Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Využití informačních technologií v letecké přepravě na letištích a možnosti zabezpečení proti možným hackerským útokům

Bakalářská práce

Autor: Radek Kápička
Studijní obor: ai3-p

Vedoucí práce: Ing. Hana Švecová

Hradec Králové Duben 2021

Prohlášení:

Prohlašuji, že jsem bakalářskou/diplomovou práci zpracoval/zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2021 Radek Kápička

Poděkování:
Chtěl bych tímto poděkovat mé vedoucí bakalářské práce Ing. Haně Švecové za odborné vedení práce, cenné rady, náměty a odborné připomínky. Dále bych rád poděkoval své rodině za podporu po celou dobu mého studia.

Anotace

Bakalářská práce se zaměřuje na využití informačních technologií v letecké přepravě a na letištích, a možnosti zabezpečení proti hackerským útokům. V práci jsou popsány informační a komunikační systémy využívané jak leteckými společnostmi, tak i správou samotných letišť. Dále práce navazuje analýzou hackerských útoků na letiště, která obsahuje útoky z minulosti, tak i útoky z posledních let. V návaznosti na zmíněné útoky dále práce pokračuje kapitolou, která se zaobírá tématy zabezpečení proti možným útokům a metodologií prevence proti útokům. V závěru práce jsou popsány kroky k lepšímu zabezpečení letišť, kde jsou shrnuty investice letišť do zabezpečení kybernetického prostoru a akce prováděné mezinárodními společnostmi pro bezpečnost.

Annotation

Title: The use of information technology in air transport at airports and security options against possible hacker attacks

The bachelor thesis focusses on usage of information technologies in air transport and on airports and security options against hacker-attacks. In this work are described information and communication systems used both by airlines and by the airport itself. Furthermore, the work follows with a research on hacker attacks on the airport, which includes attacks from the past, as well as attacks from recent years. In connection with the mentioned attacks, the work continues with a chapter that deals with topics such as security against possible attacks and the methodology of prevention against attacks. At the end, the work describes the steps to better secure airports, which summarizes the investment of airports in cybersecurity and the actions taken by international security companies.

Obsah

Seznam obrázků

1 Úvod

Vzhledem k rychlosti vývoje nových technologií je zapotřebí neustále sledovat nejnovější trendy a na ně se adaptovat. To vše se děje i v leteckém průmyslu. Proto prvním cílem práce je zmapovat vývoj informačních systémů právě v letectví. Zde jsou popsány vývoje systémů v letectví od samotného počátku. Na tuto část navazuje analýza systémů využívaných v moderní letecké přepravě. Jsou zde informace o systémech, které využívají letecké společnosti, globálních distribučních systémech, což jsou například systémy pro distribuci letenek pasažérům. Posledními systémy v této části jsou informační systémy letiště, které pomáhají správcům letiště například se správou budov a podobně.

Vzhledem k tomu, kolik je na letištích různých systémů, které jsou závislé na připojení k internetu, bylo by velice nepravděpodobné, že by na tyto systémy nebyly prováděny kybernetické útoky. V práci je souhrn některých kybernetických útoků provedených v minulosti, ale i v posledních letech. Útoky jsou vedeny nejčastěji na letecké společnosti, ale nevyhýbají se ani vlastní správě letišť či samotným výrobcům letadel.

Následně na hackerské útoky navazuje část, která řeší problematiku zabezpečení proti útokům. Zde je popsán vývoj zabezpečení proti útokům kybernetickým, tak i fyzickým (teroristické útoky). Na což navazuje metodologie prevence proti kybernetickým útokům. V této kapitole jsou takzvané scénáře, které představují možné kybernetické útoky a věci s nimi spojené, jako například, jak útok vypadá, jak se proti němu dá bránit, či jaký je postup, když dojde k samotnému útoku. V poslední části této kapitoly jsou zaznamenány kroky k lepšímu zabezpečení letišť. Sem patří reporty z posledních let, kde jsou zobrazeny investice letišť do ochrany kybernetického prostoru, ale i plány na následující roky.

2 Cíl práce

Cílem této bakalářské práce je analýza leteckých informačních technologií (systémů) využívaných v letecké přepravě a na letištích a analýza kybernetických útoků včetně návrhu doporučení pro efektivnější zabezpečení informačních technologií (systémů) využívaných v letecké přepravě a na letištích.

3 Metodika

Metodický postup pro zpracování této kvalifikační práce lze rozdělit do tří částí, které na sebe chronologicky navazují. V první části bude provedena je analýza existujících informačních systémů používaných v letecké přepravě a na letištích. V druhé části bude provedena analýza kybernetických útoků v informačních systémech letecké přepravy včetně charakteristiky analyzovaných hrozeb. Ve třetí části bude provedeno vy vyhodnocení a návrh možných doporučení při předcházení kybernetickým útokům v informačních systémech využívaných v letecké přepravě.

4 Informační technologie v letecké přepravě

4.1 Základní pojmy

4.1.1 Informační a komunikační technologie

Informační technologie jsou úzce spojovány s komunikačními technologiemi. Proto se tyto pojmy často spojují do jednoho, viz. anglický název ICT (Information and Communication Technologies). Termín ICT vznikl v polovině 80. let minulého století a je definován takto: „ICT jsou všechny druhy elektronických systémů používaných pro vysílání, telekomunikaci a počítačem zprostředkovanou komunikaci“ (Haddon, 2004). Jako příklady jsou uváděny počítače, videohry, telefony, internet, ale například i online platební metody. Kombinace tohoto pojmu a daných příkladů vyjadřuje, co může ICT zahrnovat bez toho, abychom museli určovat přesně dané hranice toho, co do ICT patří a co ne. Což je žádoucí vzhledem k tomu, že se tento obor stále vyvíjí (Haddon, 2004).

Nárůst zájmu o informační a komunikační technologie přišel v 90. letech minulého stolení. V této době se o ICT zajímalo mnoho komerčních, ale i akademických výzkumů. Předpokladem pro vznik výzkumů bylo hned několik faktorů. Hlavním z nich byl výskyt nových služeb a zařízení, která se začala na trhu objevovat (nejdůležitějšími byly internet a mobilní telefony) (Haddon, 2004). V komerční sféře si většina společností (zejména telekomunikačních společností) v oboru ICT uvědomila důležitost soukromého uživatele jako cíle jejich marketingu. Potřebovaly totiž znát lépe svůj trh, aby tak mohly být více konkurenceschopní (Haddon, 2004). V dnešní době si uvědomujeme důležitost ICT, což je vidět například na počtu studentů, kteří mají o tento obor zájem. Navíc se tento vědní obor stále rozvíjí a vznikají tak nové expertní oblasti, které je potřeba zkoumat.

4.1.2 Letecká přeprava

Letecká přeprava patří mezi jeden z nejmladších typů přepravy osob, ale i nákladu. Bez letecké přepravy si v současné době nedokážeme představit každodenní život. Letadla nevyužíváme jen při cestě na dovolenou. S leteckou dopravou přicházíme do styku takřka každý den, ačkoliv nepřímo. Například ovoce v supermarketu, které

se k nám dováží z exotických zemí, mohlo být přepravováno letadlem, či námi dlouho očekávaná zásilka ze zahraničí mohla být dopravována taktéž letecky.

Jak již naznačuje odstavec výše, letecká přeprava pro nás má hned několik významů. Tím prvním je význam hospodářský. Sem spadá hned několik důležitých oblastí. Nejdůležitějšími z nich jsou mezinárodní obchod a cestovní ruch. Mezi největší přednosti letecké přepravy v sektoru mezinárodního obchodu patří její rychlost. Třeba při přepravě trvanlivých potravin (například exotického ovoce) je jedinou možností letecká doprava. Pokud by se ovoce přepravovalo lodí nebo autem či vlakem, došlo by ke zkažení a tím pádem k znehodnocení zboží.

Dalším důležitým významem je význam společenský. Vzhledem k rozvoji letecké přepravy a konkurence mezi aeroliniemi jsou letenky stále dostupnější. To znamená, že lidé mohou cestovat po celém světě a poznávat nové kultury a tím se společensky obohacují. Letecké přepravy lze využít nejen na osobní úrovni, ale také například na úrovni politické. Pomocí letadla je možné, aby docházelo k návštěvám vysoce postavených politiků a tím k utužování mezistátních vztahů.

V neposlední řadě je potřeba zmínit důležitý ekonomický přínos letecké přepravy. A tím je vytváření nových pracovních pozic. Každé odvětví cestovního ruchu vytváří přímé a nepřímé pracovní nabídky. Mezi přímé pracovní pozice vyvolané leteckou přepravou řadíme například pozice přímo v aeroliniích či práce na letištích. Za nepřímé pracovní pozice považujeme různé firmy vyrábějící techniku, která je potřeba na letištích. Zde můžeme zahrnout vše od výrobců bezpečnostních rámů, přes zprostředkovatele informačních systémů na letištích až po výrobce součástek pro letadla. Posledními pozicemi jsou takzvané vyvolané pracovní pozice. Sem můžeme řadit různá ubytovací zařízení, hotely či restaurace.

4.2 Informační systémy využívané v moderní letecké přepravě

Za posledních pár desítek let se vývoj letecké přepravy posunul mílovými kroky vpřed. Doby, kdy museli cestující trávit svůj drahocenný čas ve frontách na odbavení zavazadel či u pasové kontroly, se pomalu blíží ke konci. To vše hlavně díky internetu a vývoji nových technologií, jako jsou například bezkontaktní technologie (platba pomocí NFC či rozpoznávání obličeje při pasové kontrole) nebo vývoje

zdokonalování mobilních aplikací sloužících k online odbavení cestujících (Haddon, 2004).

V dnešní uspěchané době je nejdůležitějším faktorem čas. To platí obzvlášť v letecké přepravě. Zde je potřeba v reálném čase předávat informace a reagovat na možné změny napříč kontinenty, což umožňuje internet a všechny informační systémy na něm závislé. Tyto systémy propojují různé softwarové aplikace, jež využívají společnosti participující v letecké přepravě. Bez databázových a komunikačních systémů by nebylo možné zajistit tak rozsáhlou nabídku v letecké přepravě, jako známe dnes. Před všemi automatizovanými systémy byli cestující závislí na informacích, které jim byly poskytovány pouze v podobě tištěných brožur či letáků. Takto připravené materiály byly bohužel příliš pracné na výrobu, časově i finančně náročné, ale hlavně byly tyto informace statické, tedy nebylo možné je často měnit, což je v tomto odvětví potřebné.

Odpovědí na tento problém měl být první informační systém zvaný CRS (Computer Reservation System), který byl představen jako experiment v roce 1960. Měl sloužit k evidenci prodaných sedadel v letadle. Vzápětí, v roce 1963, byl aerolinkami Spojených států amerických (American Airlines) představen první CRS zvaný SABRE (Semi-Automated Business Research Environment). CRS se tak stal primárním systémem k distribuci informací v letecké přepravě a měl velký vliv na konkurenční boj mezi aerolinkami. V roce 1976 ho začaly využívat cestovní kanceláře a následně se stal univerzálním pomocníkem v oblasti turismu.

