https://doi.org/10.26552/ pas.Z.2024.2.5

UNIVERSITY OF ŽILINA

SYSTÉM RIADENIA INFORMAČNEJ BEZPEČNOSTI (ISMS) A NÁVRH JEHO IMPLEMENTÁCIE U PREVÁDZKOVATEĽA LETISKA

Jakub Gahír
Air Transport Department
University of Žilina
Univerzitná 8215/1
010 26 Žilina

Denis Kontárová
Letové prevádzkové služby
Slovenskej republiky, štátny podnik
Ivanská cesta93
823 07 Bratislava

Abstract

The thesis is mainly focused on solving the problem of information security management system, subsequent analysis of legislative requirements in the Slovak Republic and the EU and comparison of the current state of implementation of the information security management system in the selected area at the M. R. Štefánik Airport in Bratislava with the minimum requirements for the selected area specified in the legislation. The work is systematically divided, with the first part being devoted to introducing the reader to the issues of the information security management system. The second part is focused on the analysis of individual legislative requirements in the Slovak Republic and the EU respectively. The third part is devoted to the components of the information security management system itself. The following fourth part is the main one and deals with the elaboration of the proposal for the implementation of the information security management system at the airport operator and the comparison of the current state of implementation in the selected area at the M. R. Štefánik Airport with the minimum requirements for the given area.

Keywords

ISMS. Information Security Management System. Information Security. Risk Management. Components and Tools. Implementation Design. Airport Operator.

1. Úvod

Informačná bezpečnosť je jedným z najzaujímavejších odvetví, v ktorom sa dá pracovať. Aby ste sa však v tejto rozmanitej a náročnej profesii zorientovali, je dôležité pochopiť, ako sa za posledných niekoľko desaťročí vyvinula do dnešnej podoby a oboznámiť sa s jazykom, ktorý odborníci v tejto oblasti používajú na komunikáciu. Pred tridsiatimi alebo štyridsiatimi rokmi, keď boli informačné technológie ešte v plienkach, sa takmer vôbec nepočítalo so zamestnávaním špecializovaných pracovníkov v oblasti bezpečnosti IT. Namiesto toho boli v krízových situáciách mobilizovaní najznalejší a najskúsenejší systémoví architekti, administrátori a programátori, ktorí si museli poradiť so všetkým, čo sa na nich vrhlo. Ešte koncom 90. rokov minulého storočia neboli v netechnických podnikoch presne definované úlohy. Namiesto toho bola funkcia informačnej bezpečnosti prikrútená k iným pracovným pozíciám, ako napríklad vedúci prevádzky, správca systému, správca siete a dokonca aj manažér kvality (v závislosti od zamerania).

Cieľom článku je navrhnúť možnosť(i), ako aplikovať systém riadenia informačnej bezpečnosti v prostredí prevádzkovateľa letiska a to na základe zistení o súčasnom stave, podmienok stanovených v nariadeniach Európskej únie a odborníkov v odvetví informačnej bezpečnosti. Výstupom tak bude návrh spôsobu implementácie systému na letisku a porovnanie súčasného stavu implementácie systému riadenia informačnej bezpečnosti na letisku M. R. Štefánika v Bratislave.

2. Problematika informačnej bezpečnosti

Kybernetika sa v dnešných médiách stala všadeprítomným prívlastkom, ktorý označuje všetko, čo sa týka súkromia alebo bezpečnosti na internete. Málokedy sa stane, aby sme nepočuli alebo nečítali o kybernetickej vojne, kybernetických útokoch, kybernetickej bezpečnosti, kyberšikane a kybernetickej bezpečnosti. Odkiaľ sa však vzal tento zvláštny prívlastok? [1]

Prvé dôkazy o používaní (okrem gréckeho koreňa znamenajúceho riadenie) pochádzajú zo 40. rokov 20. storočia, keď matematik Norbert Weiner písal o kybernetike ako o počítačových systémoch, ktoré by jedného dňa mohli fungovať na základe spätnej väzby a byť samosprávne. V 80. rokoch 20. storočia sa tento termín pridával k akémukoľvek slovu, aby znelo futuristicky alebo špičkovo, a nahradil menej cool termíny, napr. digitálny. V 90. rokoch 20. storočia sa kybernetika vyvinula v úplne novom význame, keď sa na scéne objavili erotické portály, ktoré sa vzťahovali na virtuálny chat s partnerom v dial-up IRCS a online fórach [1].

Ako roky plynuli a vyššie spomenuté portály boli do veľkej miery nahradené online pornografiou a zoznamkami, vláda si tento pojem vzala späť a armáda začala hovoriť o ďalšej zmene vojnových paradigiem, ktoré sa presunuli na bojisko kybernetiky. A s kybernetickou vojnou prišla aj kybernetická bezpečnosť, kybernetické útoky a kybernetická spravodajská služba [1].

Dnes sa kybernetika dá v podstate pripojiť k čomukoľvek, ale médiá zamerali jej používanie predovšetkým na bezpečnostný priemysel, a preto sme sa všetci stali odborníkmi na kybernetickú bezpečnosť, či sa nám to páči, alebo nie. Dôležité však je uvedomovať si rozdiely medzi jednotlivými druhmi bezpečnosti - či už sa jedná o kybernetickú alebo informačnú [1].

