přístupový systém nemá žádné přímé propojení do kritické infrastruktury. Tímto tedy nemá žádný přímý vliv na KI. Zprostředkovaný vliv na KI může nastat v případě, že by neoprávněným vstupem do chráněného prostoru došlo k ohrožení systému propojeného se systémem patřícím do KI.

Doporučení pro zajištění kybernetické bezpečnosti kartového přístupového systému je jeho důsledné oddělení od běžných systémů letiště a fyzické zabezpečení komunikačních kabelů. Dále je nutné zajistit, aby použitá technologická platforma čipových karet poskytovala odpovídající mechanizmy zabezpečení (šifrování, autentizace), aby jejich implementace byla aktuální a bezpečná proti prolomení, a také aby přístupový systém tyto mechanizmy využíval.

Proti hrozbě podvržení identity je nutné se bránit jednak důsledným dodržováním bezpečnostní politiky, použitím bezpečné technologické platformy a využíváním bezpečnostních mechanizmů. Zvýšení odolnosti proti podvržení identity je možno dosáhnout využitím vícefaktorové autentizace (PIN, otisk prstu, sken duhovky apod.).

Proti manipulaci s daty je nutné se bránit důsledným oddělením od běžných systémů a fyzickým zabezpečením komunikačních kabelů. Ochrana databáze uživatelů karet a jejich oprávnění, stejně jako záznamy vstupů se mají chránit zajištěním integrity dat, zabezpečením propojení na síť LAN a řízením přístupu k systému. Proti manipulaci s daty na kartě je potřeba se bránit použitím bezpečné technologické platformy čipových karet a důsledným využíváním bezpečnostních mechanizmů.

Obrana před hrozbou popíratelnosti spočívá v prokazatelném zajištění integrity záznamů o vstupech do chráněných prostor a použití technologie čipových karet odolné proti podvržení identity.

Proti hrozbě úniku informací je nutné se bránit šifrováním dat na kartě a použití bezpečné platformy čipových karet. Proti úniku informací z centrálního serveru je nutné se bránit řízením přístupu a dodržováním bezpečnostní politiky.

Před hrozbou odepření služby je třeba se bránit jednak fyzickou ochranou jednotlivých prvků systému (snímačů, zámků, kabelů, řídicích počítačů a centrálního serveru), a dále dostatečným dimenzováním centrálního serveru a filtrováním dat. Vzhledem k povaze komunikace bezkontaktních čipových karet nelze stoprocentně ochránit snímače karet před zarušením elektromagnetickým polem. Případné rušení je předpokládáno lokální, tj. může zasáhnout provoz jednoho nebo několika málo snímačů.

Před hrozbou zvýšení oprávnění je třeba se chránit volbou bezpečné platformy, tj. technologie čipových karet, která poskytuje potřebné bezpečnostní mechanizmy (autentizace, šifrování), a to na vysoké úrovni bezpečnosti s ohledem na aktuální znalosti útoků na čipové karty. Dále je potřeba zvolit systém, které dostupné bezpečnostní mechanizmy využívá a dodržuje tzv. best practices při návrhu a implementaci systému. Je také potřeba dodržovat bezpečnostní politiky a příslušně k tomu školit zaměstnance.

5.2 Analýza ICT letištního provozu

V této části textu budeme rozebírat kybernetické ohrožení ICT letištního provozu. Do analýzy zahrneme jednotlivé komponenty systému DCS, dále systémy CUS, FIDS a databázi AODB.

5.2.1 DCS – Departure Control System

Tabulka 4 obsahuje charakterizaci vzájemného propojení jednotlivých komponent systému DCS s vnějšími systémy, a dále klasifikaci ohrožení ve vztahu ke kritické infrastruktuře. Ve sloupcích ohrožení jsou uvedeny jednotlivé typy možných ohrožení, s případným dopadem na kritickou infrastrukturu.

	Propojení na jiný systém (lokální/vnější)	**Přímé lokální ohrožení**	**Indukované ohrožení KI**	**Přímé ohrožení KI**	**Poznámka**
Check-In/Boarding	DCS, SITA, AODB, CUS	Podvržení identity a oprávnění, získání neoprávněného přístupu do systému. Únik a manipulace osobních dat pasažérů.	Ohrožení plynoucí z nesprávných osobních údajů.	Nebezpečí v případě získaného oprávnění, které platí i pro vnější systémy. Propojeni, ale ne přímé ohrožení.	Neznámá osoba na palubě
BHS – Baggage Handling System	DCS, SITA, FIDS, AODB, CUS	Podvržení identity a oprávnění, získání neoprávněného přístupu do systému. Únik a manipulace s údaji zavazadel pasažérů.	Ohrožení plynoucí z nesprávných údajů zavazadel pasažérů.		bomba
BRS - Baggage Reconciliation Systém	DCS, SITA, AODB, CUS	WLAN ruční skener	Check-In, BHS SITA, FPMS	Možné propojení přes databázi systémů	bomba
FPMS – Flight Plan Management System	DCS, SITA, AODB, CUS, Koordinace s vnějškem		? Koordinace s vnějškem	Možné při synchronizaci letových plánů	DOS
W&B – Weight and Balance	DCS, AODB, CUS, (Check-In)	Rozvážení letadla.	Check-In		Narušení těžiště letadla