Hlavním cílem CRS je vyřízení žádosti na jednom místě a eliminace fyzické a distanční vzdálenosti mezi zprostředkovatelem a zákazníkem. Tento systém má univerzální pokrytí a zahrnuje informace pro aerolinky, cestovní kanceláře, hotely a další. Termín CRS se dnes již tak často nepoužívá, stal se totiž částí komplexnějšího systému známého jako PSS (Passenger Service System), který obsahuje CRS a DCS (Departure Control System) (Pruša a kol., 2015)[1].

V současné době jsou informační technologie v letecké přepravě využívány hlavně k zvýšení efektivity celého odvětví a snižování nákladů. K tomu přispívá organizace

[1] Co je počítačový rezervační systém je dostupné zde https://colorwhistle.com/computer-reservation-system/

IATA (International Air Transport Association), jejímž cílem je například zlepšovat podmínky fungování v letecké přepravě pro své členy stejně tak ale pro širokou veřejnost. Další vizí je trvale přispívat k rozvoji letecké dopravy a zároveň vytvářet úspory v odvětví. Proto organizace přišla v roce 2004 s programem zvaným Simlyfying the Business. Projekt od svého vzniku zaznamenal již několik fází, ve kterých se snaží implementovat nová řešení za pomoci nejmodernějších informačních a komunikačních technologií tak, aby přinesla užitek jak přepravcům, tak i cestujícím. Podle prvotních plánů se mělo každoročně ušetřit 6,5 miliard dolarů za předpokladu, že budou realizovány čtyři hlavní cíle projektu. Jedním z cílů byl přechod na elektronické letenky (tento cíl se podařilo splnit již v roce 2008, tedy za pouhé 4 roky), s tímto bodem souvisel i druhý bod, který měl na starosti zavedení čárových kódů pro identifikaci letenek, což umožňuje cestujícím tisknout si letenky doma či ponechat letenku v čistě elektronické verzi (např. v mobilním telefonu). Třetím bodem bylo zavedení samoobslužného odbavení cestujících. Posledním bodem bylo učinit proces zacházení se zavazadly účinnějším tak, aby se předešlo jejich poškození či dokonce ztracení, což je pro aerolinky velice nákladné a pro samotné cestující je to velkou komplikací při cestování (Barkat, 2015).

Organizace IATA vydává v závislosti na projektu Simlyfying the Business pravidelně od roku 2011 každoroční přehled cílů a témat, jakým způsobem se letecká přeprava posouvá kupředu. Tyto oficiální roční zprávy se nazývají White Papers a zahrnují tři hlavní oblasti. První z nich je poskytování pravdivých informací cestujícím, druhou je zefektivnění zavedených procesů při cestování a poslední je podpora a umožnění maloobchodního prodeje. Například čtyři hlavní body pro rok 2018 byly:

- **Project DNA** – Krátkodobou vizí tohoto bodu je, aby se IATA stala digitální certifikační autoritou tak, aby všichni business partneři mohli být důkladně identifikováni. Dlouhodobým cílem je toto řešení rozšířit mezi více a více partnerů, až k samotným zákazníkům.
- **Project Honeymoon** – Záměrem je znovu definovat pojetí takzvaného codesharingu a rozvinout komerční dohody mezi dopravci.
- **Project Husky** – Vizí tohoto projektu je vybudovat digitální cestovní ekosystém orientovaný na zákazníka, který by propojoval aerolinky,

cestovní kanceláře, hotely a nesčetné množství dalších cestovních maloobchodů.

- **Project Panini** – Cílem tohoto projektu je dramaticky zjednodušit proces distribuce a používání voucherů (například jídelních voucherů) tím, že by bylo pasažérům umožněno platit za tyto služby pomocí letenky. To by cestujícím usnadnilo, a hlavně zpříjemnilo, jejich už tak stresující pobyt na letišti[2].

Ačkoliv je zde uvedeno, že informační a komunikační technologie mají kladný dopad na leteckou dopravu (snižování režijních nákladů a zvýšení efektivity práce), je důležité zmínit, že tyto modernizační kroky jsou spojeny s nemalými počátečními náklady (vývoj či případné zakoupení softwarových licencí, nákup nového hardwarového příslušenství a v neposlední řadě zaškolení zaměstnanců k práci s novým vybavením).

4.2.1 Informační technologie využívané v leteckých společnostech

Jak již bylo několikrát zmíněno, informační a komunikační technologie hrají v letecké přepravě nemalou roli a jsou považovány za nezbytnou součást přepravního procesu. Každá přepravní společnost je nucena evidovat přehled nabízených letů. S rostoucím zájmem o cestování letadlem je také zapotřebí mít co nejpřesnější a nejaktuálnější informace o stavu volných míst na palubě letů, které společnost nabízí k prodeji. V začátcích letecké přepravy osob byly informace o letech a volných místech na palubě zprostředkovávány zákazníkům v podobě papírových brožur a letáků, samotná evidence na straně aerolinek byla vedena také v papírové formě. To bohužel často vedlo k chybám zapříčiněným lidským faktorem (nezaevidování místa, nabídnutí jedné sedačky více zákazníkům…). Proto s rozvojem nové technologie přešly letecké společnosti k využívání různých inventárních systémů, které fungují dodnes. Tyto systémy umožňují udržovat potřebné informace aktuální. Díky této evidenci je také možné zprostředkovávat prodej letenek cestujícím. Došlo k výraznému snížení v chybovosti oproti papírové

[2] Přehled cílů a témat organizace IATA je dostupný zde https://www.iata.org/contentassets/8dbfa2bc1aca46c9aabad704ec905598/air-tt-white-paper.pdf

evidenci a také je možné uchovávat daleko detailnější informace. Inventární systémy jsou schopné uchovávat také informace o všech letových řádech dané společnosti, což dovoluje spravovat rezervace na konkrétních linkách. Rezervace obsahují informace o obsazenosti sedadel na palubě letadla, ale i o všech pasažérech v letadle. Uchovávají se informace jako je jméno a příjmení cestujícího, třída, kterou si zaplatil, datum a čas odletu či další zvláštní požadavky. Nutností je, aby tyto systémy byly provázány s dalšími systémy využívané leteckou společností (rezervační, odbavovací nebo prodejní systém) (Prusa, 2015).

V oblasti obchodně-provozních činností aerolinek mají informační systémy hned několik využití. Prvním a nejdůležitějším využitím je automatizace obchodně-provozních aktivit, což dovoluje používané postupy zefektivnit. Příkladem jsou systémy pro rozvoj a plánování sítě linek, jejichž cílem je optimalizovat letové řády aerolinek. Úkolem těchto systémů je na základě přístupných informací (nákladovost jednotlivých tras, předpokládaná poptávka, konkurenční nabídka) sestavit síť linek, kterou bude letecká společnost nabízet. Data, dle kterých jsou výpočty prováděny se shromažďují z různých statistik (BSP statistiky, které jsou založeny na počtu prodaných letenek na jednotlivých trzích nebo Official Airline Guide, kde jsou evidovány aktuální letové řády většiny aerolinek)[3].

Mezi další informační technologie používané v leteckých společnostech můžeme zařadit systémy pro plánování letadel a posádek. Ty jsou nápomocné při plánování obsazení letů palubním personálem. Také však obsahují nástroj pro řešení neplánovaných situací (zrušení či zpoždění letu atd.). Cílem je minimalizovat škody, které by mohly být způsobeny při odchýlení od standardních letových řádů. K tomuto systému je zapotřebí dostatečně rozsáhlé databáze s informacemi o palubním personálu. V databázi je nutné evidovat údaje jako jsou nalétané hodiny, kvalifikace personálu či záznamy o směnách, které personál absolvoval, aby nedošlo k přetížení personálu, který by vlivem únavy mohl chybovat, což by, hlavně u pilotů, mělo fatální následky. Kromě plánování letadel a posádky jsou tyto systémy

[3] Informace o evidenci OAG jsou dostupné na https://www.oag.com/about-oag

využívány k výpočtům letových plánů, kde je potřeba zohlednit například aktuální informace o stavu počasí a další informace z letištních systémů.

Dalšími využívanými systémy jsou revenue integrity systémy, které jsou úzce spojeny s již zmíněnými inventárními systémy. Revenue integrity systémy se snaží o co nejvyšší obsazenost jednotlivých letů. Dělají to takovým způsobem, že procházejí již vzniklé rezervace a dle přednastavených parametrů vyřazují takové rezervace, které jsou považovány za pravděpodobně neuskutečnitelné. Parametry pro vyřazení rezervace mohou být například fiktivní jméno, či vícekrát opakující se identická rezervace atd. Tyto systémy jsou napojené také na rezervační systémy, kde kontrolují, zda došlo ke správnému spárování letenky s rezervací a její následnému vystavení.

4.2.2 Globální distribuční systémy

Jak je uvedeno výše, na zavedení informačních a komunikačních technologií do leteckého průmyslu měly největší podíl letecké společnosti, které pomocí globálních distribučních systémů mohly poskytovat přístup do rezervačních systémů větší množině prodejců. V dnešní době se však situace otočila o 180 stupňů. V podstatě ani jeden ze čtyř hlavních globálních systémů není vlastněn aerolinkami. Kromě zmíněných čtyřech hlavních systémů bylo vyvinuto i několik menších, ty jsou však užívány pouze regionálně.

Jak již bylo zmíněno výše, prvním globálním distribučním systémem byl systém SABRE. Ten si svoje postavení na špičce zachoval až dodnes, kdy je ze všech systému nejrozšířenější. Semi Automated Business Research Environment neboli SABRE vznikl vlastně náhodou, když se v roce 1953 na pravidelném letu z Los Angeles do New Yorku potkal tehdejší prezident American Airlines C.R. Smith s obchodním zástupcem firmy IBM, R.B. Smithem. Výsledkem jejich konverzace o leteckém průmyslu byla myšlenka vytvoření systému schopného vytvářet a evidovat rezervace letenek a zároveň tato data v reálném čase distribuovat prodejcům po celém světě. Vývoj systému SABRE vyšel na 40 milionů dolarů. V prvním roce využívání systému se do něj zapojilo 130 cestovních kanceláří, kdy na konci osmdesátých let, tedy necelých 20 let od spuštění, bylo do systému zapojeno již 130 000 terminálů rozmístěných po celém světě. V dnešní době je do systému

zapojeno více než 400 aerolinek, kdy většina zastoupení je na území Spojených států amerických. Jak bylo zmíněno, tak dnes již není žádný globální distribuční systém vlastněn aerolinkami, stejně tomu je i u SABRE, kdy v roce 2000 došlo k odloučení od American Airlines[4].

Dalším systémem byl Galileo, který vznikl v roce 1971. Galileo však začal být systém nazýván až od roku 1993. Původně totiž vycházel ze systému Apollo, což byl centrální rezervační systém, který byl využíván americkou leteckou společností United Airlines. Časem se systém rozšířil mezi více aerolinek (KLM, Swissair, British Airways a další). V roce 2006 došlo k odkoupení systému společností Travelport. Na rozdíl od systému SABRE má Galileo od roku 1999 své zastoupení i v ČR (Průša a kol., 2015). Galileo má podobné zastoupení jako systém SABRE, a to ve více než 400 cestovních kancelářích[5].