3. Metodika a metódy skúmania

Pri tvorbe článku boli použité viaceré metódy skúmania. V prvom rade bolo potrebné preštudovanie odbornej literatúry a legislatívy v oblasti informačnej bezpečnosti. V ďalších častiach

som využil metódu analýzy a komparácie jednotlivých legislatívnych požiadaviek na vytvorenie jednotného celku pravidiel na implementáciu systému riadenia informačnej bezpečnosti u prevádzkovateľa letiska ale aj metódu interview s bezpečnostným analytikom a interným audítorom na letisku M. R. Štefánika v Bratislave na zistenie aktuálneho stavu implementácie v mnou zvolenej oblasti a následnej komparácie s minimálnymi požiadavkami na systém riadenia informačnej bezpečnosti v určenej oblasti.

4. Výsledky

Systém ISMS je potrebné implementovať tak, aby zahŕňal tri kľúčové aspekty: riadenie, riziko a súlad (GRC). Tento rámec integruje rozmery bezpečnostného rizika a výkonnosti s cieľom určiť vhodné a vyhovujúce nástroje kontroly bezpečnosti informácií. Vhodne zvolené kontrolné nástroje účinne zabezpečujú potrebnú úroveň ochrany na dosiahnutie cieľov bezpečnosti letectva [2][3][4].

4.1. Perspektíva riadenia

Táto perspektíva kladie dôraz na zabezpečenie vedenia a riadenia na dosiahnutie cieľov organizácie. Kľúčové prvky zahŕňajú:

- Vyšší manažment preukazuje záväzky subjektu aktívnym definovaním a zabezpečením úzkej účasti na implementácii ISMS. Tým sa vytvára prístup „zhora nadol“.
- Ciele v oblasti bezpečnosti a ochrany informácií sú zosúladené a konzistentné s obchodnými cieľmi organizácie. Preskúmania vedením sú kľúčovým nástrojom na monitorovanie tohto zosúladenia.
- Stanovujú sa politiky informačnej bezpečnosti, v ktorých sa uvádzajú zásady a ciele, ktoré má subjekt dosiahnuť. Úlohy, zodpovednosti, kompetencie a zdroje sú jasne definované pre účinný systém ISMS. Okrem toho účinné komunikačné stratégie zabezpečujú jasné posielanie správ interným aj externým zainteresovaným stranám [2][3][4].

4.2. Perspektíva rizika

Riadenie rizík je v kontexte bezpečnosti letectva rozhodujúcim aspektom systému ISMS. Slúži ako základ pre transparentné a efektívne rozhodovanie a stanovenie priorít kontrol a možností ošetrenia rizík. Táto perspektíva zahŕňa:

- Riziká informačnej bezpečnosti sa posudzujú, ošetrujú a monitorujú s cieľom podporiť riadenie rizík bezpečnosti letectva pre kľúčové procesy a informačné aktíva, od ktorých závisia. To zahŕňa definovanie požiadaviek na ochranu, zváženie vystavenia sa riziku a stanovenie kritérií akceptovateľnosti rizika na základe priemyselných noriem a metodík [2][3][4].

4.3. Perspektíva dodržiavania predpisov

Dodržiavanie regulačných, právnych a zmluvných požiadaviek je elementárne z pohľadu dôležitosti [2][3][4].

Z tohto hľadiska je potrebné definovať, implementovať a udržiavať potrebné ustanovenia o bezpečnosti informácií. Pravidelné monitorovanie a overovanie, ako napríklad interné audity, zabezpečujú účinnosť a súlad s týmito ustanoveniami [2][3][4].

Vychádzajúc z princípov riadenia, rizík a súladu (GRC), toto nariadenie identifikuje komplexný súbor procesov a tematických oblastí, ktoré sa považujú za nevyhnutné na vytvorenie účinného systému riadenia informačnej bezpečnosti (ISMS) [2][3][4].

Okrem týchto základných procesov je pre úspešnú implementáciu a prevádzku systému ISMS rozhodujúcich niekoľko ďalších faktorov:

- Systém ISMS by mal byť bezproblémovo integrovaný s existujúcimi procesmi organizácie, celkovou štruktúrou riadenia a bezpečnostnými opatreniami. V ideálnom prípade by mal byť čiastočne alebo úplne integrovaný so zastrešujúcim systémom riadenia zahŕňajúcim informačnú bezpečnosť, bezpečnosť letectva a riadenie kvality. To podporuje holistický prístup k riadeniu rizík a znižuje potenciálne siločiary medzi týmito kritickými oblasťami.
- Pri navrhovaní procesov, postupov, systémov a kontrolných mechanizmov informačnej bezpečnosti by sa mali úvahy o informačnej bezpečnosti začleniť už v prvých fázach. Tento proaktívny prístup zabezpečuje bezproblémovú integráciu, maximalizáciu účinnosti, minimalizáciu narušenia existujúcich funkcií a optimalizáciu nákladov. Neskoršie dodatočné zavedenie opatrení na zabezpečenie informácií môže tieto výhody negovať.
- Proces riadenia rizík zohráva dôležitú úlohu pri určovaní vhodných vlastností preventívnych kontrol. Tieto kontroly by mali byť prispôsobené tak, aby sa dosiahla a udržala prijateľná úroveň rizika informačnej bezpečnosti v kontexte bezpečnosti letectva.
- Efektívny proces riadenia incidentov umožňuje, aby organizácia mohla rýchlo odhaliť incidenty informačnej bezpečnosti. To si vyžaduje vopred definované úlohy, postupy, scenáre reakcie a plány, ktoré uľahčia koordinovanú, cielenú a účinnú reakciu v prípade výskytu incidentov.
- Systém ISMS by mal byť dynamickým systémom, ktorý je neustále monitorovaný a prehodnocovaný. Zistené nedostatky a oblasti na zlepšenie by mali byť riešené prostredníctvom priebežných vylepšení. Tým sa podporuje kultúra neustáleho učenia sa a prispôsobovania, čím sa zabezpečí, že systém ISMS zostane účinný vzhľadom na vyvíjajúce sa hrozby a zraniteľnosti [2][3][4].