Tabulka 4. Typy komunikaci mezi jednotlivými komponenty systému DCS s vnějšími systémy.

Tabulka 5 obsahuje klasifikaci ohrožení jednotlivých komponent systému DCS podle metodiky STRIDE. Jednotlivé buňky obsahují charakterizaci příslušného ohrožení, a ve zkratce uvádějí, prostřednictvím kterých kanálů (podle OSSTMM, viz tab. 1).

Typ ohrožení	**Podvržení identity**	**Manipulace s daty**	**Popíratelnost**	**Únik inf.**	**Odepření služby**	**Zvýšení oprávnění**

Komponenta	(S)	(T)	(R)	(I)	(D)	(E)
Check-In/Boarding	Ano – přístup L, D	Ano – pasažér: nesouhlas osobních dat L, B, D	Ne	Ano – seznam pasažérů (osobní údaje) L, B, D	Ano B, D	Ano – přístup L, D
BHS – Baggage Handling System	Ano – přístup L, D	Ano – rentgenový snímek, hmotnost L, B, D	Ne	Ano – rentgenové snímky L, B, D	Ano B, D	Ano – přístup L, D
BRS - Baggage Reconciliation Systém	Ano – přístup L, D	Ano – porušení párovaní L, B, D	Ne	Ano – destinace pasažérů L, B, D	Ano B, D	Ano – přístup L, D
FPMS – Flight Plan Management System	Ano – přístup L, D	Ano – rozpory v letových plánech L, B, D	Ne	Ne	Ano B, D	Ano – přístup L, D
W&B – Weight and Balance	Ano – přístup L, D	Ano – rozvážení L, B, D	Ne	Ne	Ano B, D	Ano – přístup L, D

Tabulka 5. Třídy kybernetických ohrožení metodiky STRIDE pro jednotlivé komponenty systému DCS.

Systém DCS (viz výše) jednak zajišťuje provoz letiště samotného, a tedy jeho narušení může mít za následek přímé lokální ohrožení bezpečnosti, ale také je propojen s ostatními letišti přes systém výměny zpráv (např. SITA-TEX). Tím pádem jeho narušení může způsobit indukované ohrožení, a tedy mít zprostředkovaný dopad i na jiná letiště, potenciálně i prvky KI. Jako možná narušení uvažujeme podvržení identity, manipulaci s daty, únik informací, odepření služby a zvýšení oprávnění.

Podvržení identity se týká zejména přístupu k systému prostřednictvím přihlašovacích údajů zaměstnance. Může nastat v důsledku útoků na sociální vrstvě (lidský kanál), případně útokem na zranitelný systém přes síť LAN (datový kanál). V závislosti na konkrétním modulu DCS může mít podvržení identity různé dopady, a to podle konkrétní funkce jednotlivých modulů. Podvržením identity nastane neoprávněný přístup do systému, který může být prostředkem k vzniku ostatních druhů ohrožení bezpečnosti. Podobná situace nastává při ohrožení bezpečnosti zvýšením oprávnění.

Specificky v komponentě systému DCS Check-In/Boarding mohou manipulace s daty a únik informací mít za následek zfalšování resp. prozrazení osobních údajů cestujících. Tato ohrožení nastávají prostřednictvím lidského, bezdrátového nebo datového kanálu.

Obdobně v komponentě BHS mohou manipulace s daty a únik informací mít za následek zfalšování resp. únik rentgenových snímků obsahu zavazadel a manipulaci s informací o hmotnosti zavazadel. Narušení může nastávat prostřednictvím lidského, bezdrátového nebo datového kanálu.

V komponentě BRS mohou manipulace s daty a únik informací mít za následek porušení informací o párování cestující-zavazadlo, v případě úniku informací je následek prozrazení destinace cesty a informace o zavazadlech cestujících. Narušení může nastávat prostřednictvím lidského, bezdrátového nebo datového kanálu.

V komponentě W&B může manipulace s daty způsobit rozvážení letadla a tím ohrožení jeho bezpečnosti. Narušení může nastávat prostřednictvím lidského, bezdrátového nebo datového kanálu.