Roku 1987 byl založen skupinou aerolinek (Lufthansa, Iberia, SAS a Air France) globální distribuční systém Amadeus. Primárně tento systém působí v Evropě a Asii, ale má své zastoupení i v Africe či Spojených státech amerických. Zastoupen je mezi více než 700 leteckými dopravci a působí ve 195 zemích světa. Stejně jako u ostatních zmíněných systémů přešlo vlastnictví do soukromého sektoru[6].

Posledním ze čtyřech hlavních globálních distribučních systémů je Worldspan. Ten vznikl na počátku devadesátých let minulého století, kdy se stejně jako systém Galileo stal součástí skupiny Travelport. Oproti Galileu, který je zastoupen i v České republice, je Worldspan primárně zastoupen v Spojených státech amerických a v ČR není zastoupen vůbec.

Je zcela zřejmé, že trh s globálními distribučními systémy není otevřen pro nově příchozí. Ale jak již bylo zmíněno, existují i regionální distribuční systémy, které mají velký význam především v regionální dopravě. Nejvíce jsou tyto systémy využívány v asijských zemích. Příkladem regionálních distribučních systémů je například AXESS International Network, který je vlastněn Japan Airlines společně se

---

[4] Informace o historii systému SABRE zde https://www.sabre.com/files/Sabre-History.pdfv

[5] Informace o historii systému Travelport zde https://www.companieshistory.com/travelport/

[6] Informace o systému Amadeus dostupné na http://www.amadeus.com/msite/global-report/2014/en/pdf/amadeus-global-report-2014.pdf

společností Travelport a je zaměřen na dopravu na území Japonska. V Číně byl do roku 2012 jediným vládou povoleným globálním distribučním systémem Travelsky. Od roku 2012 Čína povolila vstup na domácí trh i zahraničním poskytovatelům (Zelenka a kol., 2008).

Pro letecké společnosti je výhodné podporovat co nejvíce globálních distribučních systémů, protože každý systém je spjat s jinými cestovními kancelářemi, které jsou schopné zprostředkovat nabídku aerolinek. Tedy na čím více distribučních kanálů budou aerolinky napojeny, tím bude jejich dosah na nabídku vyšší a zvýší se jim šance k prodeji letenek.

Globální distribuční systémy jsou využívané kromě cestovních kanceláří také turistickými portály. Tyto portály poskytují uživatelům náhled do distribučních systémů a možnost koupit letenky přímo od aerolinek, tedy bez prostředníka v podobě cestovní kanceláře. (Zelenka a kol., 2008). V posledních letech je tato možnost nákupu velmi oblíbena hlavně kvůli možným nízkým cenám. Například pokud aerolinka ví, že na let, který má naplánovaný odlet za dvacet hodin nebude naplněna kapacita letadla, poskytne zbývající sedadla za sníženou cenu, aby tak naplnila letadlo co nejvíce a přišla o co nejméně nákladů. Příkladem portálů, které tyto služby nabízí je booking.com, skyscanner.cz, letuska.cz nebo kayak.com.

4.2.3 Informační systémy využívané na letištích

4.2.3.1 AMS (Asset Management System) – systém pro správu aktiv

AMS zahrnuje softwarové aplikace používané k plánování a správě letištních aktiv a prostředků. Letiště je komplexní dynamický systém neustále reagující na interní i externí podněty. To vyžaduje nepřetržitou správu letištních aktiv a prostředků 24 hodin denně, 365 dní v roce. Aby mohli správci letištního provozu splnit tyto náročné podmínky, jsou závislí na automatizovaných systémech, kterými lze dané podněty sledovat a spravovat. Tyto systémy také poskytují nástroje, které umožňují sledovat životní cyklus prostředků. To je velmi důležitá funkce při snaze o dosažení vysoké úrovně provozní efektivity (Marks, 2015).

Letištní aktiva jsou velmi různorodá díky jejich vlastnostem, úkolům a rolím, které mají plnit v rámci organizace letištního provozu. AMS systémy umožňují letištnímu

operátorovi vytvářet plán správy aktiv, popisující dlouhodobou strategii pro nejlepší využití každého z nich (Marks, 2015).

Náročná práce musí být naplánována, sledována, dokumentována a evidována. AMS tyto postupy usnadňuje tak, že umožňuje zaměstnancům letištního provozu naplánovat a sledovat autorizovanou práci a projekty podle jednotlivých aktivit údržby, místa, kde je práce vykonávána a přiřazené obsluhy. Systém je rovněž schopen vyúčtovat činnosti dodavatelů a celkové náklady spojené s každou funkcí nebo činností (Marks, 2015).

Komerčně dostupné AMS jsou například od společnosti AAAE (American Association of Airport Executive) systém Spatial Airport Asset Management Systém, Maximo Systém od společnosti IBM nebo AxisFM Facilities Asset Management software. Tyto typy komerčně dostupných systémů pomáhají přesně řešit problémy při plánování rozpočtu či budoucím přizpůsobení letiště pro obsluhu větších letadel a podobně složitá strategická rozhodnutí (Marks, 2015).

Nástroje softwaru pro správu aktiv jsou používány k hledání způsobů, jak snížit náklady na provoz, úsporu energií a jak používat vybavení a zdroje efektivněji. Jejich využívání je klíčem k úspěchu ve všech dynamických obchodních organizacích, obzvlášť na letištích. Zlepšení v plánování rozpočtu a rozhodování vede ke snížení nákladů na provoz, údržbu a prodloužení životnosti používaných zařízení (Marks, 2015).

Primárními uživateli AMS jsou správci letištních zařízení a personál údržby a provozu, který plánuje používání aktiv a servisních úloh. Dalšími uživateli jsou pracovníci letištního provozu a účetnictví, kteří využívají systém ke generování denních reportů sloužících k fakturaci hotových úkolů a využívaných zdrojů. Sekundárními uživateli jsou nájemci letištních prostor, například letecké společnosti, ale stejně tak i návštěvníci letiště a cestující, kteří využívají zdrojů letiště a leteckých společností (Marks, 2015).

Správa informačního spojení s rozhraním pro AMS zahrnuje počítačové systémy používané ke správě letištních zdrojů. Tento software může sestávat z nezávislých aplikací s přímým připojením nebo ze softwarových modulů, které jsou integrovány v letištních aplikacích. Mezi klíčové funkce patří přidávání nových aktiv a sledování jejich stavu, hodnot nebo podobných aktivit či využívaných zdrojů (Marks, 2015).

Hardwarem používaným pro AMS jsou servery, kde jsou uloženy aplikace a jednotlivá zařízení, ze kterých lze přistupovat k softwaru. Mezi další vybavení mohou patřit skenery a čtečky čárových kódů pro sledování aktiv, RFID tagy a další zařízení sloužící k evidenci a sledování letištního inventáře (Marks, 2015).

AMS může běžet na stávající letištní síti nebo může být spuštěn na síti prodejce softwaru, se kterým má letiště smlouvu o údržbě a provozu systému. V druhém zmíněném případě zajišťuje provozovatel připojení systému k letištní síti nebo poskytne zařízení, ze kterého se lze do systému připojit a zde následně monitorovat a upravovat aktiva v inventáři (Marks, 2015).

Systém správy aktiv může být spojený s ERP (ERP, česky plánování podnikových zdrojů, je systém, kterým společnost pomocí počítače řídí a integruje většinu oblastí své činnosti), kde buď oba sdílí společnou databázi nebo má každý systém přidělen svoji unikátní databázi. Data uložená v databázi zahrnují informace o majetku, personálu, vybavení, zařízení, systémech, veřejných službách a financích na letišti. Data zadávaná do AMS slouží k plánování, předpovědím a rozpočtování (Marks, 2015).

4.2.3.2 BMS (Building Management Systems) – systém pro správu budov

Systém správy budov zahrnuje interoperabilní inteligentní systémy, zařízení a body, které monitorují a kontrolují letištní elektromechanické systémy pro automatické dveře, osvětlení prostor, napájení, detektory kouře, požáru a podmínek v prostředí letiště. BMS je spojeno s mechanickými systémy, které monitorují a kontrolují provozní stav a výkon určitých letištních systémů, jako je například EMS (Electrical Monitoring System) nebo další systém se stejnou zkratkou EMS (Environmental Management Systém) (například senzory pro měření oxidu uhličitého) a systém HVAC (heating, ventilation, air cooling/conditioning – systémy pro regulaci teploty, ventilace, klimatizace/odvětrávání). Každý komponent systému je naprogramován tak, aby automaticky ovládal vytápěcí jednotky, otevíral a zavíral ventilace a reguloval ventilátory v nich. Tyto úkony slouží k udržování přednastavené teploty a prodění vzduchu uvnitř budov. Systém také manipuluje s osvětlením, s ohledem na naprogramované plány využití jednotlivých částí budov, vypíná a zapíná osvětlení v daných sektorech (Marks, 2015).

BMS využívá PLC (Programmable Logic Controllers – programovatelné logické automaty) nakonfigurované pro každý monitorovaný systém zvlášť. Automaty jsou počítačové jednotky, které mají vstupní a výstupní funkce. Zařízení PLC jsou instalována mezi hostitelským systémem BMS a systémy, které mají být monitorovány. Input/output funkce umožňují logickým automatům přijímat instrukce od hostitelského počítače BMS a posílat je do monitorovaných systémů a naopak. Tyto informace jsou posílány na základě předem daných podmínek nebo změn stavů sledovaných systémů (Marks, 2015).

Systém správy budov poskytuje klíčovým uživatelům informace o provozním stavu, informuje je o aktuálním výkonu a varuje před výpadky systému. Po přihlášení do systému je uživatel schopen pomocí GUI (Graphical User Interface – rozhraní umožňující ovládat počítač za pomoci ovládacích prvků) upravit nastavení osvětlení, HVAC nebo ventilačních systémů. Uživatelé jsou také schopni monitorovat tyto systémy pomocí řídícího panelu, který ukazuje stav a výkon systému v reálném čase. BMS může být propojen s VTMS (Vertical Transportation Monitoring Systém) (například eskalátory a výtahy) pro monitorování výkonu, detekci výpadků a dalších monitorovacích funkcí. Kromě toho lze systém správy budov připojit k systémům omezeného přístupu, CCTV (kamerového systému) a systému požárního poplachu. Některé z těchto systémů také umožňují provozovatelům letišť zadávat příkazy pro opravy či servisní volání, a tím snižovat požadavky na pracovní sílu pomocí automatizace pracovních postupů (Marks, 2015).

Primárními uživateli BMS jsou zaměstnanci údržby letišť a smluvní servisní technici. Tito pracovníci zajišťují, aby systémy fungovaly efektivně na základě přednastavených parametrů. Systémy pro správu budov řídí letištní zařízení, která poskytují bezpečné a pohodlné prostředí pro každého uvnitř budov letiště. Dalo by se tedy říct, že mezi sekundární uživatele systému patři všichni zaměstnanci, cestující a návštěvníci letiště (Marks, 2015).