Vyššie uvedené základné zložky súvisia s požiadavkami v tomto nariadení, pre ktoré obrázok poskytuje vysokoúrovňové zobrazenie aspektov, ktoré sú výraznejšie vo fáze implementácie, a aspektov, ktoré charakterizujú prevádzkovú fázu, ako aj preskúmanie a možné zlepšenie, ak funkcie nefungujú podľa plánu [2][3][4].

Monitorovanie súladu

Pre účely posúdenia súladu s ustanoveniami by organizácia mala zaviesť funkciu pravidelného monitorovania miery zhody systému riadenia s príslušnými požiadavkami a primeranosti postupov vrátane zavedenia procesu vnútorného auditu a procesu riadenia rizík informačnej bezpečnosti. Ak organizácia už zaviedla funkciu monitorovania súladu podľa vykonávacieho predpisu pre svoju oblasť, takáto funkcia by mala zahŕňať monitorovanie systému riadenia s príslušnými požiadavkami v rámci rozsahu jej činností. Monitorovanie súladu by malo zahŕňať mechanizmus spätnej väzby zistení auditu zodpovednému manažérovi alebo v prípade projektových organizácií vedúcemu projektovej organizácie alebo povereným osobám, aby sa zabezpečilo vykonanie potrebných nápravných opatrení [2][3][4].

Na účely monitorovania súladu by sa mali v plánovaných intervaloch vykonávať interné audity, ktoré poskytnú vedeniu uistenie o stave ISMS a informácie o:

- súlade ISMS s požiadavkami nariadení a vlastnými požiadavkami organizácie, ktoré sú buď uvedené v politike, postupoch a zmluvách v oblasti informačnej bezpečnosti, alebo vyplývajú z cieľov informačnej bezpečnosti alebo z výsledkov procesu zaobchádzania s rizikami;
- účinnom zavádzaní a udržiavaní ISMS [2][3][4].

Vnútorné audity by sa mali riadiť nezávislým prístupom a rozhodovacím procesom založeným na dôkazoch. Okrem toho by sa pri zostavovaní programu auditu mala zohľadniť dôležitosť príslušných procesov a definície kritérií a rozsahov auditu. Mali by sa uchovávať zdokumentované informácie potvrdzujúce výsledky auditu, ich oznamovanie príslušnému vedeniu a program auditu [2][3][4].

Pri zisťovaní miery zhody s ustanoveniami by organizácia mala zaviesť a udržiavať procesy pre kontrolu bezpečnosti informácií tak, aby boli dostatočne spoľahlivé a účinné pri ochrane informácií, a zabezpečovali zásady "need-to-know" (t. j. obmedzenie prístupu k informáciám len na tie osoby, ktoré ich potrebujú na plnenie svojich povinností). Prevádzkovateľ (organizácia) by mal chrániť zdroj informácií v súlade s príslušnými ustanoveniami stanovenými v nariadení (EÚ) 2018/1139 [2][3][4].

4.4. Integrácia systému ISMS s existujúcimi systémami riadenia

Organizácia môže pri zavádzaní ISMS využiť existujúce systémy riadenia tým, že ho integruje s týmito existujúcimi systémami [2][3][4].

Integráciou ISMS s existujúcimi systémami riadenia môže organizácia znížiť úsilie a náklady potrebné na zavedenie a udržiavanie ISMS a zároveň zabezpečiť konzistentnosť a súlad s celkovým prístupom organizácie k riadeniu. Nižšie je uvedený neúplný zoznam potenciálnych synergií, ktoré možno využiť pri integrácii ISMS s existujúcim systémom riadenia:

- *Využitie existujúcich politík a postupov*: organizácia môže využiť svoje existujúce politiky a postupy ako základ pre svoj systém ISMS. To môže pomôcť zabezpečiť konzistentnosť a minimalizovať potrebu dodatočnej dokumentácie.
- *Zosúladenie ISMS s inými systémami riadenia*: organizácia môže zosúladiť ISMS s inými systémami riadenia, ako sú systémy riadenia bezpečnosti (SMS, SeMS), aby sa zabezpečil súlad ISMS s celkovým prístupom organizácie k riadeniu.
- *Použiť existujúce procesy riadenia rizík:* organizácia môže použiť svoje existujúce procesy riadenia rizík na identifikáciu a posúdenie rizík informačnej bezpečnosti, ktoré môžu potenciálne viesť k ohrozeniu bezpečnosti letectva.
- *Opätovné použitie existujúcich kontrolných mechanizmov*: organizácia môže opätovne použiť existujúce kontrolné mechanizmy, ako sú kontroly prístupu alebo proces riadenia incidentov, na implementáciu kontrolných mechanizmov informačnej bezpečnosti požadovaných v rámci ISMS.
- *Proces neustáleho zlepšovania*: organizácia môže využívať procesy neustáleho (kontinuálneho) zlepšovania existujúcich systémov riadenia na postupné zlepšovanie ISMS [2][3][4].

4.5. Hodnotenie rizík

Pri hodnotení rizík môžu sa použiť nižšie uvedené úrovne klasifikácie rizík pre možnosť výskytu scenára ohrozenia a závažnosť bezpečnostných následkov, to však nebráni organizácii vytvoriť ďalšie prechodné kategórie, ak to považuje za potrebné pre posúdenie rizík. Organizácia by mala špecifikovať a zdokumentovať aplikované, pre organizáciu špecifické, klasifikačné úrovne s presnou kvalitatívnou alebo kvantitatívnou definíciou v zmysle rozsahu alebo intervalu číselných hodnôt, aby sa umožnil dostatočne kalibrovaný, konzistentný odhad, hodnotenie a komunikácia v rámci organizácie alebo s prepojenými subjektmi. Potenciál výskytu scenára ohrozenia sa môže vyjadriť ako interval pravdepodobností vrátane trvania pozorovania [2][3][4].