V komponentě FPMS může manipulace s daty způsobit potíže při organizaci provozu na letišti. Narušení může nastávat prostřednictvím lidského, bezdrátového nebo datového kanálu.

Pro celý systém DCS připadá v úvahu hrozba odepření služby, která může nastat formou zahlcení serverů nebo propojení sítí LAN nebo WLAN.

Systém DCS nemá žádné přímé propojení do kritické infrastruktury, nemá tedy přímý vliv na KI. Zprostředkovaný vliv na KI může nastat v případě, že narušením lokálního systému bude narušena integrita dat, která se přenášejí do prvků KI. V případě komponenty Check-In/Boarding se jedná o ohrožení plynoucí z nesprávných osobních údajů cestujících, a následně vstup útočníků na palubu letadla i na letišti patřícím do KI. V případě komponenty BHS se jedná o ohrožení plynoucí z nesprávných údajů o odbavených zavazadlech (nekontrolovaný obsah zavazadla v oblasti KI). Podobné ohrožení plyne i v případě komponenty BRS. Pro komponentu FPMS připadá v úvahu ohrožení KI v případě, že se letové plány sdílí s prvky KI a mají vliv na řízení letiště patřícího do KI. V případě komponenty W&B jsou dopady narušení převážně lokální a nemají výrazný vliv na KI.

Proti hrozbě podvržení identity, manipulaci s daty, úniku informací a zvýšení oprávnění je nutné důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou. Dále je nutné zabezpečit fyzickou a kryptografickou ochranu počítačů propojených pomocí sítě LAN, dbát na odpovídající kryptografické zabezpečení případných bezdrátových sítí a důsledně dodržovat bezpečnostní politiku při řízení přístupu k systému.

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních prostředků, řízením přístupu a filtrováním dat. Dále je potřeba zajistit fyzickou ochranu před neoprávněnou manipulací s počítači a síťovými prvky.

5.2.2 Systémy CUS, FIDS, AODB

Tabulka 6 obsahuje charakterizaci vzájemného propojení jednotlivých komponent ICT letištního provozu s vnějšími systémy, a dále klasifikaci ohrožení ve vztahu ke kritické infrastruktuře. Ve sloupcích ohrožení jsou uvedeny jednotlivé typy možných ohrožení, s případným dopadem na kritickou infrastrukturu.

	Propojení na jiný systém (lokální/vnější)	**Přímé lokální ohrožení**	**Indukované ohrožení KI**	**Přímé ohrožení KI**	**Poznámka**
CUS (CUTE + CUSS)	DCS, SITA, AODB	Podvržení identity a oprávnění, získaní neoprávněného přístupu do systému (pro CUTE). Únik a manipulace osobních dat pasažérů.	Ohrožení plynoucí z nesprávných osobních údajů (pro CUTE).	Nebezpečí v případě získaného oprávnění, které platí i pro vnější systémy. Propojeni, ale ne přímé ohrožení (pro CUTE).	Neznámá osoba na palubě
FIDS	DCS, AODB	Šíření poplašné zprávy, manipulace s daty.	Není	Není	
AODB	DCS, SITA, CUS, FIDS	Úplná kontrola nad ICT letového provozu.	Manipulace s daty, která ovlivňují KI		

Tabulka 6. Typy komunikaci mezi jednotlivými komponenty ICT infrastruktury letištního provozu (mimo DCS) s vnějšími systémy.

Tabulka 7 obsahuje klasifikaci ohrožení jednotlivých komponent ICT letištního provozu podle metodiky STRIDE. Jednotlivé buňky obsahují charakterizaci příslušného ohrožení, a ve zkratce uvádějí, prostřednictvím kterých kanálů (podle OSSTMM, viz tab. 1).

Typ ohrožení **Komponenta**	**Podvržení identity (S)**	**Manipulace s daty (T)**	**Popíratelnost (R)**	**Únik inf. (I)**	**Odepření služby (D)**	**Zvýšení oprávnění (E)**
CUS (CUTE + CUSS)	Ano – přístup CUTE – obsluha CUSS – cestující L, D	Ano – pasažér: nesouhlas osobních dat L, B, D	Ne	Ano – seznam pasažérů (osobní údaje) L, B, D	Ano – útokem po síti B, D	Ano – přístup L, D
FIDS	Ano – útok na server L, D	Ano – obsluha, server L, D, B	Ne	Ne, výstupy jsou veřejné	Ano – útokem po síti D	Ne
AODB	Ano – útok na server L, B, D	Ano L, B, D	Ne	Ano L, B, D	Ano L, B, D	Ano L, B, D

Tabulka 7. Třídy kybernetických ohrožení metodiky STRIDE pro jednotlivé komponenty ICT infrastruktury letištního provozu (mimo DCS).