Připojení systému BMS vyžaduje softwarové aplikace, které integrují řadu zařízení pro kontrolu a monitorovací systémy. Softwarové aplikace jako COGZ nebo Manager Plus umožňují uživatelům pracovat v rámci různých funkcí nebo modulů aplikace. Moduly mohou být vyhrazeny pro pracovní aktivity, požadavky, aktiva, správu inventáře, nákup nebo další funkce, v závislosti na potřebách systému a jeho

konkrétní konfiguraci. Aplikace může běžet na letištním centrálním serveru nebo může mít podobu webové aplikace, která je spravována na straně zprostředkovatele. Ten následně poskytuje přístup k aplikaci klíčovým uživatelům (Marks, 2015).

Hardware potřebný pro podporu BMS zahrnuje nakonfigurované počítače, řídící moduly, monitory stavu a systémové servery. BMS může být nastaven tak, aby používal buď připojení přes LAN síť poskytovanou letištěm nebo přes síť LAN poskytovanou provozovatelem daných zařízení, který má s letištěm smlouvu na správu BMS. Systém obsahuje databázi, například SQL Server, kde se ukládají informace o majetku, konfiguraci programů nebo rozpisů prací. BMS přijímá data ze sledovaných systémů a odesílá jim nazpět instrukce na základě přednastavených pokynů nebo změn ve stavu systému. Systém pro správu budov může být také propojen s AMS kvůli přidělování letištních zdrojů a vybavení pro systémy, které vyžadují údržbu nebo opravy (Marks, 2015).

4.2.3.3 EMS (Environmental Management System) – systém monitorování prostředí

EMS je interoperabilní se systémem BMS, zahrnuje síť spojující senzory a monitorovací a kontrolní systémy, které zaznamenávají a poskytují informace o podmínkách prostředí letiště (Marks, 2015).

Letiště představují velkou hrozbu v ohledu na životní prostředí. Fungují totiž jako malá soběstačná města. Produkují ekologický odpad a znečišťují ovzduší, což může ovlivnit veřejné zdraví nebo bezpečí v okolí letiště. Letiště, která dostávají finanční příspěvky od států, na snížení těchto nežádoucích produktů, jsou povinná implementovat programy pro snížení hluku a přemístit neletištní nemovitosti, které jsou nevyhnutelně vystaveny nebezpečným hladinám hluku (Marks, 2015).

Mnoho letišť má programy a specializované týmy, které mají za úkol starat se o snižování hluku a dodržování všech předpisů v oblasti životního prostředí. Tyto týmy dohlížejí na kvalitu ovzduší, sanaci podzemních vod, požadavky NEPA (National Environmental Protection Agency – Národní agentura pro ochranu životního prostředí) a na požadavky ohledně hlukových hladin. Dále se zabývají environmentálními restrikcemi nebo dokumenty a stížnostmi ohledně hluku

letadel, a také slouží jako zastánci programů pro podporu životního prostředí jako je například recyklace materiálů a šetření vody (Marks, 2015).

V rámci programu snižování hluku je v okolí letiště nainstalována síť mikrofonů. Mikrofony zaznamenávají okolní zvuky v decibelech a následně určují, zda jsou zvukové emise, které přichází z letecké dopravy, v přijatelných limitech pro obyvatele v okolí letiště. Správci používají aplikace k analýze dat shromážděných z terénních zařízení, která jsou umístěna v různých environmentálních systémech. Počítačový software jako Brüel & Kjær ANOMS (Airport Noise and Operations Management System) dokáže identifikovat a sledovat ohniska hluku, jejich vzorce a detekovat tak oblasti s nepřijatelnými hladinami hluku. Lze také provádět počítačové simulace, které mohou určit hlukové hladiny na základě provozu letadel, směru větru, vzdálenosti od vzletové dráhy či pojezdové dráhy, zařízení pro údržbu nebo budov terminálu. Výstupy ze simulací pomáhají správcům letišť určit potenciální potřebu odkoupit přilehlé pozemky, v rámci programu pro snižování hluku na letištích. Klíčoví uživatelé EMS jsou inženýři pro životní prostředí na letišti, úředníci dohlížející na snižování hluku, odhadce letištního majetku a realitní makléř, zaměstnanci letiště a zaměstnanci FAA (Federal Aviation Administration). Nepřímými uživateli jsou lidé, kteří bydlí v okolí letiště, zejména ti, kteří mají svůj pozemek v přímých letových drahách vzletů a přistání. Aplikace vyvinuté různými výrobci zařízení pro monitorování dodržování předpisů v oblasti životního prostředí zahrnují jak běžně dostupné komerční systémy, tak i aplikace přizpůsobené potřebám konkrétního letiště. Některé z těchto programů umožňují letišti provozovat v rámci jednoho softwaru více aplikací pro správu prostředí, zatím co další programy se zaměřují pouze na jeden problém životního prostředí, například na kvalitu ovzduší. Například ADMS (Adaptive Data Modular Systems) měří kvalitu ovzduší a úrovně emisí v okolí letiště a sbírá data z různých zdrojů znečištění vzduchu, jako jsou letadla, pozemní vozidla nebo průmysl obklopující letiště (Marks, 2015).

Hardwarové komponenty pro EMS zahrnují zařízení pro monitorování dat v terénu, která měří hluk, emise, hladiny určitých chemikálií pocházejících z letištního provozu a dalších průmyslových odvětví v okolí letiště. Data zaznamenána těmito

zařízeními jsou nahrána na servery, odtud jsou následně dostupná pomocí softwaru pro správu životního prostředí na letišti (Marks, 2015).

Data ze zařízení v terénu jsou přenášena pomocí přenosných nebo bezdrátových připojení do hostitelského počítače. Některá zařízení mohou komunikovat bezdrátově s prodejci SaaS (Software as a Service – software jako servis je typ nasazení softwaru, kdy aplikaci hostuje provozovatel služby), namísto s hostitelským počítačem přímo na letišti. V takovém případě dodavatel poskytuje aplikaci přes webové připojení, ke kterému má přístup přes ISP (Internet service provider) letiště. V databázi je tady shromážděno vše ohledně monitorovacích zařízení nasazených v terénu, místech mapování, státních standardech, známých zdrojích znečištění a uživatelích systému (Marks, 2015).

4.3 Útoky na letiště

4.3.1 Útoky v minulosti

V této části následuje výčet kybernetických útoků a jejich následků, které byly zaznamenány v reportu organizace ENISA (European Union Agency for Cybersecurity), který byl zaměřen na zabezpečení moderních tzv. chytrých letišť.

V srpnu 2016 zůstaly tisíce pasažérů po celém světě uvězněni na letištích. Důvodem bylo přerušení dodávky elektřiny, které se stalo ve městě Atlanta, poblíž sídla aerolinek Delta. Následkem byl výpadek počítačového systému aerolinií a bylo nutné přerušit veškeré lety společnosti. Selháním systému byly ovlivněny všechny důležité systémy aerolinek jako například systémy pro check-in, informační panely s pokyny pro cestující, webové stránky aerolinek a také aplikace pro mobilní telefony[7].

V červenci 2016 se podařilo útočníkům úspěšně napadnout dvě největší vietnamská letiště a největšího národního dopravce Vietnam Airlines. Hackeři se rychle zmocnili tabulí s informacemi o jednotlivých letech a také zvukových systémů uvnitř obou letišť. Místo informací o odletech a příletech vysílaly informační tabule a letištní

[7] Článek o kybernetickém útoku provedeném na Delta Airlines dostupný zde https://www.bbc.com/news/world-us-canada-37007908

rozhlas, podle místních médií, anti-vietnamské a filipínské slogany. Na toto bylo reagováno okamžitým vypnutím obou systémů. Mezitím se útočníci zmocnili webových stránek aerolinií Vietnam Airlines, které byly přesměrovány na škodlivý web se zahraniční doménou. V pozadí se však hackeři zmocnili dat o uživatelích, kteří s aeroliniemi v poslední době cestovali, a všechna data publikovali online[8]. V důsledku tohoto útoku provedly vietnamské úřady komplexní kontrolu čínských zařízení a technologií se záměrem zajistit bezpečnost informací na vietnamských letištích. Existovala totiž obava, že za útokem stála skupina čínských hackerů známa jako 1937 cn[9].

Také v červenci roku 2016 na jednom z italských letišť Fiumicino došlo chybou třetí strany k výpadku automatického systému sloužícímu k check-inu pasažérů. Tento výpadek způsobil dvouhodinové zpoždění v procesu odbavování pasažérů. Chyba byla spojena s výpadkem u providera poskytujícího internetové připojení pro systém automatického odbavení cestujících[10].

Po přistání 17. dubna 2016 nahlásil pilot British Airways, při letu z Ženevy, kolizi s dronem při přiblížení k londýnskému letišti Heathrow. Tento incident poukázal na problém s ohledem na používání dronů v blízkosti letiště. Zatímco kolize s ptáky byly již podrobně prozkoumány, tak doposud nebyla skoro žádná data zaznamenávající střety a následné škody při kolizi letadla s dronem[11].

Výrobce civilních letadel Airbus Group je zasažen kybernetickými útoky v průměru 12krát za rok. Převážná většina útoků je ve formě ransomware (ransomware, tzv. vyděračský program, je typ škodlivého programu, který zablokuje přístup k počítačovému systému, či zašifruje data na disku, následně od obětí vyžaduje výkupné za obnovení přístupu k datům) nebo jsou to nepřátelské útoky prováděné

---

[8] Článek o útocích na vietnamská letiště https://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/

[9] Článek o krocích provedených vietnamskými úřady po útocích na letiště https://tuoitrenews.vn/news/society/20160804/vietnam-to-inspect-use-of-chinese-technology-following-cyberattacks-on-airports/6052.html

[10] Původní článek o útocích provedených na římské letiště https://roma.repubblica.it/cronaca/2016/07/18/news/fiumicino_problema_tecnico_al_t3_code_per_i_controlli_arrivano_in_strada-144357812/?ref=HREC1-6

[11] Článek o střetu letadla British Airways s dronem https://www.bbc.com/news/uk-36067591

státem sponzorovanými útočníky. Šéf bezpečnosti Airbusu uvedl příklad, jak se ransomware může dostat do vnitřního informačního systému společnosti. Útočníci neatakují systémy zvenčí, což by bylo velice obtížné, ale zevnitř. Docílí toho tak, že kompromitují počítač, který zaměstnanec používá i mimo práci, nahrají mu do něj ransomware a ten se potom, co se zaměstnanec připojí právě z tohoto počítače do firemního intranetu, rozšíří do celé korporátní sítě Airbusu, kde zašifruje data uložená na serverech, či osobních počítačích[12].

4.3.2 Útoky v posledních letech

Kybernetické útoky jsou v posledních letech zaměřovány převážně na aerolinky. Hlavním důvodem útoku na letecké společnosti je jejich závislost na počítačové síti při aktivitách jako například bookování letenek, telefonická podpora, ale i rozsáhlé back-office (back-office je část společnosti, která se většinou skládá z administrativních pracovníků, kteří nejednají přímo se zákazníkem, jsou zde zahrnuty funkce jako správa záznamů, dodržování předpisů, účetnictví atd.) funkce, které běžně ovlivňují vícero subjektů zapojených do leteckého businessu[13].