Výraz „trvanie pozorovania“ sa vzťahuje na časové obdobie, počas ktorého sa scenár hrozby pozoruje alebo monitoruje. Má zásadný význam pri určovaní pravdepodobnosti výskytu scenára hrozby, pretože pravdepodobnosť výskytu sa môže meniť v závislosti od dĺžky obdobia pozorovania [2][3][4].

S cieľom uľahčiť vzájomnú porovnateľnosť metodík hodnotenia rizík medzi spolupracujúcimi organizáciami môže organizácia priradiť hodnotenie potenciálu výskytu scenára ohrozenia k jednej z týchto kategórií:

- *Vysoký potenciál výskytu*: scenár hrozby sa pravdepodobne vyskytne. Útok súvisiaci so scenárom hrozby je uskutočniteľný a podobné scenáre hrozby sa v minulosti vyskytli mnohokrát.
- *Stredný potenciál výskytu*: scenár hrozby sa pravdepodobne nevyskytne. Útok súvisiaci so scenárom hrozby je možný a podobný scenár hrozby sa mohol vyskytnúť v minulosti.
- *Nízky potenciál výskytu*: výskyt scenára hrozby je veľmi nepravdepodobný. Uskutočnenie scenára

hrozby je teoreticky možné, nie je však známe, že by k nemu došlo [2][3][4].

4.6. Vzťah medzi interným a externým ohlasovaním

Organizácie by mali interne zhromažďovať a oznamovať incidenty a zraniteľnosti. Pre úplný a účinný systém podávania správ je potrebné interné aj externé podávanie správ. Interné hlásenia by sa mali včas posúdiť a v prípade, že potenciálny vplyv na bezpečnosť predstavuje nebezpečný stav, organizácie by mali iniciovať nahlasovanie týchto interných hlásení [2][3][4].

4.7. Stratégia detekcie

Pri vypracúvaní stratégie detekcie by mala organizácia pre položky v rozsahu detekcie udalostí definovať podmienky, ktoré spúšťajú proces, ktorý by si napríklad vyžadoval zásah personálu a ďalšiu analýzu.

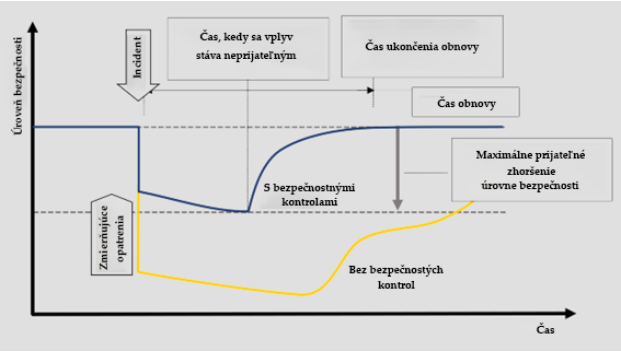
Mali by tak zohľadňovať abnormálne správanie, ako aj podstatné odchýlky od východiskových podmienok a relevantnú koreláciu viacerých nezávislých udalostí [2][3][4].

4.8. Ciele obnovy a načasovanie

Úroveň prevádzky a bezpečnosť môžu byť vzájomne prepojené, takže v niektorých prípadoch, keď je úroveň prevádzky ohrozená incidentom informačnej bezpečnosti a klesne, úroveň bezpečnosti urobí to isté. Je to napríklad prípad riadenia letovej prevádzky: ak sa zníži kvalitatívna úroveň poskytovaných letových prevádzkových služieb alebo sa stanú nespoľahlivými, veľmi pravdepodobne sa časom zníži aj bezpečnosť letov [2][3][4].

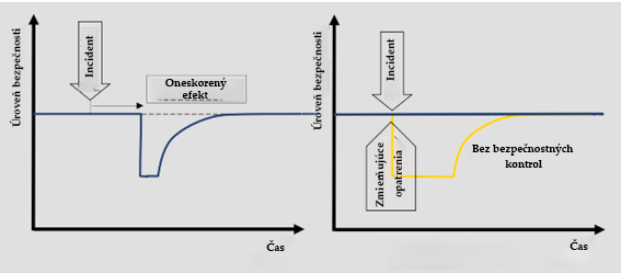
V iných prípadoch však môže byť vzťah medzi úrovňou prevádzky a bezpečnosťou opačný alebo môžu byť oddelené, takže keď dôjde k incidentu a úroveň prevádzky klesne, úroveň bezpečnosti sa zachová. Jedným z príkladov je ohrozenie procesu načítavania softvéru na palube lietadla. V tomto prípade by zistený incident, po ktorom by nasledovalo rozhodnutie prerušiť operáciu načítavania, zachoval existujúcu úroveň bezpečnosti [2][3][4].

Na obrázku č. 1 je znázornený koncepčný rámec, ktorý možno zvážiť pri definovaní cieľov reakcie a obnovy vrátane času obnovy. V najhoršom prípade znázorňuje, ako sa môže v čase meniť očakávaná úroveň prevádzkovej bezpečnosti procesu alebo činnosti, keď dôjde k incidentu informačnej bezpečnosti. V tomto scenári sa úroveň bezpečnosti najprv zníži v dôsledku incidentu a potom sa zhoršuje, kým plynie čas. Na obrázku je znázornený aj očakávaný účinok, ktorý by mali mať zmierňujúce opatrenia a kontrolné mechanizmy, a to: pri obmedzení poklesu prevádzkovej bezpečnosti hneď po vzniku incidentu a pri zlepšení obnovy, t. j. návratu na očakávanú úroveň bezpečnosti [2][3][4].



Obrázok 1. Očakávaný účinok, ktorý by mali mať zmierňujúce opatrenia a kontrolné mechanizmy

Ako už bolo spomenuté, medzi úrovňou prevádzky a bezpečnosťou môžu existovať rôzne vzťahy, ktoré by viedli k odlišnému zobrazeniu uvedeného obrázku. V určitých prípadoch môže mať incident oneskorený vplyv na úroveň bezpečnosti (napr. ohrozené vývojové prostredie), ako je znázornené na obrázku č. 8, alebo nemusí mať žiadny vplyv, ak je riadne kontrolovaný, ako v prípade už spomínaného ohrozeného procesu načítania softvéru, ktorý je znázornený na obrázku č. 2 [2][3][4].



Obrázok 2. Oneskorený vplyv na úroveň bezpečnosti

Okrem toho je potrebné poznamenať, že ten istý incident sa môže riešiť rôznymi spôsobmi, pretože existuje niekoľko faktorov, ktoré môžu ovplyvniť bezpečnosť [2][3][4].

Postup obnovy alebo plán obnovy by mal opisovať opatrenia na obnovu po incidente a interné alebo externé zdroje, ktoré sa na tom podieľajú (napr. zamestnanci, IT, budovy, poskytovatelia) [2][3][4].

Zdroje potrebné na uplatnenie opatrení na obnovu by mali byť k dispozícii, aby bolo možné včas realizovať opatrenia na obnovu po vzniku incidentu. Tieto zdroje môžu byť k dispozícii interne alebo ich môžu poskytovať zmluvné organizácie. Zmluvné zabezpečenie činností obnovy by sa malo stanoviť pred vznikom incidentu (proaktívne) a zmluva by mala obsahovať ustanovenia o včasnej reakcii zmluvnej strany [2][3][4].

Návrat do bezpečného a chráneného stavu si môže spočiatku vyžadovať núdzové opatrenia, čo sú činnosti, ktoré sa iniciujú na základe najlepších informácií dostupných v danom čase, skôr ako sa dosiahne úplné pochopenie situácie, a tieto opatrenia môžu potenciálne (dočasne) zhoršiť úroveň služieb alebo funkcií. Návrat do bezpečného a chráneného stavu by sa mal vyhodnotiť na základe počiatočného posúdenia rizika a môže sa len dočasne líšiť od bežných prevádzkových podmienok. Každé zvýšenie zostatkového rizika a trvanie tohto zvýšeného rizika, t. j. v dôsledku zavedenia núdzových opatrení, by však malo byť

zdokumentované a akceptované na príslušnej úrovni zodpovednosti za riadenie [2][3][4].

Uvedené činnosti obnovy môžu byť tiež výsledkom reakcie na incidenty, v prípade ktorých organizácia dostala informácie, ktoré si vyžadujú zavedenie primeraných opatrení s cieľom reagovať na incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva [2][3][4].

V takomto kontexte organizácia nemusí mať proces alebo plán obnovy pokrývajúci konkrétnu udalosť. Preto sa zvyčajne vyžaduje, aby organizácia definovala konkrétny plán obnovy a aby ho schválil príslušný orgán [2][3][4].

4.9. Neustále zlepšovanie

Proces neustáleho zlepšovania, by mal byť zameraný na neustále zlepšovanie účinnosti, vhodnosti a primeranosti ISMS. To by sa malo dosiahnuť aktívnym a systematickým hodnotením ISMS a všetkých jeho prvkov - vrátane jeho vyspelosti. Hodnotenie by malo zohľadňovať výsledky a závery iných procesov informačnej bezpečnosti vrátane zaistenia auditov, preskúmania manažmentom, hodnotenia výkonnosti, účinnosti a vyspelosti, ako aj výsledky odvodených nápravných opatrení a korekcií [2][3][4].

Kontext a rizikové prostredie organizácií nie sú nikdy statické, a preto si vyžadujú dynamické prispôsobovanie, vývoj a zmeny cieľov, architektúr, organizačných štruktúr a procesov organizácie, aby sa riziká informačnej bezpečnosti udržali na prijateľnej úrovni. V dôsledku toho by sa mal systém ISMS považovať za vyvíjajúcu sa a učiacu sa súčasť/element organizácie, ktorý je potrebné neustále monitorovať a zlepšovať, aby sa zabezpečil súlad s bezpečnostnými cieľmi a efektívnosťou organizácie [2][3][4].

Cieľom CIP je neustále zlepšovať účinnosť, vhodnosť, primeranosť a, ak sa to považuje za potrebné, efektívnosť ISMS. Organizácia môže integrovať CIP časti IS do niektorého iného už prevádzkovaného CIP a môže uplatňovať metódy, ako je cyklus PDCA alebo DMAIC [2][3][4].

CIP je založený na proaktívnom a systematickom hodnotení ISMS a všetkých jeho prvkov vrátane procesov a kontrol bezpečnosti informácií riadených ISMS. Posúdenie by sa malo vykonať na základe organizačných cieľov pre požadované úrovne výkonnosti, účinnosti a vyspelosti. Tieto ciele sa môžu okrem zabezpečenia dosiahnutia súladu s požiadavkami podľa tohto nariadenia zamerať aj na ciele stanovené politikou alebo normami organizácie a rozhodnutiami vedenia [2][3][4].

Uvedené hodnotenie vychádza z výsledkov hodnotenia výkonnosti, výstupov auditov, procesov rizík a incidentov, ako aj z už uplatnených nápravných a korekčných opatrení.

Možnosti zlepšenia môžu byť identifikované na základe výsledkov hodnotenia CIP alebo môžu byť predložené ako návrhy z iných zdrojov. Identifikácia často zahŕňa odchýlky alebo nápravné opatrenia, ako aj neúčinné procesy alebo kontroly, ktoré nie sú odstránené [2][3][4].

Návrhy na zlepšenie pochádzajú z týchto zdrojov:

- *Riadenie rizík*: výsledky pravidelnej analýzy rizík a následné ošetrenie rizík sú primárnym faktorom zlepšovania ISMS, pričom proces ošetrenia rizík zahŕňa monitorovanie zavedených bezpečnostných opatrení a hodnotenie ich účinnosti.
- *Hodnotenie výkonnosti a účinnosti*: závery z ukazovateľov výkonnosti, ich meranie, analýza a priebežné monitorovanie, ako aj výsledok hodnotenia účinnosti vrátane výsledkov následne uplatnených korekcií a nápravných opatrení.
- Hodnotenie vyspelosti vrátane výsledkov následne uplatnených opráv a nápravných opatrení.
- Skúsenosti získané z procesu odhaľovania, riešenia a reakcie na bezpečnostné incidenty a z možného riešenia základnej príčiny.
- Výsledky interných auditov sa môžu použiť na overenie toho, či ISMS a kontroly v rámci rozsahu auditu spĺňajú požiadavky organizácie, a na určenie toho, kde existujú potenciálne oblasti na zlepšenie.
- Preskúmanie a vyhodnotenie aktuálneho akčného plánu manažmentom, stanovenie alebo revízia cieľov alebo rozhodnutie o možnostiach a opatreniach na zlepšenie.
- Program návrhov organizácie preskúmania, prieskumy alebo hodnotenia so zamestnancami alebo spätná väzba od dodávateľov alebo spolupracujúcich strán [2][3][4].

Všetky výsledky tohto procesu by mali byť zdokumentované. Výsledné opatrenia sa môžu začleniť do zastrešujúceho akčného plánu, ktorý sa centrálne konsoliduje a pravidelne reviduje podľa príslušných politík. Výsledný akčný plán môže byť ďalej rozdelený na taktický, krátkodobý/strednodobý akčný plán a strategický, dlhodobý akčný plán [2][3][4].

4.10. Implementácia ISMS na letisku M. R. Štefánika

Systém riadenia nie je z veľkej časti individualizovaný, ale je riadený na úrovni skupín. To znamená, že existuje užívateľ OCC, Ramp Control atď., pod ktorého spadá viacero individuálnych zamestnancov. Táto skupina má jednoznačne dané zloženie a existuje relačná väzba na zmenu, ktorá v danom čase dané zariadenia obsluhuje. V praxi to znamená, že je jasne definované podľa dochádzkového systému, akí zamestnanci majú aktuálne prístup k informačným systémom danej skupiny, a tí, ktorí potrebujú širšie oprávnenia a prístupy, majú individuálny účet (týka sa najmä riadiacich a administratívnych funkcií). U prevádzkovateľa letiska teda funguje tzv. hybridný systém riadenia digitálnych identít vo vzťahu k priamym užívateľom alebo tým, ktorí sú oboznamovaní s informáciami prostredníctvom tlače alebo formulárov.

Tieto identity, či už individuálne alebo skupinové, definujú oprávnenia do určitých informačných systémov pomocou Microsoft serveru, ktorý cez certifikát zariadenia overuje zariadenie a užívateľa na základe štandardnej alebo dvoj-faktorovej autentifikácie a následne v rozsahu logických štruktúr nastavených v active directory. Ten má informáciu o tom, že daná osoba á prístup k tomuto priečinku, aplikácie, webovému portálu atď. a na základe tejto informácie sa danej identite udelí prístup.

Jednotlivé servery sú prepojené väzbami aj vo vzťahu k riadeniu bezpečnosti a sú zrkadlené tak, aby sa zabezpečila maximálna dostupnosť. Pomocou týchto serverov (vrátane firewallov) sú riadené a overované prístupy k identitám a zariadeniam.

Prístup k systémom, internetu a ďalším službám je odčlenený s priamou väzbou na poskytovateľa internetu tak, aby boli odtienené všetky ostatné siete, prvky a komponenty nachádzajúce sa na letisku kvôli riadeniu bezpečnosti. Takýmto spôsobom je riadený proces, aby človek, ktorý sa pripojí na wifi, či už vo verejnej alebo neverejnej časti terminálu, neohrozí interné informačné systémy, ktoré musia mať zaistenú požadovanú dostupnosť. Spôsob, ktorým sa tento systém nastaví, je už na prevádzkovateľovi základnej služby, v našom prípade na prevádzkovateľovi letiska, a je popísaný v internej dokumentácii v pravidlách používania a nakladania s IT prostriedkami. Z hľadiska bezpečnostných opatrení letisko využíva:

4.10.1. Zásadu čistého stola

- Na stole nesmú ostávať akékoľvek dokumenty, súvisiace so spoločnosťou alebo jej zákazníkmi a dokumenty, obsahujúce akékoľvek citlivé informácie,
- Dokumenty po vytlačení treba okamžite z tlačiarní odniesť

4.10.2. Zásadu čistej obrazovky

- V prípade aj krátkodobého opustenia pracoviska je potrebné zamedziť použitie PC jeho uzamknutím pričom každá pracovná stanica musí byť vždy uzamknutá alebo vypnutá, pokiaľ s ňou nikto nepracuje. Uzamknutie počítača bráni nielen neoprávnenému použitiu, ale aj k prípadnému prečítaniu citlivých informácií na obrazovke
- Musí byť nastavený šetrič obrazovky chránený heslom
- Na ploche operačného systému sa nesmú vyskytovať súbory, ktorých názvy obsahujú náznak hesla alebo heslo samotné. Taktiež na ploche nesmú ostať otvorené dokumenty, obsahujúce citlivé informácie
- V prípade skupinových identít je bezpečnosť zabezpečená prístupom do kancelárie len pre vyhradené osoby pomocou kľúčového systému.

Tieto opatrenia slúžia k zamedzeniu zneužitia digitálnej identity a sú implementované podľa potrieb prevádzkovateľa letiska. Prijímajú sa vo vzťahu k hodnoteniu a kategorizácií jednotlivých aktív.

Riadenie prístupov osôb k sieti a informačným systémom je postavené na logických štruktúrach Microsoft servera a active directory. Ten všetko centrálne riadi a prostredníctvom neho sú riadené oprávnenia pre jednotlivé sieťové prvky pomocou doménového administrátora.

Prístup k sieťovým zariadeniam, zdieľaným dátam, informačným systémom ako aj pracovným staniciam je riadený a kontrolovaný a vychádza zo zásady „potreba vedieť“. Prístup k osobným údajom majú len poučené oprávnené osoby.

Celý systém od požiadavky na rozsah oprávnení, ktorá sa vybaví a odošle cez prihlasovacie meno a heslo, zabezpečuje prístupy na úrovni základného operačného systému, sieťových prvkov a jednotlivých informačných systémov. Ďalej sa tieto prístupy monitorujú pomocou rôznych prvkov.

Na riadenie zodpovednosti slúžia interné predpisy, ktoré určujú, čo má daný zamestnanec robiť a akým spôsobom zabezpečiť minimalizovať možnosť zneužitia prístupov do informačných systémov.

Existuje centrálna správa, ktorá využíva virtuálne oddelených definícií, cez ktorú je riadený prístup k daným sieťam. Ak je užívateľ zamestnancom prevádzkového dispečingu (napr.), tak sa mu pomocou logických štruktúr definujú oprávnenia do systémov vyžívaných práve touto pracovnou funkciou.

Štandardne využívaným operačným systémom je Windows 11, existujú aj počítače, ktoré „bežia na“ Windows 10 prípadne starších, ktoré pre spoločnosti už nie sú bezpečnostne ideálne, ale za určitých podmienok je možné ich stále využívať. Prístup k operačnému systému znamená, že sa do daného operačného systému musí osoba autentifikovať a v rámci jeho služieb sa nepovoľujú služby a procesy, ktoré nesúvisia s pracovným zaradením alebo priamo letiskovou infraštruktúrou a tým vytvoriť potenciálnu hrozbu. Jedným z príkladov môže byť počítač od výrobcu DELL, ktorý sa automaticky snaží odosielať dáta do centrály spoločnosti, a preto je dôležité takéto služby trvalo deaktivovať, aby sa minimalizovali otvorené porty.

Prístup k aplikáciám je zabezpečený pomocou funkcie active directory, kde sa nachádzajú definované aplikácie a štruktúry, cez overovanie certifikátu alebo s podmienkou ďalšej autentifikácie. V prípade neúspešnej autentifikácie sa tento záznam uloží a po úspešnej autentifikácii sa zobrazí overenému používateľovi.

Monitorovanie prístupu a používania informačného systému funguje pomocou systému log, ktorý zaznamenáva prístupy jednotlivých identít do systému alebo aj príchod a odchod zamestnanca z pracoviska.

Riadenie vzdialeného prístupu je zabezpečované pomocou služby VPN.

Identifikátory na autentizáciu na vstup do siete a informačného systému sú prideľované každému jednotlivcovi v riadiacej alebo administratívnej funkcii alebo skupine osôb s rovnakým pracovným zaradením, do ktorej môže spadať až 15 zamestnancov.

Riadenie týchto identifikátorov zabezpečujú prístupové heslá do systémov, aplikácií atď., ktoré sa v pravidelných intervaloch menia.

Je zabezpečená kontrola a monitorovanie všetkých potrebných informácií vrátane prihlásenia, odhlásenia, otvorenia (priečinku, súboru, aplikácie), zmeny (hesla, názvu, umiestnenia), uloženia (súboru, priečinku). Každý objekt je priradený k systému, ktorý určuje akcie, aké môže daný používateľ v systéme vykonávať.

Databáza active directory je v pravidelných intervaloch revidovaná najmä vďaka systému log, ktorý monitoruje príchody a odchody zamestnancov. V praxi to znamená, že akonáhle zamestnanec odíde, tak sa v active directory deaktivuje na serverovej časti a následne sa aplikuje na všetky komponenty

sieťových prvkov. Konto sa nedá úplne vymazať, pretože v minulosti predstavovalo skupinu údajov, ktoré pod danou identitou boli robené, a tým pádom sú stále dohľadateľné a archivovateľné, ale je vo forme, ktorú vie aktivovať len určitá skupina a teda nie je možné sa cez ňu autentifikovať do systému.

Osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle bezpečnostnej politiky je v prípade bratislavského letiska systémový administrátor pre jednotlivé systémy.

4.11. Súlad s minimálnymi požiadavkami

V zvolenej oblasti riadenia informačnej bezpečnosti (v riadení prístupov) má letisko M. R. Štefánika systém dostatočne implementovaný, avšak s určitými rezervami, s ktorými je potrebné rátať do budúcnosti. Jedná sa hlavne o používané operačné systémy na niektorých z počítačov, ktoré využívajú Windows 10, prípadne staršie systémy. V prípade Windowsu 10 je potrebné rátať s koncom podpory od Microsoftu v polovici októbra budúceho roka, a teda bude potrebné z hľadiska bezpečnosti aktualizácia všetkých počítačov na Windows 11. Dá sa predpokladať, že počítače, na ktorých beží v súčasnej dobe Windows 10, nie sú kompatibilné s novšou verziou operačného systému a bude potrebné ich kompletne vymeniť, čo bude znamenať veľkú finančnú investíciu.

Druhou oblasťou, v ktorej prevádzkovateľ letiska spĺňa požiadavky legislatívy len čiastočne, je vytvorenie jednoznačného identifikátoru na autentizáciu na vstup do siete a informačného systému pre každú osobu. Ako som spomínal, na letisku funguje tzv. hybridný systém v oblasti virtuálnych identít čo znamená, že osoby v riadiacich alebo administratívnych funkciách majú svoju vlastnú identitu, a teda vlastný doménový účet pod svojim menom. Zvyšní zamestnanci spadajú pod virtuálne identity skupín, do ktorých môže spadať až 15 zamestnancov, čo predstavuje problém pri zisťovaní osôb, ktoré môžu v danom čase informačné systémy a siete reálne využívať. Na druhej strane by založenie osobných virtuálnych identít aj pre ostatných zamestnancov bolo nepraktické z hľadiska prevádzky. V tom prípade by si každý, kto dnes píše maily na skupinové identity, musel v ten daný deň zistiť, kto je práve na pracovisku, aby vedel, akej osobnej identite svoju požiadavku napíše. Riešením tohto problému by bolo preposielanie správ z osobnej virtuálnej identity na skupinovú, avšak tu sa dostávame do kolobehu nepraktických a finančne náročných riešení. Preto toto tzv. hybridné riešenie vnímam ako dostatočné a zároveň najpraktickejšie z hľadiska druhu a špecifických požiadaviek prevádzky a komunikácie s externými stranami.

V ostatných oblastiach spĺňa letisko M. R. Štefánika minimálne požiadavky na dostatočnej úrovni, v niektorých dokonca tieto požiadavky prevyšuje a zabezpečuje tak vyššiu úroveň informačnej bezpečnosti a dostupnosti ako v súčasnej dobe vyžaduje legislatíva.

Do budúcnosti je plán prevádzkovateľa letiska v oblasti riadenia informačnej bezpečnosti napredovať, na základe čoho bola vypracovaná stratégia kybernetickej bezpečnosti a zároveň aj rozpočet na ďalší rozvoj.

5. Záver

Cieľom môjho článku bolo analyzovať súčasnú legislatívu v oblasti riadenia informačnej bezpečnosti, na základe tej vypracovať návrh implementácie systému riadenia informačnej bezpečnosti u prevádzkovateľa letiska, zistiť pomocou interview aktuálny stav implementácie v zvolenej oblasti a porovnať ho s minimálnymi požiadavkami, ktoré vyžaduje legislatíva.

Analýza preukázala nedostatok národnej legislatívy v oblasti požiadaviek kladených na systém riadenia informačnej bezpečnosti, kde figuruje zatiaľ len zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a ďalšie vyhlášky, ktoré tento zákon upravujú. Vzhľadom na fakt, že informačná bezpečnosť má oveľa širší záber ako bezpečnosť kybernetická, bude potrebné transponovať nariadenia EÚ aj do národnej legislatívy.

Vypracovaný návrh implementácie systému ISMS obsahuje nevyhnutné riešenia pre zabezpečenie dostatočnej integrity, dostupnosti, autentifikácie a dôvernosti. Opiera sa o 3 základné perspektívy a to: perspektívu riadenia, perspektívu rizika a perspektívu dodržiavania predpisov. Ďalej boli vypracované ciele, spôsoby monitorovania súladu. Navrhnutý bol taktiež rozsah identifikácie a monitorovania rizík ako aj kritériá ich akceptácie.

Pri porovnaní súčasného stavu implementácie informačnej bezpečnosti vo zvolenej oblasti na letisku M. R. Štefánika boli zistené mierne nedostatky v oblasti operačného systému a jednoznačných identifikátorov na autentizáciu na vstup do siete a informačných systémov. Pri operačnom systéme bude nutné tento nedostatok vyriešiť najneskôr do októbra budúceho roka, kedy Microsoft ukončí svoju podporu pre operačný systém Windows 10.

V prípade identifikátorov bolo vyhodnotené, že aj napriek nedostatku voči minimálnym požiadavkám legislatívy súčasný implementovaný tzv. hybridný systém virtuálnych identít postačuje požiadavkám letiska či už z hľadiska bezpečnosti, ale aj prevádzky a praktickosti.

Referencie

[1] CAMPBELL, Tony (2016). Practical Information Security Management: A Complete Guide to Planning and Implementation. Burns Beach, Australia: Apress. [citované 2024-01-15].

[2] SlovLex (bez dáta). Online. Dostupné na: https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2018/69/20220630_5330728-2.pdf [citované 2024-03-20]

[3] EASA (2022). Online. Dostupné na: https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-information-security?page=8#_DxCrossRefBm363782835 [citované 2024-04-07]

[4] STN (2014). STN ISO/IEC 27001. SR. Úrad pre normalizáciu, meteorológiu a skušobníctvo [citované 2024-04-15]