5.2.2.1 Systém CUS

Systém CUS slouží pro check-in pasažérů, který může být proveden buď prostřednictvím samoobslužného terminálu CUSS anebo prostřednictvím terminálu s obsluhou CUTE. CUS systém je propojen jednak na lokální DCS a letištní databázi AODB, prostřednictvím níž je propojen na SITA a do dalších letištních systémů. Jeho narušení může mít za následek přímé lokální ohrožení bezpečnosti, ale také je propojen s ostatními letišti přes systém výměny zpráv (např. SITATEX). Tím pádem jeho narušení může způsobit indukované ohrožení, a tedy mít zprostředkovaný dopad i na jiná letiště, potenciálně i prvky KI. Jako možná narušení uvažujeme podvržení identity, manipulaci s daty, únik informací, odepření služby a zvýšení oprávnění.

Podvržení identity se týká zejména přístupu k systému prostřednictvím přihlašovacích údajů zaměstnance. Může nastat v důsledku útoků na sociální vrstvě (lidský kanál), případně útokem na zranitelný systém před síť LAN (datový kanál). Podvržením identity nastane neoprávněný přístup do systému, který může být prostředkem k vzniku ostatních druhů ohrožení bezpečnosti. Podobná situace nastává při ohrožení bezpečnosti zvýšením oprávnění.

Manipulace s daty a únik informací mohou mít za následek zfalšování resp. prozrazení osobních údajů cestujících. Tato ohrožení nastávají prostřednictvím lidského, bezdrátového nebo datového kanálu. Specificky pro komponentu CUSS je nutno poukázat na zvýšené riziko manipulace se zařízením, protože cestující se zařízením přímo interaguje.

Pro systém CUS připadá v úvahu hrozba odepření služby, která může nastat formou zahlcení serverů nebo propojení sítí LAN nebo WLAN.

Systém CUS nemá žádné přímé propojení do kritické infrastruktury, nemá tedy přímý vliv na KI. Zprostředkovaný vliv na KI může nastat v případě, že narušením lokálního systému bude narušena integrita dat, která se přená-

šejí do prvků KI. Jedná se o ohrožení plynoucí z nesprávných osobních údajů cestujících, a následně vstup útočníků na palubu letadla i na letišti patřícím do KI.

Proti hrozbě podvržení identity, manipulaci s daty, úniku informací a zvýšení oprávnění je nutné důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou. Dále je nutné zabezpečit fyzickou a kryptografickou ochranu počítačů propojených pomocí sítě LAN, dbát na odpovídající kryptografické zabezpečení případných bezdrátových sítí a důsledně dodržovat bezpečnostní politiku při řízení přístupu k systému.

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních prostředků, řízením přístupu a filtrováním dat. Dále je potřeba zajistit fyzickou ochranu před neoprávněnou manipulací s počítači a síťovými prvky.

5.2.2.2 Systém FIDS

Systém FIDS je propojen na letištní databázi AODB, prostřednictvím níž je propojen na DCS, FPMS, SITA a do dalších letištních systémů. Jeho narušení může mít za následek přímé lokální ohrožení bezpečnosti. Tím pádem nemá žádný přímý ani zprostředkovaný vliv na KI. Jako možná narušení uvažujeme podvržení identity, manipulaci s daty a odepření služby.

Podvržení identity se týká zejména přístupu k systému prostřednictvím přihlašovacích údajů správce systému. Může nastat v důsledku útoků na sociální vrstvě (lidský kanál), případně útokem na zranitelný systém před síť LAN (datový kanál).

Manipulace s daty může mít za následek zfalšování informací zobrazovaných na informačních panelech. Toto ohrožení nastává prostřednictvím lidského, bezdrátového nebo datového kanálu.

Hrozba odepření služby může nastat formou zahlcení serverů nebo propojení sítí LAN nebo WLAN.

Systém FIDS nemá žádné přímé propojení do kritické infrastruktury, nemá tedy přímý ani zprostředkovaný vliv na KI.

Proti hrozbě podvržení identity a manipulaci s daty je nutné důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou. Dále je nutné zabezpečit fyzickou a kryptografickou ochranu počítačů propojených pomocí sítě LAN, dbát na odpovídající kryptografické zabezpečení případných bezdrátových sítí a důsledně dodržovat bezpečnostní politiku při řízení přístupu k systému. Zobrazované informace jsou z podstaty věci veřejné, tudíž není potřeba je utajovat. Je ale potřeba zajistit jejich integritu.