Ústředí britské low-cost aerolinky EasyJet na londýnském letišti Luton bylo zasaženo kybernetickým útokem, který měl za příčinu únik osobních záznamů pasažérů. V květnu roku 2020 byl čínský hacker podezřelý ze zcizení emailových adres a detailů o cestě u skoro devíti milionů zákazníků EasyJet. K odcizení dat mělo dojít v lednu. Skupina hackerů, do které patřil i podezřelý útočník, se v minulosti zaměřovala na cestovní záznamy a další data, pomocí kterých sledovala pohyb vytypovaných jednotlivců se záměrem získat detaily o jejich kreditních kartách. Toto nebyl ovšem první útok provedený na aerolinky EasyJet. Letecká společnost čelila kybernetickým útokům i v minulosti. V srpnu roku 2018 se pokoušela škodlivá webová stránka zmást uživatele některých aerolinek, včetně EasyJet, aby vyplnili své osobní údaje, šlo tedy o tzv. phishing (phishing je technika používána hackery

---

[12] Článek o kybernetických útocích prováděných na společnost Airbus dostupný zde https://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131

[13] Článek o útocích prováděných v posledních letech, které jsou cíleny převážně na aerolinie, dostupný zde https://cyware.com/news/recent-attacks-on-airlines-suggests-hackers-are-now-more-interested-in-passenger-data-dfcecd34

k získávání citlivých údajů, důvěru veřejnosti si získávají vystupováním pod veřejně známými sociálními sítěmi, platebními portály, úřady státní správy atd.)[14]. Rovněž v srpnu roku 2017 došlo k podobnému útoku, kde hackeři na Facebooku vytvořili falešný profil aerolinky EasyJet a následně zde lákali na smyšlenou soutěž o letenky zdarma, jedinou podmínkou bylo vyplnění osobních dat v krátkém dotazníku[15].
Kybernetické útoky jsou celosvětový problém, který trápí aerolinky, letiště, výrobce letadel a další společnosti v tomto odvětví. Podle SITA (Société Internationale de Télécommunications Aéronautiques), se pouze 35 % aerolinek a 30 % letišť považuje za připravené v ohledu hrozby kybernetických útoků. Některé útoky, které proběhly v loňském roce:

- V únoru 2020 holandská low-cost aerolinka Transavia utrpěla kybernetický útok, který měl za následek únik dat u skoro osmdesáti tisíc pasažérů[16].
- V lednu roku 2020 bylo indické letecké společnosti SpiceJet odcizeno skoro 1,2 milionu osobních informací o pasažérech. Útočník se k citlivým datům dostal tak, že prolomil heslo do systému pomocí brute-force útoku (brute-force útok je pokus o rozluštění hesla bez znalosti dešifrovacího klíče, jedná se tedy o testování všech možných kombinací hesla).
- Také v lednu roku 2020 došlo k úniku důvěrných dokumentů o sloučení dvou aerolinií Malaysia Airlines a AirAsia Group Bhd[17].

4.4 Zabezpečení proti možným hackerským útokům

Navzdory všem snahám o vylepšení bezpečnosti na letištích, je letecký sektor stále problémem, který je třeba neustále řešit. Prvním útokem, ačkoliv ne hackerským,

---

[14] Článek o kybernetických útocích cílených a aerolinie EasyJet dostupný na https://www.infosecurity-magazine.com/news/mobile-phishing-campaign-offered/
[15] Článek o falešných facebookových profilech společnosti EasyJet dostupný na https://www.glasgowlive.co.uk/news/glasgow-news/easyjet-warn-customers-over-scam-13510021
[16] Článek o úniku dat u skoro 80 000 pasažérů společnosti Transavia dostupný zde https://simpleflying.com/transavia-data-breach/
[17] Článek o útocích prováděných v posledních letech, které jsou cíleny převážně na aerolinie, dostupný zde https://cyware.com/news/recent-attacks-on-airlines-suggests-hackers-are-now-more-interested-in-passenger-data-dfcecd34

byl teroristický útok 11. září 2001. Tato událost odstartovala teroristickou aktivitu, v oblasti leteckého průmyslu, po celém světě. Například exploze v roce 2006, sebevražedné útoky (2009 a podobné pokusy se objevují i nadále), pokusy o zničení letadla za pomoci improvizovaných výbušných zařízení a mnoho dalších událostí. Tyto útoky ukázaly, že stejně jako se vyvíjí metody prevence teroristických útoků, tak se vyvíjí i techniky útočníků, kteří se adaptují na nejnovější trendy bezpečnostních opatření implementovaných mezinárodními autoritami zodpovědných za bezpečnost v letectví (Suciu, 2018).

Systémy používané na letištích jsou výsledkem velkého počtu výzkumů, které mají za úkol předcházen potenciálním teroristickým aktivitám. Hlavním úkolem těchto systémů je monitorovat osoby uvnitř areálu letiště za pomoci analýz založených na chování, výrazu obličeje a psychologických profilech.

Názory na prevenci proti terorismu za pomoci analýzy chování se liší. Mnoho výzkumných pracovníků věří, že praktiky určené k detekci podezřelého chování mají potenciál pomoci procesu zadržení teroristů a přináší tak větší bezpečnost. Ostatní poukazují na problémy, které mohou nastat ve spojitosti s implementací těchto nových bezpečnostních mechanismů. Tyto systémy pro detekci osob se mohou stát nebezpečným nástrojem v rukou kybernetických útočníků (Suciu, 2018).

Po mnoha výzkumech v oblasti kybernetické bezpečnosti a jejího vlivu na kritickou infrastrukturu, bylo zjištěno, že mnoho vyspělých zemí věří, že bezpečnost letecké přepravy je hlavním problémem následujících let. S časem byl zaznamenán i rozvoj ICT v civilním letectví, přesněji v oblasti výstavby a rozvoje letecké přepravy. To znamená převážně rozvoj v implementaci komunikačních metod a navigačního vybavení. Bohužel, v návaznosti na tyto výhody, se vyskytly také problémy s kybernetickou bezpečností (Suciu, 2018).

4.4.1 Související práce v oblasti kybernetické bezpečnosti

Tato část bude zaměřena na úsilí podniknutá mezinárodně k vylepšení metod používaných k prevenci celosvětových pokusů o prolomení opatření spojených s bezpečností na letištích a soukromí online služeb, nabízených pasažérům.

V rámci akcí ICAO (International Civil Aviation Organization) a ICCAIA (International Coordinating Council of Aerospace Industries Associations), argumentovali že nové technologie jsou náchylné ke kybernetickým útokům. Proto bylo nutností vytvořit výzkumný tým zodpovědný za monitorování, správu a implementaci praktik a postupů potřebných k zajištění kybernetické bezpečnosti.
V roce 2013 IFALPA (International Federation of Air Line Pilots' Associations) zveřejnila zprávu[18] týkající se hrozby kybernetických útoků na letadla, letiště a různé online systémy pro cestující. Hlavním úkolem této zprávy bylo detailně pospat problémy se zabezpečením navigačních dat, která by mohla ovlivnit bezpečnost letišť, která nejsou adekvátně zabezpečená.
Organizace CANSO (Civil Air Navigation Services Organization) založila v roce 2014 výzkumnou skupinu. Jejíž práce vedla k vytvoření studie s názvem "Cyber Security and Risk Assessment Guide"[19]. Hlavním cílem této práce bylo vylepšit implementaci ustanovení sektorálních metod mezi zprostředkovateli ANSP (Air Navigation Service Provider).
V roce 2014 několik asociací jako ICAO, CANSO, ICCAIA and IATA podepsali plán CACSA (Civil Aviation Cyber Security Action). Tento plán donutil asociace k sjednocení sil ve snaze zmírnit kybernetické útoky. Spolupráce přispěla k rozvoji vyspělejší kultury, co se týče opravdového rizika vzniku kybernetických útoků a jak se proti nim bránit.
Nicméně globální pohled na problém je takový, že v leteckém sektoru pro civilní přepravu je potřeba zdokonalit technologie a prostředky k zajištění bezpečnosti na letištích. Ovšem problémem v tomto ohledu je skutečnost, že mnoho těchto technologií je používáno v ostatních průmyslových oblastech, což je činí ještě zranitelnějšími vůči potenciálním útočníkům. Podle studií provedených v předchozích letech bylo zjištěno, že počet kybernetických útoků, cílených na civilní

---

[18] Zpráva společnosti IFALPA týkající se hrozby kybernetických útoků na letadla dostupná zde http://www.anpac.it/attachments/article/575/130605-IFALPA-Cyber%20threats%20who%20controls%20your%20aircraft.pdf
[19] Studie s názvem „Cyber Security and Risk Assessment Guide" od organizace CANSO https://issuu.com/canso/docs/canso_cyber_security_and_risk_asses

letectví, stoupl. V závislosti na cílovém systému je možné zneužít velké množství zranitelných dat[20].

Následující systémy by mohly způsobit vážné problémy v oblasti lidského bezpečí a národní ochrany, pokud by byly ohroženy. Pokud se zaměříme na kybernetické útoky, nejčastěji napadané jsou následující systémy: počítačové systémy mezinárodních letišť, systémy řízení letadel za letu a systémy řízení letového provozu[21].

Internet je používán na letištích k jednoduchým operacím s informacemi nebo ke komunikaci. Další důležitý cíl by mohly představovat systémy SCADA (Supervisory Control and Data Acquisition). Tyto systémy nejčastěji slouží k ovládání ventilace, přepravy zavazadel atd.[22] (Khalid, 2016). Protože převážná většina mobilních aplikací vyžaduje ke svému fungování připojení k internetu, bezpečnostní systém letiště může být přetížen, což může mít dopady na provoz letiště. Tato skutečnost činí bezpečnostní systémy potenciálními cíli kybernetického útoku. Útoky mohou být fyzické (kamery, USB disky, počítače atd.) nebo virtuální (trojan, DoS, phishing atd.).

Vliv zavedení WiFi na letištích je, z pohledu několika expertů na bezpečnost, enormní. Španělský expert Hugo Teso demonstroval na konferenci EASA (European Aviation Safety Agency), jak donutit letadlo havarovat za pomoci ovládání systému řízení letadla, a to pomocí softwaru mobilní aplikace, kterou sám vytvořil[23]. Ruben Santamarta pomocí WiFi přístupného zábavního letového systému dokázal, že je možné zasáhnout do satelitní komunikace a díky tomu ovládat systém letové

---

[20] Studie ohledně výskytu kybernetických útoků na civilní letectví dostupné zde https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf a následně zde https://www.accenture.com/t20171010T121722Z__w__/us-en/_acnmedia/PDF-63/Accenture-Cyber-Threatscape-Report.pdf

[21] Článek zaměřený na zranitelné systémy v leteckém průmyslu https://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx

[22] Studie zaměřená na zabezpečení chytrých letišť https://www.enisa.europa.eu/publications/securing-smart-airports

[23] Článek o ovládnutí letadla pomocí mobilní aplikace dostupný na https://www.spiegel.de/international/business/hackers-warn-passenger-planes-vulnerable-to-cyber-attacks-a-1035172.html

navigace[24]. Přesně ta stejná věc se povedla v roce 2015 Chris Robertsovi, který podle dokumentace FBI po zadání jednoduchého příkazu CLB (climb) donutil letadlo stoupat.

4.4.2 Metodologie prevence proti kybernetickým útokům

Tato část je zaměřena na některé způsoby rozpoznání, zda je komunikační systém zranitelný vůči kybernetickým útokům, či nikoliv. Následné simulace jsou připraveny speciálně pro prostředí letiště a systémů zde používaných. Analýzou výsledků, takto simulovaných útoků, lze získat představu o tom, kde jsou slabá místa systému, na které se mohou útočníci zaměřit. Pomocí nasbíraných dat tak mohou být vytvořena řešení, jak takové hrozby řešit a také jak jim lze předcházet. V následující části jsou znázorněny některé scénáře, které popisují možné kybernetické útoky a jejich řešení (Suciu, 2018).

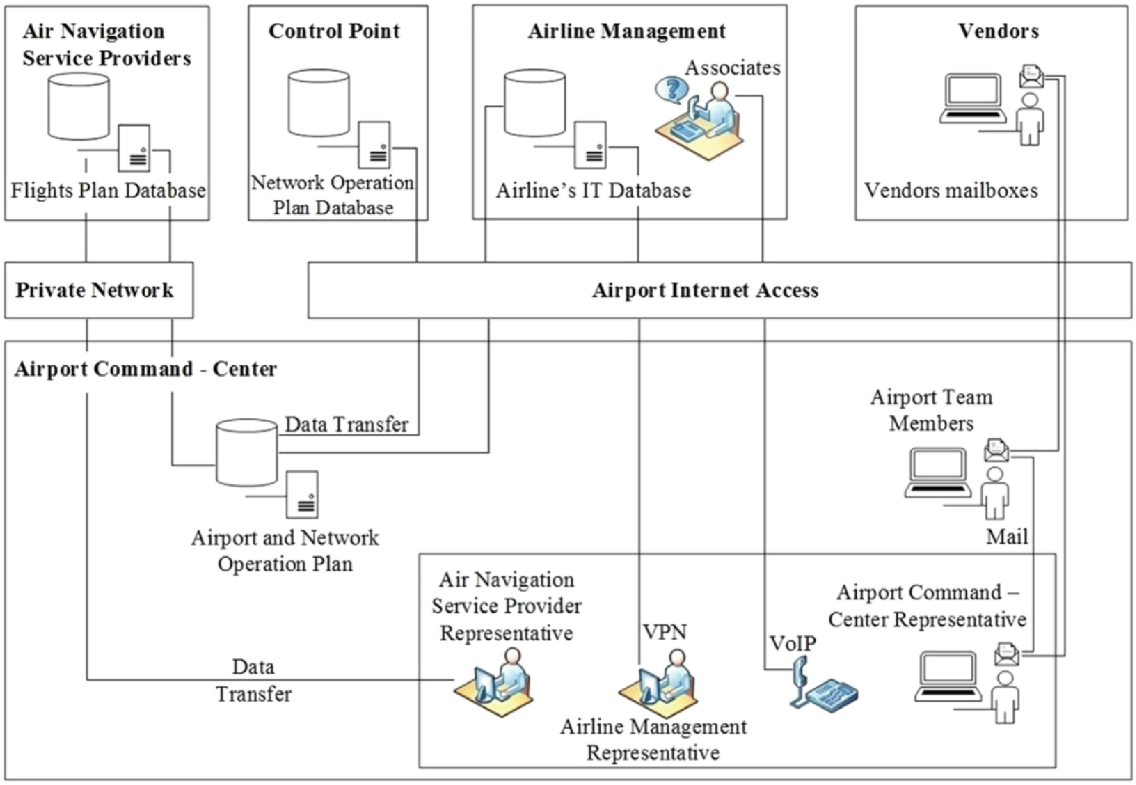
4.4.2.1 Prevence proti DDoS útokům na letištích

První scénář zahrnuje skutečnost, že skupina útočníků chce vydírat střední až velkou firmu. Jako formu vydírání zvolí výhružku v podobě DDoS útoku. Letištní společnosti jsou pro kybernetický zločin ideálním cílem. Splňují totiž dvě důležité podmínky. Těmi jsou závislost na připojení k internetu a mnoho finančních zdrojů. K samotnému útoku je zapotřebí znát IP adresu vlastněnou letištěm, což pro útočníky není žádným problémem dohledat. A v druhé řadě nějaké zdroje potřebné k vyvolání útoku (Suciu, 2018).

V případě, že management letiště odmítne zaplatit útočníkům požadovanou částku, útok bude zahájen. Následkem bude ztraceno připojení k internetu pro celé letiště. Pokud se potvrdí, že je letiště opravdu napadeno, je důležité okamžitě zahájit vyšetřování, které pomůže vyřešit kritickou situaci. Na obrázku pod odstavcem je znázorněna architektura sítě a všech síťových prvků na letišti. K veškeré komunikaci mezi jednotlivými částmi komunikační sítě letiště je zapotřebí internetové připojení. Pokud dojde k jeho ztracení, nebude tak možné aktualizovat

[24] Článek o ovládání letové navigace dostupný zde https://www.theregister.com/2013/04/13/faa_debunks_android_hijack_claim/

informace ze sektoru Airport Operation Plan (AOP) a Network Operation Plan (NOP), protože síť nebude schopna zvládnout potřebný tok dat (Suciu, 2018).



Obrázek 1 Schéma architektury sítě na letišti převzato z (Suciu, 2018).

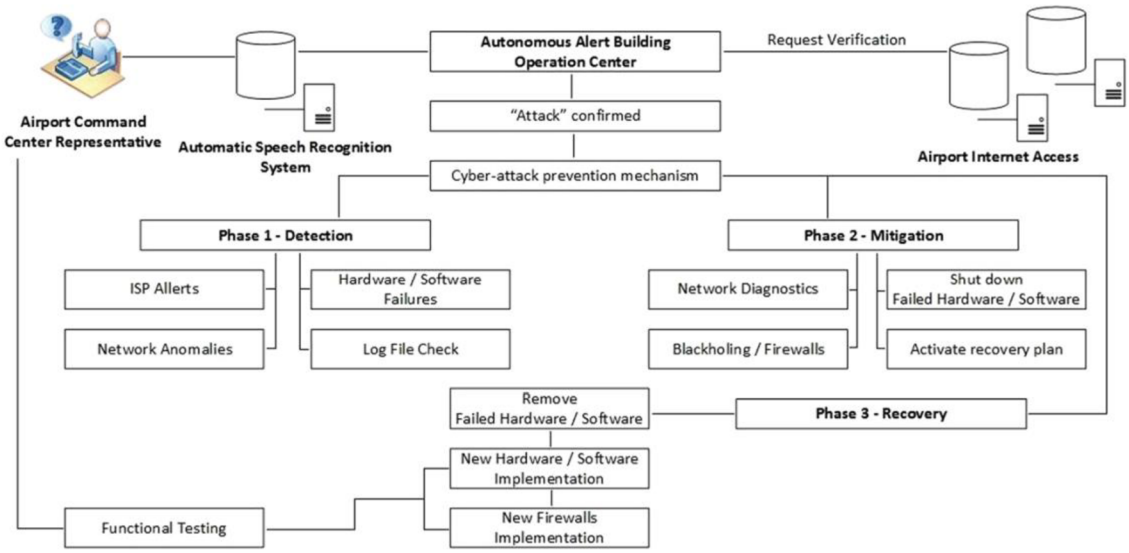
Preventivní opatření – mohou být použity následující metody:

1. **Objemová ochrana** – Je to jedna z metod používána providery k prevenci a identifikaci možných DDoS útoků. Provideři jsou také schopni filtrovat všechny požadavky obdržené z různých vysílacích zdrojů. Takto je možné snížit zatížení sítě neobvyklými požadavky, které by mohly znamenat potenciální hrozbu, a propouštět tak jen běžné a bezpečné požadavky na letištní IP adresu. Případně mohou být některé IP adresy, ze kterých chodí podezřelé dotazy, přidány na tzv. blacklist (pokud je adresa přidána do blacklistu, není možné se z dané IP adresy připojit do sítě).
2. Alternativní metodou, používanou při prevenci proti kybernetickým útokům na letiště, je vývoj sekundární internetové sítě. Tato síť má alokovaný jiný rozsah IP adres a je používána jen v nouzových situacích.

3. K co nejefektivnějšímu využití ochranných mechanismů je zapotřebí nasadit výkonné hardwarové vybavení, které má speciální internetová rozhraní. Hlavní rolí těchto zařízení je neustále monitorovat přihlašovací aktivity a frontu požadavků na dané IP adresy. V případě detekování útoku bude fronta s požadavky přesměrována do těchto zařízení, kde dojde k tzv. pročištění fronty[25].

Metoda protekce zmíněná v předešlých bodech se nazývá blackholing (V síti takto označujeme místa, kde příchozí/odchozí provoz zaniká, aniž by informoval odesílatele, že data nedosáhla svého cíle.). V tomto případě napadené IP adresy automaticky posílají upozornění top-level providerům, kteří pro ně zablokují veškerou frontu s dotazy. Velmi důležitá část této procedury je minimalizace lidského faktoru v procesu monitorování fronty s dotazy. Proto k informování vedení letiště o útoku není prostředníkem člověk, ale inteligentní systém. Při obdržení telefonátu, že je letiště napadeno, zástupci letiště budou podrobeni systému pro rozpoznání hlasu a poté dojde ke spuštění mechanismu znázorněnému na následujícím obrázku č.2[26].

[25] Report zaměření na preventivní opatření v zabezpečení kybernetického prostoru https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf
[26] Viz. 25



Obrázek 2 Funkcionalita mechanismu prevence kybernetického útoku převzato z (Suciu, 2018).

Detekce je založena na bezobslužném učení pro detekci anomálií. Bezobslužné učení umožňuje identifikaci či detekci anomálií v chování na logické úrovni. Detekční metoda je implementována za pomoci kombinace shlukové analýzy (shluková analýza je vícerozměrná metoda vycházející ze statistiky, která slouží ke klasifikaci objektů – třídí jednotky do skupin na základě podobnosti objektů) v první fázi (bezobslužné učení), následované fází učení pod dohledem (po objevení anomálií, které naznačují bezpečnostní problémy, incidenty atd.) (Suciu, 2018).

4.4.2.2 Prevence proti hrozbám Blended Attack na letištích

Co je to vlastně blended attack? Předpokladem je, že skupina útočníků chce narušit běžný provoz letiště, bez toho, aniž by byl pokus o vniknutí rychle detekován. K dosažení tohoto cíle je ideální zvolit právě blended attack, který neustále zahajuje nové útoky. Jeden z nich má za úkol být rychle detekován, aby na sebe vzal veškerou pozornost. Během toho, co se systém snaží zastavit tento první útok je v pozadí spuštěn další, který má již za cíl, ve většině případů, opět ochromit fungování letištní sítě, tedy tzv. DDoS útok. Pracovníci bezpečnostní ochrany budou muset řešit první falešný útok, ten hlavní mezitím zůstane bez povšimnutí. Díky tomu, že první útok je jen záminka, je tedy lehce vyřešitelný. Bezpečnostní technici po jeho odražení tedy

mohou nabýt dojmu, že hrozba byla odvrácena. Což je v tomto případě velký omyl (Suciu, 2018).