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních prostředků, řízením přístupu a filtrováním dat. Dále je potřeba zajistit fyzickou ochranu před neoprávněnou manipulací s počítači a síťovými prvky.

5.2.2.3 AODB – Provozní databáze letiště

Provozní databáze letiště tvoří srdce ICT letištní infrastruktury. Přímý průnik muže způsobit kolaps provozu celého letiště. Vzhledem k propojení s ostatními letišti může mít ohrožení AODB indukovaný dopad na kritickou infrastrukturu. Jako možná narušení uvažujeme podvržení identity, manipulaci s daty, únik informací, odepření služby a zvýšení oprávnění.

Podvržení identity se týká zejména přístupu k systému prostřednictvím přihlašovacích údajů zaměstnance. Může nastat v důsledku útoků na sociální vrstvě (lidský kanál), případně útokem na zranitelný systém před síť LAN

(datový kanál). Podvržením identity nastane neoprávněný přístup do systému, který může být prostředkem k vzniku ostatních druhů ohrožení bezpečnosti. Podobná situace nastává při ohrožení bezpečnosti zvýšením oprávnění.

Manipulace s daty a únik informací mohou mít za následek zfalšování resp. prozrazení veškerých informací shromažďovaných v databázi a zpracovávaných ostatními systémy letiště jako DCS, CUS, FIPS apod., včetně detailních informací o letech, letových plánech, zavazadlech a osobních údajů cestujících. Dále mohou být zasaženy informace, které jsou sdíleny s ostatními letišti. Tato ohrožení nastávají prostřednictvím lidského, bezdrátového nebo datového kanálu.

Odepření služby může mít za následek kolaps celého informačního systému, a následně celého provozu letiště. Může nastat formou zahlcení serverů nebo propojení sítí LAN nebo WLAN.

Některé údaje obsažené v AODB jsou sdíleny s informačními systémy patřícími do KI. Zprostředkovaný vliv na KI může nastat v případě, že narušením lokálního systému bude narušena integrita dat, která se přenášejí do prvků KI.

Proti hrozbě podvržení identity, manipulaci s daty, úniku informací a zvýšení oprávnění je nutné důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou. Dále je nutné zabezpečit fyzickou a kryptografickou ochranu počítačů propojených pomocí sítě LAN, dbát na odpovídající kryptografické zabezpečení případných bezdrátových sítí a důsledně dodržovat bezpečnostní politiku při řízení přístupu k systému.

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních prostředků, řízením přístupu a filtrováním dat. Dále je potřeba zajistit fyzickou ochranu před neoprávněnou manipulací s počítači a síťovými prvky.

6 Metodika zabezpečení ICT infrastruktury malých mezinárodních letišť v ČR

Obsahem této kapitoly jsou metodická bezpečnostní opatření a doporučení pro všechny ICT systémy používané na malých mezinárodních letištích s ohledem na platnou legislativu zasahující obdobné informační struktury.

Nejdříve shrneme to, co pro obdobné systémy (ale patřící do kritické infrastruktury) předepisuje vyhláška, která je prováděcím předpisem zákona o kybernetické bezpečnosti. Pak zdůrazníme bezpečnostní požadavky na malá mezinárodní letiště jednak obecné, a dále specifické pro jednotlivé druhy ohrožení, které vyplynuly z analýzy provedené v předchozí kapitole.

Vyhláška č. 316/2014 Sb. [10] stanoví pro správce informačního systému a správce komunikačního systému kritické informační infrastruktury stanovit, hodnotit a aktualizovat bezpečnostní politiku:

§ 5
Bezpečnostní politika
(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoví bezpečnostní politiku v oblastech
a) systém řízení bezpečnosti informací,
b) organizační bezpečnost,
c) řízení vztahů s dodavateli,
d) klasifikace aktiv,
e) bezpečnost lidských zdrojů,
f) řízení provozu a komunikací,
g) řízení přístupu,
h) bezpečné chování uživatelů,
i) zálohování a obnova,
j) bezpečné předávání a výměna informací,
k) řízení technických zranitelností,
l) bezpečné používání mobilních zařízení,
m) poskytování a nabývání licencí programového vybavení a informací,
n) dlouhodobé ukládání a archivace informací,
o) ochrana osobních údajů,
p) fyzická bezpečnost,
q) bezpečnost komunikační sítě,
r) ochrana před škodlivým kódem,
s) nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
t) využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a
u) používání kryptografické ochrany.

[…]

(3) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pravidelně hodnotí účinnost bezpečnostní politiky a aktualizuje ji.
[10]

Uvedené oblasti bezpečnostní politiky citované z vyhlášky č. 316/2014 Sb. jsou závazné pro osoby zodpovědné za provoz informačního nebo komunikačního systému kritické informační infrastruktury. Uvedené oblasti však odpovídají tzv. best practice v kybernetické bezpečnosti subjektů bez ohledu na začlenění do kritické infrastruktury.

Z analýzy provedené v předchozí kapitole vyplývají obecné požadavky na bezpečnostní opatření, která nejsou vázána na specifické ohrožení. Jedná se zejména o fyzickou ochranu, kryptografickou ochranu, ochranu bezdrátových sítí, řízení přístupu a ochranu před zavlečením nežádoucího softwaru a hardwaru.

Následují části shrnující poznatky z analýzy uvedené v předchozí kapitole. Metodická doporučení jsou rozčleněna podle jednotlivých typů ohrožení vycházejících z metodiky STRIDE. Po každý druh ohrožení jsou uvedena doporučení jednak obecně napříč přes všechny systémy ze zabezpečení provozu letiště a ICT letištního provozu, a následně specificky pro jednotlivé konkrétní systémy, kde je to vhodné.

6.1 Podvržení identity

Pro omezení hrozby podvržení identity je třeba důsledně chránit uživatelské přístupové údaje v souladu s nasazenou bezpečnostní politikou, a to jak pro běžné uživatele, tak pro administrátory. Typickým příkladem nedodržování bezpečnostní politiky je heslo napsané na papírek (na monitoru, klávesnici apod.). Další příklad je slabé heslo atd. Útokem na sociální vrstvě může být sdělení hesla po telefonu osobě vydávající se za administrátora, zadání hesla do podvodné webové stránky, která je součástí tzv. phishingu.

Z konkrétních systémů se to týká zejména HZS, kamerového systému, kartového přístupového systému, systémů DCS, CUS a FIDS a provozní databáze letiště AODB.

Specificky pro kartový přístupový systém je nutné použít bezpečné technologické platformy a využívat bezpečnostních mechanizmů. Zvýšení odolnosti proti podvržení identity je možno dosáhnout využitím vícefaktorové autentizace (PIN, otisk prstu, sken duhovky apod.).

6.2 Manipulace s daty

Před hrozbou manipulace s daty je třeba se bránit pomocí mechanizmů zajištění integrity založených na digitálních podpisech nebo tzv. MAC kódu. Dále je potřeba dodržovat pravidla validace vstupních dat a minimálního nutného oprávnění.

Z konkrétních systémů se to týká zejména HZS, perimetrického radaru, osvětlení přistávací dráhy, kamerového systému, kartového přístupového systému, systémů DCS, CUS a FIDS a provozní databáze letiště AODB.

Specificky pro perimetrický radar, osvětlení přistávací dráhy, kamerový systém a kartový přístupový systém je vhodné se bránit pomocí důsledného oddělení (i fyzického) datové sítě těchto systémů od ostatní počítačové sítě letiště. Kabely datové sítě těchto systémů je třeba fyzicky chránit před jejich napadením. Pro perimetrický radar je vhodné uvažovat o využití datových diod, které mohou komunikaci mezi sítí radaru a běžnou sítí letiště ještě posílit. Dále je vhodné nepoužívat bezdrátové připojení kamer.

Specificky pro kartový přístupový systém je nutné chránit databázi uživatelů karet a jejich oprávnění, stejně jako záznamy vstupů zajištěním integrity dat, zabezpečením propojení na síť LAN a řízením přístupu k systému. Proti manipulaci s daty na kartě je potřeba se bránit použitím bezpečné technologické platformy čipových karet a důsledným využíváním bezpečnostních mechanizmů.

6.3 Popíratelnost

Proti hrozbě popíratelnosti (přijatých/vyslaných dat) je nutné se bránit používáním bezpečných asymetrických kryptografických schémat pro autentizaci a elektronický podpis.

Specificky pro kartový přístupový systém obrana před hrozbou popíratelnosti spočívá v prokazatelném zajištění integrity záznamů o vstupech do chráněných prostor a použití technologie čipových karet odolné proti podvržení identity.

6.4 Únik informací

Před hrozbou úniku informací je nutná ochrana kryptografickými prostředky (šifrování) za předpokladu dodržování bezpečnostní politiky. Před hrozbou úniku informací lidským kanálem je nutno bránit se důsledným dodržováním bezpečnostní politiky a omezením okruhu oprávněných osob.

Z uvažovaných systémů se tato hrozba týká HZS, perimetrického radaru, kamerového systému, kartového přístupového systému, systémů DCS a CUS a databáze AODB. Pro systém FIDS platí, že zobrazované informace jsou z podstaty věci veřejné, tudíž není potřeba je utajovat. Je ale potřeba zajistit jejich integritu.

Specificky pro perimetrický radar, osvětlení přistávací dráhy, kamerový systém a kartový přístupový systém je vhodné se bránit pomocí důsledného oddělení (i fyzického) datové sítě těchto systémů od ostatní počítačové sítě letiště. I z hlediska úniku informací je vhodné nepoužívat bezdrátové připojení kamer

6.5 Odepření služby

Před hrozbou odepření služby je nutno se bránit redundancí výpočetních a komunikačních prostředků, řízením přístupu a filtrováním dat. Dále je potřeba zajistit fyzickou ochranu před neoprávněnou manipulací s počítači a síťovými prvky. Tato hrozba se týká všech uvažovaných systémů (HZS, perimetrického radaru, osvětlení dráhy, kamerového systému, kartového přístupového systému, systémů DCS, CUS, FIDS a databáze AODB).

Specificky pro perimetrický radar, osvětlení dráhy, kamerový systém a kartový přístupový systém je nutno se bránit důsledným oddělením sítě konkrétního systému od jiných sítí letiště. Dále je nutno chránit koncový prvek (radar, kameru, světlo, kartový snímač) i jejich propojení před fyzickým poškozením.

Navíc zavedení striktně jednosměrných datových toků z výstupů radaru značně ztíží provedení útoku typu DoS z vnější (běžné) počítačové sítě. Zůstává riziko rušení perimetrického radaru na spektrální úrovni. Není vhodné používat bezdrátové připojení kamer.

Vzhledem k povaze komunikace bezkontaktních čipových karet nelze stoprocentně ochránit snímače karet před zarušením elektromagnetickým polem. Případné rušení je předpokládáno lokální, tj. může zasáhnout provoz jednoho nebo několika málo snímačů.

6.6 Zvýšení oprávnění

Před hrozbou zvýšení oprávnění je třeba se chránit dodržováním bezpečnostní politiky. Dodavatel systému musí dodržovat tzv. best practices při návrhu a implementaci systému. Dále je nutné zabezpečit fyzickou a kryptografickou ochranu počítačů propojených pomocí sítě LAN, dbát na odpovídající kryptografické zabezpečení případ-

ných bezdrátových sítí a důsledně dodržovat bezpečnostní politiku při řízení přístupu k systému. Z uvažovaných systémů se tato hrozba týká HZS, kartového přístupového systému, systémů DCS a CUS a databáze AODB.

Specificky pro kartový přístupový systém je nutné jeho důsledné oddělení od běžných systémů letiště a fyzické zabezpečení komunikačních kabelů. Dále je nutné zajistit, aby použitá technologická platforma čipových karet poskytovala odpovídající mechanizmy zabezpečení (šifrování, autentizace), aby jejich implementace byla bezpečná proti prolomení, a to na vysoké úrovni bezpečnosti s ohledem na aktuální znalosti útoků na čipové karty. Systém musí být vytvořen tak, aby tyto mechanizmy účinně využíval.

7 Komunikační systémy obecně

Doporučení této metodiky vycházejí z vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) v platném znění. Přestože se tato vyhláška se na malá letiště nevztahuje, protože nejsou subjekty ve smyslu § 3 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), je vhodné podmnožinu organizačních i technických opatření předepisovaných vyhláškou aplikovat i na malá letiště. Dodržování vyhláškou předepisovaných opatření zlepší připravenost malých letišť na stav kybernetického nebezpečí a harmonizuje organizační i technická opatření používaná na malých letištích.

Po stránce organizačních opatření je nutno konstatovat, že malá letiště sama o sobě již část vyhlášky naplňují například použitím řízením rizik (§ 4 vyhlášky) a bezpečnostních politik (§ 5 vyhlášky). Zavedení a dodržování bezpečnostních politik ve smyslu vyhlášky standardizuje bezpečnostní politiky malých letišť. Samotné zavedení bezpečnostních politik ve smyslu vyhlášky však nestačí. Je nutné jejich dodržování periodicky kontrolovat ve smyslu § 15 odst. 1 písm. b) a § 15 odst. 2 a 3 a přijímat opatření, která povedou k odstranění kontrolou nalezených nedostatků. Kontroly je vhodné provádět jak interními mechanismy, tak i s použitím subjektů certifikovaných pro audit kybernetické bezpečnosti ve smyslu § 6 odst. 6 vyhlášky.

Po stránce technických opatření je opět nutno konstatovat, že malá letiště část předepisovaných technických opatření již aplikují (§§ 16-27 vyhlášky). Účinnost technických opatření je rovněž nutné kontrolovat, zejména prováděním hodnocení zranitelností (angl. vulnerability assessment) technických prostředků interními silami automatizovaně i externími nezávislými subjekty. Zjištěné nedostatky spolu s informacemi z nástrojů pro detekci kybernetických bezpečnostních událostí je nutné periodicky vyhodnocovat a opět přijímat opatření na organizační i technické úrovni, která by je buďto odstranila, anebo snížila riziko na přijatelnou úroveň.

8 Závěr

Tato metodika rozebírá problematiku obrany před kybernetickými hrozbami malých mezinárodních letišť v České republice. Malé mezinárodní letiště je v současné době každé letiště mezinárodní přepravy kromě Letiště Václava Havla v Praze. Tato malá mezinárodní letiště nespadají pod kritickou infrastrukturu dle definice Nařízení vlády č. 315/2014 [11]. Přesto je důležité se kybernetickou bezpečností malých letišť zabývat, protože kromě lokálního měřítka mohou mít vliv i na bezpečnost kritické infrastruktury. Je třeba upozornit na to, že předkládaná metodika nemůže nahradit zákon o kybernetické bezpečnosti a jeho prováděcí předpisy, může ho doplňovat a rozvíjet.

Provedená analýza se týká pouze kybernetické bezpečnosti, ne však fyzickým zabezpečením letišť, může se ho však částečně dotýkat (jako v případě kartového přístupového systému nebo perimetrického radaru). Analýza zahrnuje rozbor možných ohrožení, neobsahuje však vyhodnocení rizik – to je třeba vždy provádět pro konkrétní letiště s ohledem na pravděpodobnosti vzniku incidentů a jejich dopad na aktiva daného letiště.

V tomto textu byla provedena analýza jednotlivých komponent ICT infrastruktury malých mezinárodních letišť z hlediska hrozeb rozčleněných podle metodiky STRIDE a komunikačních kanálů podle metodiky OSSTMM. Do analýzy byly zahrnuty systémy zabezpečení provozu letiště (např. hasičský záchranný systém nebo perimetrický radar) a ICT letištního provozu (zahrnující systémy sloužící pro odbavení cestujících a centrální databázi).

Metodická doporučení jsou strukturována podle jednotlivých kategorií ohrožení podle metodiky STRIDE. V každé kategorii jsou uvedena obecná doporučení (bez vazby na konkrétní komponenty systému), a dále specifická doporučení pro určité komponenty informačních systémů.

Předkládaná metodika mohla vzniknout jen za aktivní účasti a podpory managementu a personálu Letiště Ostrava, za což jim patří naše poděkování.

Tato metodika vznikla v době, kdy je problematika kybernetické bezpečnosti zvláště aktuální. Bezpečnost letecké dopravy osob je vystavena neustálým útokům ze strany teroristů, přičemž obecně stoupá četnost útoků využívajících stále sofistikovanějších metod a prostředků pro zneužití ICT infrastruktury. Současná letecká doprava se bez ICT infrastruktury neobejde a je jen otázkou času, kdy se propojí kybernetický terorizmus s útoky na bezpečnost letecké dopravy.

Poděkování

Tato metodika vznikla za podpory grantu č. VG20132015130, „Využití nástrojů krizového řízení, rizikového inženýrství, systémového inženýrství a moderních technologií ke zvýšení ochrany před protiprávními činy na mezinárodních letištích v České republice“.

Autoři metodiky by dále rádi vyjádřili poděkování panu Danielu Nogolovi a dalším zaměstnancům Letiště Ostrava za cenné podněty a pomoc při vypracování této metodiky.

9 Literatura

1. Organizace severoatlantické smlouvy: *Lisbon Summit Declaration.* 2010. http://www.nato.int/cps/en/natolive/official_texts_68828.htm
2. Česká republika: *Bezpečnostní strategie České republiky 2011*.
3. Národní bezpečnostní úřad: *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015*.
4. Vláda České republiky: *Usnesení vlády č. 781/2011*. https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E.
5. Národní bezpečnostní úřad: *Věcný záměr zákona o kybernetické bezpečnosti*. 2011.
6. Národní bezpečnostní úřad: *Akční plán ke Strategii pro oblast kybernetické bezpečnosti v České republice na období 2012 - 2015*.
7. Ministerstvo vnitra České republiky. *Příloha k nařízení vlády č. 432/2010 Sb.*
8. The Institute for Security and Open Methodologies. *OSSTMM 3 – The Open Source Security Testing Methodology Manual.* http://www.isecom.org/research/osstmm.html, 2010.
9. Microsoft Corp. *The STRIDE Threat Model*. https://msdn.microsoft.com/library/ms954176.aspx, 2005.
10. Vláda ČR: *Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)*. 2014.
11. Vláda ČR: *Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.* 2014

Příloha 1

VG20132015130 - Analýza propojení a funkčnosti informačních systémů letiště