Výsledkem útoku může být změna letových plánů, jako například odlety nebo přílety, čímž vzniknou nechtěná zpoždění. Například pokud letadlo dorazí do dané destinace dříve, než bylo očekáváno, personál zodpovědný za bezpečné přistání letadla, by se musel dostavit na své pozice dříve. Pokud by byl naopak let zpožděn, personál by musel na letadlo čekat. Tento čas by mohl být využit k přípravě ostatních letů – zde tedy vznikají časové prostoje. Kvůli pozdním příletům by ostatní lety musely čekat kvůli obsazenosti letových drah. To by mělo za příčinu pozdní odlety letadel. Další problémy vzniklé se zpožděním jsou například nakládání/vykládání zavazadel, čištění letadel či doplňování paliva. Pokud by se takovýto útok uskutečnil například na mezinárodním letišti, zpoždění spojená s tímto problémem se mohou projevit celosvětově v závislosti na zpoždění letů mezi letišti (Suciu, 2018).

Personál zodpovídající za bezpečnost na letišti zjistí velice obtížně, že první útok byl jen záminkou pro následující větší útok. K vyhnutí se této situaci je zapotřebí proškolit a řádně zaučit personál o možném maskování velkého útoku dalším menším útokem. V ohledu na minimalizaci rizika vzniku těchto situací mohou být do systému implementovány hardwarové či softwarové komponenty, které budou neustále monitorovat provoz letištního vybavení (např. systém správy budov, uzavřený televizní okruh, komunikační a letový informační systém atd.). Další možností, jak předcházet podobným útokům, je analyzovat předešlé útoky podobného rázu a vyvinou a integrovat efektivnější bezpečnostní algoritmy, které budou sledovat letový provoz a dokáží rychle detekovat podezřelé množství na sebe navazujících zpoždění (Suciu, 2018).

4.4.2.3 Shrnutí hrozeb kybernetických útoků na letištích

Zajištění vysoké úrovně zabezpečení letištních prostor představuje zásadní aspekt, který musí být vyřešen co nejrychleji. Běžný provoz letiště může být snadno narušen, pokud dostupnost a integrita bezpečnostních systémů bude ohrožena. Při zvážení již zmíněných hrozeb hlavními kybernetickými hrozbami mohou být:

- Komunikační systémy starší generace, jejichž bezpečnostní mechanismy mohou bát lehce prolomeny. S touto technikou je prakticky nemožné zajistit na letišti dokonalou bezpečnost.
- Využívání zákaznických služeb, které jsou poskytovány společnostmi třetích stran. Tato možnost zvyšuje počet uživatelů, kteří mohou přistupovat k jádru infrastruktury, což může ovlivnit bezpečnost sítě.
- Dokonce i pokud většina systémů je řádně zabezpečená, je potřeba se ujistit, že alespoň nějakou míru zabezpečení mají všechny prvky sítě. Například pokud letištní access pointy nejsou spolehlivé, může kvůli nim být ohrožena celá síť. Dále jsou v poslední době na letištích implementovány prvky IoT (Internet of Things), které mají několik bezpečnostních rizik. (Arseni, 2015)

Pokud tyto problémy nebudou vyřešeny co nejrychleji, bude prevence proti teroristickým útokům stále těžší dosáhnout. To bude mít velký vliv na mezinárodní leteckou přepravu, což časem ovlivní důvěru veřejnosti a celkově mezinárodní bezpečnost (Suciu, 2018).

4.4.3 Kroky k lepšímu zabezpečení letišť

Momentální největší slabinou letišť jsou informační systémy a samotná síť, pomocí které jsou tyto systémy propojeny. Toto si ovšem uvědomují i zástupci samotných letišť, a tak investují nejen do zabezpečení, ale obecně do sektoru IT&T (informační technologie a telekomunikace) v prostorách letiště. V roce 2018 byla očekávaná investice do IT&T struktury 5,69 % z celkového zisku letiště, tento odhad byl nakonec překonán a celková investice za rok 2018 byla 6,06 %, což znamená přibližně 10 miliard dolarů celosvětově[27]. V roce 2019 byl očekáván další nárůst až na 6,26 %, což nakonec bohužel nebylo naplněno a v roce 2019 byla investice letišť do IT&T pouze 4,77 % z celkových zisků. Díky krizi způsobené koronavirem, což

[27] IT INSIGHT report od společnosti SITA pro rok 2019 https://www.sita.aero/globalassets/docs/surveys--reports/it-insights-2019.pdf

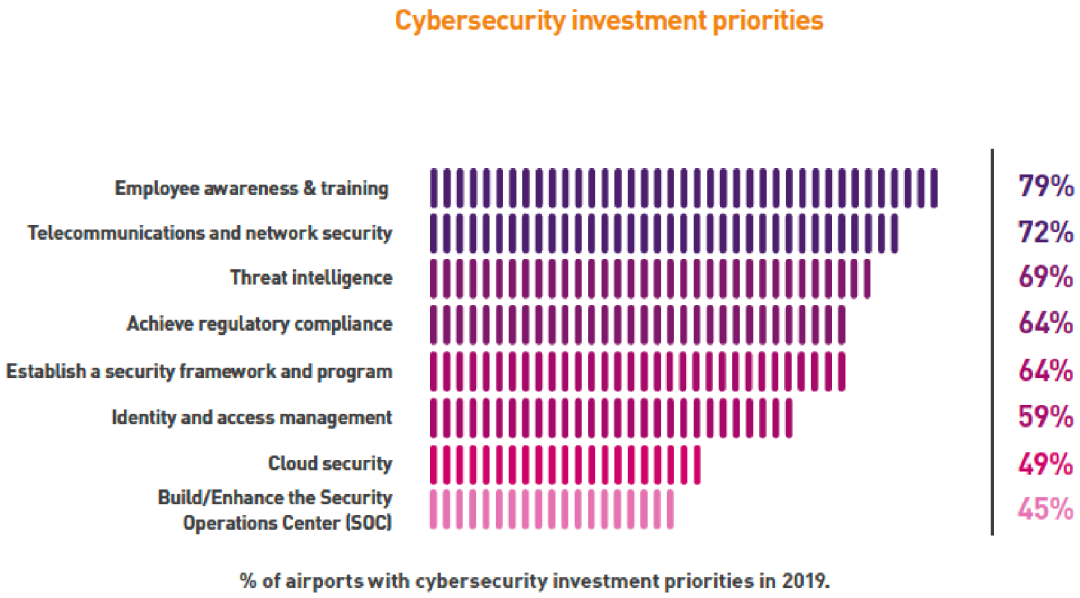
mělo za následek úpadek zisků letišť přibližně o 60 %, byl značně ponížen i rozpočet na rok 2020, který činí pouhé 3,21 %, tedy přibližně 3,5 miliardy dolarů[28].
Priority investic v roce 2020 do oboru IT&T kladou důraz na bezpečnost a zdraví zaměstnanců i cestujících. Proto hlavní investice povedou do automatizovaného měření teploty pasažérů a zaměstnanců, kontrolování rozestupů mezi jednotlivými osobami, robotů, kteří budou desinfikovat prostory letiště atd. V dohledu následujících tří let však nadále zůstávají dlouhodobé priority stále stejné a tedy: kybernetická bezpečnost, cloudové služby a tzv. business intelligence. Investice do těchto oblastí přispívá k digitální transformaci letišť. Plány do budoucna jsou:

- vývoj nových služeb pro pasažéry, které mohou využívat pomocí chytrého telefonu,
- přizpůsobit služby personálu tak, aby byly přístupné přes mobil nebo tablet,
- zrychlit práci z domovu pomocí vzdálených či virtuálních IT služeb do roku 2023[29].

Investice letišť v rámci kybernetické bezpečnosti v roce 2018 lehce klesly z 10 % na 8 % (procentuální část z celkové investice do IT&T). V roce 2019 byl očekáván nárůst až na 12 %, což nakonec nebylo naplněno. Iniciativa CIO (Chief Information Officer) pro kybernetickou bezpečnost vzrostla během několika posledních let kvůli zaměření na průmysl, sdílený osvědčených postupů, vzdělání a benchmarking nástroji poskytnutým ACI (Airport Council International). Investice do vzdělání a tréninku zaměstnanců je klíčovým faktorem při zlepšování kybernetické bezpečnosti na letištích. 79 % procent letišť uvádí tuto investici jako nejdůležitější. Dalšími prioritními oblastmi pro investice v oboru kybernetické bezpečnosti jsou: zabezpečení sítě a telekomunikací, a tzv. thread intelligence (thread intelligence je povědomí o hrozbách a jejich aktérech, tyto informace pomáhají předcházet či

[28] IT INSIGHT report od společnosti SITA pro rok 2020 https://www.sita.aero/globalassets/docs/surveys--reports/2020-air-transport-it-insights.pdf
[29] Viz. 28

alespoň zmírňovat škodlivé události v kybernetickém prostoru). Další oblasti investic jsou zaznamenány v grafu níže[30].



Obrázek 3 Graf prioritizace investic do kybernetické bezpečnosti (SITA, 2020).

[30] IT INSIGHT report od společnosti SITA pro rok 2019 https://www.sita.aero/globalassets/docs/surveys--reports/it-insights-2019.pdf

5 Závěry a doporučení

Bakalářská práce měla za cíl informovat o systémech běžně používaných na letištích a upozornit na problematiku spojenou s kybernetickými útoky v leteckém průmyslu. Jelikož systémů používaných v souvislosti s letištěm, létáním a vším kolem něj je nespočet, byly do práce vybrány jen ty nejdůležitější systémy, které ať už přímo či nepřímo ovlivňují cestující, pracovníky letiště či osoby pohybující se v okolí letiště.

Co se týče problematiky samotných kybernetických útoků, byly do práce zařazeny útoky z minulosti, ale také útoky z posledních let. Cílem práce bylo popsat útoky na letiště či systémy spojené s leteckým průmyslem, jako například systémy leteckých společností. Ukázalo se, že právě tyto systémy jsou v posledních letech nejčastějším cílem útočníků. Záměrem je získat osobní data co největšího počtu cestujících určité aerolinie.

Posledním cílem práce bylo zjistit, jaké kroky zabezpečení proti možným hackerským útokům letiště provádějí. V dnešní době, kdy jsou všechny systémy propojeny pomocí internetu, je potřeba se bránit především proti kybernetickým útokům. Proto se část práce zaměřuje právě na scénáře, které znázorňují možné potenciální útoky jako jsou například DDoS útoky či Blended Attack útoky. V těchto scénářích jsou analýzy útoků, které zahrnují informace, jak útokům předcházet, ale také jak postupovat v případě že k samotnému útoku dojde. Součástí kapitoly je také souhrn investic, které proudí do kybernetického zabezpečení letišť.

V budoucí, například diplomové, práci by bylo možné tuto tématiku rozšířit o podrobnou analýzu slabých míst systémů, na které nejčastěji cílí kybernetické útoky. A navrhnout konkrétní řešení, jak posílit a zabezpečit právě místa nejvíce využívaná hackery pro přístup do systémů.

6 Seznam použité literatury

[1] Pruša J. a kol. Svět letecké dopravy. II., rozšířené vydání. Praha: Gallileo Training, 2015. ISBN 978-80-260-8309-2.

[2] Barkat A. Travel and Tourism Management. Indie: PHI Learning, 2015. ISBN 9788120350588.

[3] Haddon L. Information and Communication Technologies in Everyday Life [online]. Berg, 2004 [cit. 2020-09-09]. Dostupné z: https://www.researchgate.net/publication/259256921_Information_and_Communication_Technologies_in_Everyday_Life

[4] What Is a Computer Reservation System? Colorwhistle [online]. 2020 [cit. 2020-09-09]. Dostupné z: https://colorwhistle.com/computer-reservation-system/

[5] About OAG. OAG [online]. [cit. 2020-09-09]. Dostupné z: https://www.oag.com/about-oag

[6] Zelenka. J. a kol. E-Turismus v oblasti cestovního ruchu [online]. 2008 [cit. 2020-09-09]. Dostupné z: https://www.researchgate.net/publication/275951375_e-Turismus_v_oblasti_cestovniho_ruchu

[7] Amadeus Global Report 2014 [online]. 2014 [cit. 2020-09-09]. Dostupné z: http://www.amadeus.com/msite/global-report/2014/en/pdf/amadeus-global-report-2014.pdf

[8] The Sabre Story [online]. 2015 [cit. 2020-09-09]. Dostupné z: https://www.sabre.com/files/Sabre-History.pdf

[9] Travelport history, profile and history video [online]. [cit. 2020-09-09]. Dostupné z: https://www.companieshistory.com/travelport/

[10] White paper 2018 [online]. 2018 [cit. 2020-09-09]. Dostupné z: https://www.iata.org/contentassets/8dbfa2bc1aca46c9aabad704ec905598/air-tt-white-paper.pdf

[11] Marks A. a Rietsema K. Airport Information Systems—Airside Management Information Systems. Intelligent Information Management [online]. 2014, 06

(03), 149-156 [cit. 2021-04-19]. ISSN 2160-5912. Dostupné z: doi:10.4236/iim.2014.63016

[12] Delta: Power cut strands thousands of passengers. BBC [online]. [cit. 2021-04-19]. 2016 Dostupné z: https://www.bbc.com/news/world-us-canada-37007908

[13] Cyberattack claims multiple airports in Vietnam. The Washington Times [online]. [cit. 2021-04-19]. 2016 Dostupné z: https://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/

[14] Vietnam to inspect use of Chinese technology following cyberattacks on airports. Tuoi Tre News [online]. 2016 [cit. 2021-04-19]. Dostupné z: https://tuoitrenews.vn/news/society/20160804/vietnam-to-inspect-use-of-chinese-technology-following-cyberattacks-on-airports/6052.html

[15] Aeroporto di Fiumicino, ore di stop e code al check in per un guasto alla connessione. La Republica [online]. 2016 [cit. 2021-04-19]. Dostupné z: https://roma.repubblica.it/cronaca/2016/07/18/news/fiumicino_problema_tecnico_al_t3_code_per_i_controlli_arrivano_in_strada-144357812/?ref=HREC1-6

[16] How Airbus defends against 12 big cyber attacks each year. IT News [online]. [cit. 2021-04-19]. 2016 Dostupné z: https://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131

[17] Recent Attacks on Airlines Suggests Hackers Are Now More Interested In Passenger Data. Cyware [online]. 2020 [cit. 2021-04-19]. Dostupné z: https://cyware.com/news/recent-attacks-on-airlines-suggests-hackers-are-now-more-interested-in-passenger-data-dfcecd34

[18] Mobile Phishing Campaign Offered Free Flights. Info security [online]. 2018 [cit. 2021-04-19]. Dostupné z: https://www.infosecurity-magazine.com/news/mobile-phishing-campaign-offered/

[19] EasyJet warn customers over scam competition on Facebook. GlasgowLive [online]. 2017 [cit. 2021-04-19]. Dostupné z:

https://www.glasgowlive.co.uk/news/glasgow-news/easyjet-warn-customers-over-scam-13510021

[20] 80,000 Passengers Affected By Transavia Data Breach. Simple Flying [online]. 2020 [cit. 2021-04-19]. Dostupné z: https://simpleflying.com/transavia-data-breach/

[21] Securing Smart Airports [online]. ENISA, 2016 [cit. 2021-04-19]. Dostupné z: https://www.enisa.europa.eu/publications/securing-smart-airports

[22] Suciu G. a kol. Cyber-Attacks – The Impact Over Airports Security and Prevention Modalities. ROCHA, Álvaro, Hojjat ADELI, Luís Paulo REIS a Sandra COSTANZO, ed. Trends and Advances in Information Systems and Technologies [online]. Cham: Springer International Publishing, 2018, 2018-03-24, s. 154-162 [cit. 2021-04-19]. Advances in Intelligent Systems and Computing. ISBN 978-3-319-77699-6. Dostupné z: doi:10.1007/978-3-319-77700-9_16

[23] Common Cyber Attacks: Reducing The Impact [online]. CERT-UK, 2015 [cit. 2021-04-19]. Dostupné z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

[24] Cyber threatscape report: Midyear cybersecurity risk review forecast and remediations [online]. Accenture, 2017 [cit. 2021-04-19]. Dostupné z: https://www.accenture.com/t20171010T121722Z__w__/us-en/_acnmedia/PDF-63/Accenture-Cyber-Threatscape-Report.pdf

[25] Aviation Unites on Cyber Threat [online]. ICAO, 2014 [cit. 2021-04-19]. Dostupné z: https://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx

[26] Cyber threats: who controls your aircraft? [online]. IFALPA, 2013 [cit. 2021-04-19]. Dostupné z: http://www.anpac.it/attachments/article/575/130605-IFALPA-Cyber%20threats%20who%20controls%20your%20aircraft.pdf

[27] CANSO cyber security and risk assessment guide [online]. CANSO, 2014 [cit. 2021-04-19]. Dostupné z: https://issuu.com/canso/docs/canso_cyber_security_and_risk_asses

[28] Khalid A. An Analysis of Airports Cyber-Security. Communications on Applied Electronics [online]. 2016, 4(7), 11-15 [cit. 2021-04-19]. ISSN 23944714. Dostupné z: doi:10.5120/cae2016652129

[29] Cyber-Attack Warning: Could Hackers Bring Down a Plane? Spiegel [online]. 2015 [cit. 2021-04-19]. Dostupné z: https://www.spiegel.de/international/business/hackers-warn-passenger-planes-vulnerable-to-cyber-attacks-a-1035172.html

[30] Mcallister N. FAA: 'No, you CAN'T hijack a plane with an Android app'. Spiegel [online]. 2013 [cit. 2021-04-19]. Dostupné z: https://www.theregister.com/2013/04/13/faa_debunks_android_hijack_claim/

[31] Addressing airport caber-security [online]. SESAR, 2016 [cit. 2021-04-19]. Dostupné z: https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf

[32] Arseni S-C a kol. Analysis of the security solutions implemented in current Internet of Things platforms. In: 2015 Conference Grid, Cloud & High Performance Computing in Science (ROLCG) [online]. IEEE, 2015, 2015, s. 1-4 [cit. 2021-04-19]. ISBN 978-6-0673-7040-9. Dostupné z: doi:10.1109/ROLCG.2015.7367416

[33] Air Transport IT Insights 2019 [online]. SITA, 2019 [cit. 2021-04-19]. Dostupné z: https://www.sita.aero/globalassets/docs/surveys--reports/it-insights-2019.pdf

[34] 'Drone' hits British Airways plane approaching Heathrow Airport. BBC [online]. 2016 [cit. 2021-04-19]. Dostupné z: https://www.bbc.com/news/uk-36067591

[35] Air Transport IT Insights 2020 [online]. SITA, 2020 [cit. 2021-04-19]. Dostupné z: https://www.sita.aero/globalassets/docs/surveys--reports/2020-air-transport-it-insights.pdf

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2019/2020

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení: **Radek Kápička**
Osobní číslo: **I1800180**
Adresa: Jonášova 442, Heřmanův Městec, 53803 Heřmanův Městec, Česká republika

Téma práce: Využití informačních technologií v letecké přepravě na letištích a možnosti zabezpečení proti možným hackerským útokům

Téma práce anglicky: The use of information technology in air transport at airports and security options against possible hacker attacks

Vedoucí práce: Ing. Hana Švecová
Katedra informačních technologií

Zásady pro vypracování:

Cílem bakalářské práce je analyzovat a popsat využití infomačních technologií v letecké přepravě, na letištích a jejich zabezpečení proti možných hackerským útokům.
Zásady:
Informační technologie v letecké přepravě a na letištích.
Zabezpečení a hackerské útoky u IS v letecké přepravě a na letištích.
Predikce vývoje informačních technologií v letecké přepravě a na letištích.
Osnova:

1. Základní pojmy
   1.1. Základní pojmy informačních technologií
   1.2. Základní pojmy v letecké dopravě
2. Informační technologie v letecké přepravě
   2.1. Informační technologie využívané aeroliniemi
   2.2. Informační technologie využívané v letištním provozu
   2.3. Informační technologie využívané v řízení letového provozu
   2.4. Informační technologie využívané cestujícími
3. Zabezpečení informačních systémů v letecké přepravě
   3.1. Analýza slabých míst informačních systémů
   3.2. Nástin zabezpečení proti možným hackerským útokům
4. Budoucnost informačních technologií v letecké přepravě
   4.1. Budoucnost informačních systémů
   4.2. Budoucnost možných hackerských útoků
   4.3. Budoucnost zabezpečení informačních systémů v letecké přepravě na letištích

Seznam doporučené literatury:

Pruša J. a kol. Svět letecké dopravy. II., rozšířené vydání. Praha: Gallileo Training, 2015. ISBN 978-80-260-8309-2.
Barkat A. Travel and Tourism Management. Indie: PHI Learning, 2015. ISBN 9788120350588.
Haddon L. Information and Communication Technologies in Everyday Life [online]. Berg, 2004 [cit. 2020-09-09]. Dostupné z: https://www.researchgate.net/publication/259256921_Information_and_Communication_Technologies_in_Everyday_Life
What Is a Computer Reservation System? Colorwhistle [online]. 2020 [cit. 2020-09-09]. Dostupné z: https://colorwhistle.com/computer-reservation-system/
About OAG. OAG [online]. [cit. 2020-09-09]. Dostupné z: https://www.oag.com/about-oag
Zelenka. J. a kol. E-Turismus v oblasti cestovního ruchu [online]. 2008 [cit. 2020-09-09]. Dostupné z: https://www.researchgate.net/publication/275951375_e-Turismus_v_oblasti_cestovniho_ruchu
Amadeus Global Report 2014 [online]. 2014 [cit. 2020-09-09]. Dostupné z: http://www.amadeus.com/msite/global-report/2014/en/pdf/amadeus-global-report-2014.pdf
The Sabre Story [online]. 2015 [cit. 2020-09-09]. Dostupné z: https://www.sabre.com/files/Sabre-History.pdf
Travelport history, profile and history video [online]. [cit. 2020-09-09]. Dostupné z: https://www.companieshistory.com/travelport/
White paper 2018 [online]. 2018 [cit. 2020-09-09]. Dostupné z: https://www.iata.org/contentassets/8dbfa2bc1aca46c9aabad704ec905598/air-tt-white-paper.pdf

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: