POŠTA TELEKOMUNIKÁCIE A ELEKTRONICKÝ OBCHOD
elektronický časopis Katedry spojov

ANALÝZA RIZÍK V ODVETVÍ KURIÉRSKYCH, EXPRESNÝCH A BALÍKOVÝCH SLUŽIEB

Stanislava Komačková[1]

Abstract: One of the basic requirements for delivering parcels is to analyse the risks involved. That is why the paper deals with the analysis of risks in the courier, express, and parcel industry through the qualitative method FMEA in the process of delivery to parcel lockers. The paper aims to identify, analyse, and recommend actions for companies operating in the CEP market. The research results provide a comprehensive overview and quantification of the risks associated with parcel locker delivery.
Keywords: CEP industry, risk analysis, FMEA method, delivery, parcel locker.

Úvod

Odvetvie kuriérskych, expresných a balíkových služieb (angl. Courier, Express, and Parcel, ďalej len „CEP") patrí medzi jedno z najdynamickejšie sa rozvíjajúcich odvetví v rámci logistického trhu. Podľa výskumnej správy spoločnosti Mordor Intelligence sa veľkosť globálneho trhu CEP v roku 2023 odhaduje na 457,38 miliardy USD, pričom sa očakáva, že do roku 2028 dosiahne 758,17 miliardy USD pri ročnej zloženej miere rastu (angl. Compound Annual Growth Rate, ďalej len „CAGR") 10,64 %. [1] Veľkosť CAGR sa líši v závislosti od výskumnej správy a prognózovaného obdobia. Napríklad spoločnosť Allied Market Research predpokladá ročný rast na úrovni 6,3 % v rokoch 2021 – 2031. [2] Spoločným menovateľom všetkých výskumných správ je veľmi priaznivá prognóza trhu. Hnacou silou rozvoja odvetvia CEP je zvýšený dopyt po balíkových zásielkach z dôvodu rastu popularity elektronického obchodovania. Trh CEP je rozdelený do niekoľkých segmentov podľa geografie, typu zákazníkov, spôsobu dopravy a pod. [3] Z geografického hľadiska patrí medzi najrýchlejšie rozvíjajúce sa trhy región Ázie a Tichomoria (rozmach elektronického obchodovania, rastúca urbanizácia a stredná trieda obyvateľstva, investície do dopravnej a logistickej infraštruktúry a politické stimuly). [4,5] Vo všetkých regiónoch CEP trhu pôsobí niekoľko nadnárodných, ale aj regionálnych operátorov, pričom tento trh možno považovať za vysoko konkurenčný. Z hľadiska trhovej kapitalizácie patria medzi najväčších operátorov spoločnosti United Parcel Service, FedEx Corporation a Deutsche Post DHL Group, ktoré sú považované za tzv. integrátorov, pretože poskytujú zákazníkom integrované služby vo všetkých fázach distribučného reťazca. [6] Konkurovať integrátorom na CEP trhu je pre menšie podniky veľmi náročné. Pre dosiahnutie úspechu na trhu musia menší operátori využívať inovatívne prístupy

[1] Ing. Stanislava Komačková, Katedra spojov, FPEDAS, Žilinská univerzita v Žiline,
e-mail: Stanislava.komackova@stud.uniza.sk

a stratégie, zamerať sa na určitý zákaznícky segment trhu a predovšetkým poskytovať kvalitné služby s pridanou hodnotou.

Poskytovať kvalitné služby však nie je možné bez aplikácie princípov manažérstva rizika (ISO 31000) a kvality (ISO 9000). Podniky pôsobiace na CEP trhu preto musia identifikovať a zároveň vyhodnocovať všetky riziká spojené s poskytovaním služieb, aby zabezpečili zákazníkmi požadovanú kvalitu. Vo všeobecnosti možno riziko definovať ako možnosť, že sa stane niečo nežiaduce, čo bude mať negatívne dôsledky. Riziká však nevyhnutne nemusia vyvolať len negatívne dôsledky. [7] Ak podniky dokážu riziká identifikovať, analyzovať, hodnotiť a vhodným spôsobom s nimi zaobchádzať, môžu predstavovať i príležitosť pre získanie konkurenčnej výhody na trhu. V súvislosti s rizikom je potrebné zdôrazniť, že v každej ľudskej aktivite existujú určité riziká, ktoré nie je možné úplne eliminovať, preto musia podniky zohľadňovať tzv. akceptovateľné riziko. Pri zohľadňovaní rizík by mal byť určený zdroj rizika, ktorý môže ovplyvniť výkon a bezpečnosť ľudí, majetku a životného prostredia podniku. [8] V závislosti od zdroja rizika možno riziká v CEP odvetví klasifikovať na interné a externé riziká. Pri rizikách interného charakteru sa udalosti odvíjajú od činnosti podniku, pričom pri externých rizikách je ich pôvodom vonkajšie prostredie mimo okolia podniku, teda ich podnik nedokáže priamo ovplyvňovať. [9]

Napriek tomu, že odvetvie CEP je charakteristické poskytovaním troch hlavných typov služieb – kuriérskych, expresných a balíkových, ktoré sa líšia rôznymi špecifikami, ako napríklad lehotou prepravy, hmotnosťou prepravovaných zásielok a typom sprievodu, procesy potrebné pre ich poskytovanie sú veľmi podobné. Expresné a balíkové služby definuje proces vybrania a distribúcie zásielok. Tento proces pozostáva z viacerých čiastkových procesov – vybranie zásielok od odosielateľov, triedenie, preprava a dodanie adresátom. V prípade kuriérskych služieb absentuje proces triedenia, pretože zásielky sa nezhromažďujú, nespracovávajú a netriedia. [10,11] Základnou požiadavkou všetkých procesov je čo najväčšia efektívnosť. Z hľadiska vynaložených nákladov je proces dodania zásielky v literatúre mnohými autormi diskutovaný ako najnákladnejší, pričom podiel tohto procesu na celkových nákladov je okolo 30 % (Fan a kol. (2022); Greasley (2019); Myerson (2020)). Pre zefektívnenie procesu dodávania podniky využívajú inovatívne prístupy, pričom jeden z najpopulárnejších spôsobov predstavuje dodávanie zásielok do balíkomatov najmä vďaka automatizovanej prevádzke v režime 24/7. Podľa Putzgera (2020) je dodávanie do balíkomatov rýchlejšie a náklady sú nižšie o 10 % v porovnaní s tradičným doručovaním na adresu adresáta (angl. door-to-door delivery). Prostredníctvom tohto spôsobu dodávania je tiež možné vyriešiť niektoré z problémov, ktoré vznikajú pri tradičnom doručovaní na adresu, ako napríklad nezastihnutie adresáta, komplikované plánovanie trasy a dopravné oneskorenia. [16] Zároveň však dodávanie zásielok do balíkomatov predstavuje pre podniky v CEP odvetví nové riziká, ktoré pri doručovaní na adresu absentujú. Akým spôsobom však podniky v CEP odvetví riziká identifikujú, analyzujú, hodnotia a zaobchádzajú s nimi nie je úplne zrejmé a v literatúre je tejto problematike venovaná veľmi malá pozornosť. Predkladaný článok sa snaží túto výskumnú medzeru vyplniť.

Metodika

Nadväzujúc na výskumnú medzeru možno stanoviť výskumný cieľ článku. Hlavným cieľom článku je identifikácia a analýza rizík, ktoré môžu spôsobiť chyby v dodávaní zásielok do balíkomatov. Vzhľadom na absenciu komplexnej štúdie zaoberajúcej sa identifikáciou, analýzou a hodnotením rizík v procese dodávania zásielok do balíkomatov možno tvrdiť, že sa jedná o explorační výskumný cieľ. Výskumný cieľ tiež možno považovať za explanačný, pretože jeho dosiahnutím možno identifikovať a zároveň vysvetliť príčiny a následky rizík, ako aj vzťahy medzi rizikami navzájom.

Pre naplnenie hlavného cieľa článku bola použitá kvalitatívna výskumná metóda. Konkrétne sa jedná o metódu Analýza príčin a následkov porúch, ktorá je taktiež nazývaná Analýza možných chýb a ich následkov (z angl. Failure Mode and Effect Analysis, ďalej len „FMEA“). Metóda FMEA bola zvolená, pretože poskytuje systémový prístup k prevencii nekvality, umožňuje zvýšiť bezpečnosť a spoľahlivosť procesov a zároveň poskytuje možnosť ohodnotiť riziko chýb a na jeho základe stanoviť priority a opatrenia vedúce k zlepšeniu kvality. [17,18,19,20] Postup realizácie metódy FMEA je znázornený v nasledujúcej tabuľke.

Tabuľka 1. Postup realizácie metódy FMEA

P.Č.	POPIS KROKU
1.	Výber procesu aplikácie FMEA.
2.	Určenie potenciálnych chýb súvisiacich s procesom.
3.	Určenie významnosti a následkov identifikovaných chýb.
4.	Určenie výskytu a príčin identifikovaných chýb.
5.	Určenie pravdepodobnosti a metód odhalenia (detekcie) identifikovaných chýb.
6.	Výpočet hodnoty rizikového čísla.
7.	Návrh nápravných opatrení na predchádzanie chybám.

Zdroj: Autor

Stanoviť závažnosť identifikovanej chyby je možné na základe indexu významnosti (viď Tabuľka 2), ktorý vyjadruje závažnosť následku chyby u zákazníka, ak by sa táto chyba u neho vyskytla. Následok chyby je jediným kritériom pre určenie významnosti.

Tabuľka 2. Index významnosti chyby

HODNOTENIE	NÁSLEDOK CHYBY	ZÁVAŽNOSŤ NÁSLEDKU
10	Nebezpečný bez varovania	Veľmi vysoké hodnotenie závažnosti, keď potenciálny spôsob zlyhania ovplyvňuje bezpečnú prevádzku bez varovania.
9	Nebezpečný s varovaním	Veľmi vysoké hodnotenie závažnosti, keď potenciálny spôsob zlyhania ovplyvňuje bezpečnú prevádzku s varovaním.
8	Veľmi vážny	Nefunkčnosť procesu s deštruktívnou poruchou bez ohrozenia bezpečnosti.
7	Vážny	Nefunkčnosť procesu s poškodením zariadenia.
6	Mierny	Nefunkčnosť procesu s malým poškodením.
5	Malý	Nefunkčnosť procesu bez poškodenia.
4	Veľmi malý	Funkčnosť procesu s výrazným znížením výkonu.
3	Nevýznamný	Funkčnosť procesu s určitým zhoršením výkonu.
2	Úplne zanedbateľný	Funkčnosť procesu s minimálnym rušením.
1	Žiadny	Žiadny následok.

Zdroj: Vlastné spracovanie podľa [18,19,20]

Ďalším krokom realizácie metódy FMEA je určenie pravdepodobnosti výskytu chyby pomocou indexu výskytu (viď Tabuľka 3), ktorý vyjadruje pravdepodobnosť, že chyba spôsobená konkrétnou príčinou nastane.

Tabuľka 3. Index výskytu chyby

HODNOTENIE	VÝSKYT CHYBY	PRAVDEPODOBNOSŤ VÝSKYTU
10	Veľmi vysoký: výskyt chyby je takmer istý	≥ 1 z 2
9		1 z 3
8	Vysoký: opakovaný výskyt chyby	1 z 8
7		1 z 20
6	Stredný: občasný výskyt chyby	1 z 80
5		1 z 400
4	Nízky: relatívne malý výskyt chyby	1 z 2 000
3		1 z 15 000
2	Vzdialený: výskyt chyby je nepravdepodobný	1 zo 150 000
1		≤ 1 z 1 500 000

Zdroj: Vlastné spracovanie podľa [18,19,20]

Podobne ako v predchádzajúcich krokoch i na určenie pravdepodobnosti detekcie chyby je nutné použiť index odhalenia (viď Tabuľka 4), ktorý vyjadruje pravdepodobnosť odhalenia chyby prostredníctvom existujúcich kontrolných metód predtým, než sa produkt dostane k zákazníkovi.

Tabuľka 4. Index odhalenia chyby

HODNOTENIE	DETEKCIA	PRAVDEPODOBNOSŤ ODHALENIA CHYBY
10	Absolútne nemožná	Metóda kontroly nedokáže odhaliť potenciálnu príčinu.
9	Veľmi vzdialená	Veľmi vzdialená pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
8	Vzdialená	Vzdialená možnosť, že metóda kontroly odhalí potenciálnu príčinu.
7	Veľmi malá	Veľmi nízka pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
6	Malá	Nízka pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
5	Stredná	Stredná pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
4	Stredne vysoká	Stredne vysoká pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
3	Vysoká	Vysoká pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
2	Veľmi vysoká	Veľmi vysoká pravdepodobnosť, že metóda kontroly odhalí potenciálnu príčinu.
1	Takmer istá	Metóda kontroly odhalí potenciálnu príčinu.

Zdroj: Vlastné spracovanie podľa [18,19,20]

Po ohodnotení významnosti, výskytu a odhalenia je potrebné stanoviť priority identifikovaných chýb na základe rizikového prioritného čísla (angl. Risk Priority Number, ďalej len „RPN"). RPN možno vypočítať ako *súčin významnosti, výskytu a odhalenia chyby*. Získaním hodnoty RPN je možné stanoviť mieru rizika identifikovanej chyby (pozri Tabuľka 5) a podľa miery rizika vypracovať nápravné opatrenia, ktoré majú slúžiť na elimináciu, prípade zníženie miery rizika.

Tabuľka 5. Rozdelenie miery rizika

MIERA RIZIKA	DETEKCIA
Vysoká	<700 – 1000>
Stredná	<125 – 700)
Nízka, resp. žiadne riziko	<1 – 125)

Zdroj: Autor

Výsledky

Ako už bolo v prechádzajúcej časti uvedené, pre identifikáciu rizík v procese dodávania zásielok do balíkomatu, bola zvolená metóda FMEA. Balíkomat (angl. parcel locker) predstavuje samoobslužné zberné miesto určené na odosielanie a doručovanie zásielok, ktoré je nepretržite prístupné zákazníkom. Zvyčajne sa nachádza na ľahko prístupných miestach a v blízkosti miest s vysokou frekvenciou dopravy a veľkým pohybom chodcov, ako sú čerpacie stanice, nákupné centrá a námestia. [21,22] Implementácia balíkomatov podnikmi CEP prebieha niekoľko rokov, preto toto riešenie možno považovať za nie príliš preskúmané, najmä z hľadiska možných rizík. Z tohto dôvodu nasledujúca tabuľka reflektuje možné riziká v podobe chýb, ktoré sa môžu vyskytnúť v tomto procese.

Tabuľka 6. Identifikácia chýb v procese dodávania zásielok do balíkomatu

CHYBA	NÁSLEDOK	PRÍČINA	METÓDA KONTROLY
NEOPRÁVNENÝ PRÍSTUP	Strata/krádež zásielky Poškodenie zásielky Náklady na náhradu škody Poškodenie balíkomatu Strata/krádež údajov	Nedostatočné zabezpečenie Kybernetický útok	Kamerový systém, automatické zámky, alarmy na upozornenie personálu či úradov v prípade podozrivých aktivít v okolí Pravidelné kontroly na predchádzanie problémom, ktoré by mohli spôsobiť neoprávnený prístup Zabezpečenie balíkomatov firewallom, ktorý je súčasťou operačného systému
CHYBA SOFTVÉRU	Nefunkčnosť systému Nedoručenie zásielky Strata/krádež zásielky Strata údajov Nespokojnosť zákazníka	Zanedbanie aktualizácie Konfiguračné chyby	Pravidelné aktualizácie softvéru
PORUCHA POUŽÍVATEĽSKÉHO ROZHRANIA (DISPLEJ)	Nefunkčnosť systému Nedoručenie zásielky Nespokojnosť zákazníka	Chyba softvéru Chyba hardvéru Nesprávne používanie Poveternostné vplyvy (extrémne teploty, vlhkosť) Vandalizmus	Pravidelná technická kontrola
PORUCHA PLATOBNÉHO TERMINÁLU	Nemožnosť vyplatiť dobierkovú sumu Nedoručenie zásielky Nespokojnosť zákazníka	Nedostatočná údržba Výpadok internetu Výpadok elektrickej energie Nesprávne použitie Vandalizmus	Pravidelná údržba Kamerový systém
OTVORENIE NESPRÁVNEJ SCHRÁNKY	Doručenie nesprávnej zásielky Strata/krádež zásielky Nespokojnosť zákazníka	Chyba v systéme	Reklamácie zákazníkov Pravidelná technická kontrola
PORUCHA OTVÁRACIEHO MECHANIZMU SCHRÁNKY	Neschopnosť otvoriť/zatvoriť schránku Poškodenie zásielky Strata/krádež zásielky Možnosť úrazu	Mechanické poškodenie Opotrebenie Nesprávna údržba Výrobná vada	Pravidelná technická kontrola a údržba
NESPRÁVNE ULOŽENIE ZÁSIELKY V SCHRÁNKE	Doručenie nesprávnej zásielky Nedoručenie zásielky Poškodenie zásielky Nespokojnosť zákazníka	Nepozornosť kuriéra Chyba v dokumentácii	Pokyny pre vkladanie zásielok do schránok Reklamácie zákazníkov
VÝPADOK ELEKTRICKEJ ENERGIE	Nefunkčnosť systému Poškodenie balíkomatu Strata údajov Nedoručenie zásielky Nespokojnosť zákazníka	Nepriaznivé poveternostné podmienky Problém s napájaním (porucha elektrickej siete, generátora alebo batérie) Vandalizmus	Pravidelná technická údržba – identifikácia potenciálnych problémov Oznámenia od poskytovateľa elektrickej energie o plánovanej odstávke elektrickej energie

CHYBA	NÁSLEDOK	PRÍČINA	METÓDA KONTROLY
VÝPADOK INTERNETU	Nefunkčnosť systému Nedoručenie zásielky Strata údajov Nespokojnosť zákazníka Neoprávnený prístup	Problém so sieťou poskytovateľa služby (ISP), údržba a aktualizácia siete Poškodenie smerovača, modemu alebo iného hardvéru Kybernetický útok (DDoS útok alebo útok na sieťové zariadenie) Nepriaznivé poveternostné podmienky Výpadok elektrickej energie	Pravidelná údržba – identifikácia potenciálnych problémov Oznámenie o plánovanom výpadku od poskytovateľa internetových služieb
PROBLÉM S KAPACITOU BALÍKOMATU	Presmerovanie zásielky na iné odberné miesto Nespokojnosť zákazníka	Zvýšený dopyt zákazníkov Neupozornenie zákazníka na plnú obsadenosť	Monitorovanie vyťaženosti balíkomatu
NEVHODNÁ VEĽKOSŤ ZÁSIELKY	Uloženie zásielky na inom odbernom mieste Poškodenie zásielky (ak je uložená do balíkomatu pomocou sily) Nespokojnosť zákazníka	Nesprávne zadané informácie o veľkosti zásielky Zmena tvaru zásielky počas prepravy	Meranie a váženie zásielky pri podaji, prípadne v procese triedenia
FYZICKÉ POŠKODENIE BALÍKOMATU	Čiastočná alebo úplná nefunkčnosť Poškodenie zásielok Možnosť úrazu	Vandalizmus Nesprávne používanie Nepriaznivé poveternostné podmienky Opotrebenie Nevhodný obal zásielky Zásielka obsahujúca nebezpečný tovar	Kamerový systém, alarmy na upozornenie personálu či úradov Kontrola správneho balenia zásielok pri podaji Informovanie zákazníkov o zásielkach vylúčených z prepravy
PROBLÉMY S AUTENTIFIKÁCIOU POUŽÍVATEĽA	Nedoručenie zásielky Nespokojnosť zákazníka	Neznalosť zákazníka Chybné údaje alebo kód Chyba softvéru	Poskytovanie zákazníckej podpory pre riešenie problémov
NEINTUITÍVNE POUŽÍVATEĽSKÉ ROZHRANIE	Frustrácia zákazníka Zvýšená miera chýb Nespokojnosť zákazníka	Neprehľadnosť a nejasnosť pokynov Chyby v dizajne (nelogicky umiestnené tlačidlá, nevhodné menu) Jazyková bariéra	Sťažnosti zákazníkov Poskytovanie zákazníckej podpory

Zdroj: Autor

Po identifikácii možných chýb, ich príčin a následkov, ako aj metód kontroly je potrebné tieto chyby kvantifikovať na základe rizikového prioritného čísla. V nasledujúcej tabuľke sa nachádza kvantifikácia identifikovaných chýb, ako aj vyhodnotenie miery rizika.

Tabuľka 7. Kvantifikácia identifikovaných chýb v procese dodávania zásielok do balíkomatov

CHYBA	VÝZNAM	VÝSKYT	ODHALENIE	RPN	MIERA RIZIKA
NEOPRÁVNENÝ PRÍSTUP	8	3	8	**192**	Stredná
CHYBA SOFTVÉRU	7	4	4	**112**	Nízka

CHYBA	VÝZNAM	VÝSKYT	ODHALENIE	RPN	MIERA RIZIKA
PORUCHA POUŽÍVATEĽSKÉHO ROZHRANIA	7	3	3	**63**	Nízka
PORUCHA PLATOBNÉHO TERMINÁLU	6	3	3	**54**	Nízka
OTVORENIE NESPRÁVNEJ SCHRÁNKY	5	4	6	**120**	Nízka
PORUCHA OTVÁRACIEHO MECHANIZMU SCHRÁNKY	9	3	3	**81**	Nízka
NESPRÁVNE ULOŽENIE ZÁSIELKY V SCHRÁNKE	4	4	6	**96**	Nízka
VÝPADOK ELEKTRICKEJ ENERGIE	8	3	7	**168**	Stredná
VÝPADOK INTERNETU	8	3	7	**168**	Stredná
PROBLÉM S KAPACITOU BALÍKOMATU	5	5	2	**50**	Nízka
NEVHODNÁ VEĽKOSŤ ZÁSIELKY	5	4	2	**40**	Nízka
FYZICKÉ POŠKODENIE BALÍKOMATU	10	3	7	**210**	Stredná
PROBLÉMY S AUTENTIFIKÁCIOU POUŽÍVATEĽA	5	5	7	**175**	Stredná
NEINTUITÍVNE POUŽÍVATEĽSKÉ ROZHRANIE	3	5	3	**45**	Nízka

Zdroj: Autor

Na základe kvantifikácie chýb možno konštatovať, že päť identifikovaných chýb predstavuje stredne veľké riziko. Riziko fyzického poškodenia balíkomatov predstavuje chybu s najvyššou prioritou. Ďalšie významné riziko predstavujú problémy s autentifikáciou používateľa, neoprávnený prístup, výpadok elektrickej energie a internetu. Na minimalizáciu rizika týchto chýb by sa podniky mali prioritne zamerať a prijať vhodné opatrenia. Ako inšpiráciu pre podniky pôsobiace v odvetví CEP možno navrhnúť nasledovné nápravné opatrenia. V prípade rizika fyzického poškodenia balíkomatu sa odporúča:

- implementovať vhodný kamerový systém s alarmom, ktorý by v prípade vandalizmu okamžite upozornil určených zamestnancov a orgány činné v trestnom konaní (niektoré balíkomaty sú vybavené kamerovým systém, ale existujú mnohé, ktoré kamerovým systémom nedisponujú),
- neinštalovať balíkomaty v lokalitách so zvýšenou kriminalitou či v oblastiach ohrozených živelnými pohromami,
- vzdelávanie zamestnancov, ako aj zvýšenie informovanosti zákazníkov prostredníctvom vhodnej marketingovej komunikácie o správnom používaní balíkomatu,
- výmena či repasovanie poškodených prvkov a ich substitúcia kvalitnými materiálmi (zmena dodávateľa).

V prípade rizika neoprávneného prístupu je vhodné prijať nasledovné opatrenia:
- pravidelná kontrola funkčnosti kamerového systému, alarmov a automatických zámkov,
- inštalácia senzorov na monitorovanie balíkomatu a následná analýza získaných údajov s cieľom identifikovať pokusy o neoprávnený prístup,
- dodržiavanie noriem ISA/IEC62443, ktoré určujú požiadavky na bezpečnosť priemyselných automatizačných systémov, vrátane balíkomatov,
- používanie silných hesiel alebo prístupových kódov, ktoré zvýšia ochranu voči kybernetickým hrozbám,
- aplikácia dvojfaktorovej autentifikácie, ktorá vyžaduje od používateľa dva spôsoby overenia identity, pričom výber spôsobu závisí od požiadaviek konkrétneho podniku,
- používanie rôznych metód šifrovania na ochranu údajov prenášaných medzi balíkomatom a externými systémami, napr. asymetrické alebo hybridné šifrovanie.

Na minimalizáciu rizika spojeného so vznikom problémov autentifikácie používateľa možno prijať nasledovné opatrenia:
- implementácia systému na hlásenie akýchkoľvek chýb alebo problémov súvisiacich s autentifikáciou používateľov, ako sú problémy s generovaním prístupových kódov alebo chyby pri identifikácii používateľa,
- aplikácia záložných metód autentifikácie, ako sú jednorazové heslá (angl. One-Time Password, „OTP“) alebo záložné kódy pre prípad, že primárna metóda autentifikácie zlyhá,
- vykonávať pravidelné kontroly funkčnosti systému autentifikácie a analyzovať údaje ako napr. počet neúspešných prihlásení, počet blokovaných používateľov alebo počet sťažností za určité obdobie, pričom tieto údaje môžu predstavovať kľúčové ukazovatele výkonnosti, na základe ktorých možno merať efektívnosť procesu.

Na zníženie miery rizika súvisiaceho s výpadkom elektrickej energie sa odporúčajú nasledovné opatrenia:
- zabezpečenie záložného zdroja energie, ktorý je schopný zabezpečiť prevádzku balíkomatu min. 24 hodín (taktiež využívanie solárnych panelov),
- zlepšenie komunikácie a spolupráce s dodávateľom elektrickej energie,
- umiestňovanie balíkomatov mimo oblastí ohrozených živelnými pohromami a na suchých a bezpečných miestach.

Na predchádzanie chýb spojených s výpadkom internetu možno za vhodné opatrenia považovať:
- zabezpečenie redundantného pripojenia k internetu, kde balíkomat môže byť pripojený k internetu prostredníctvom optickej siete, káblovej siete alebo mobilnej siete (v prípade výpadku jednej siete by sa mohol balíkomat prepnúť na druhú sieť),
- bezpečnostné zabezpečenie siete, aby sa predišlo kybernetickým útokom na sieťové zariadenia,
- zálohovanie údajov, aby nemohlo dôjsť k ich strate.

Záver

Implementácia balíkomatov podnikmi CEP predstavuje inovatívne riešenie, ktoré so sebou okrem výhod prináša aj doteraz nepreskúmané riziká. Článok poukázal na viacero rizík, ktoré by mali CEP podniky zhodnotiť nielen pri zavádzaní balíkomatov do prevádzky, ale aj pri ich optimalizácii. Aplikáciou metódy FMEA bolo zistené, že všetky identifikované chyby majú nízku alebo strednú mieru rizika, pričom z hľadiska závažnosti chýb možno za najvýznamnejšie chyby považovať fyzické poškodenie balíkomatu, poruchu otváracieho

mechanizmu schránky, výpadok internetu, elektrickej energie alebo riziko neoprávneného prístupu. Existencia týchto rizík pre podniky pôsobiace v odvetví CEP predstavuje novú výzvu, pretože v tradičnom procese dodávania zásielok na adresu sa podobné riziká nevyskytujú. Identifikovaným rizikám by preto podniky mali venovať osobitnú pozornosť a snažiť sa nájsť vhodné riešenia na ich minimalizáciu, aby sa zabezpečila spoľahlivosť a bezpečnosť procesu, ako aj spokojnosť zákazníkov s poskytovanými službami. Na základe uvedených poznatkov by bolo vhodné realizovať ďalší výskum zameraný na vyhodnotenie skúseností CEP podnikov s identifikovanými rizikami. Budúci výskum by mohol využívať rôzne výskumné metódy, ako napr. expertné rozhovory alebo dotazníkový prieskum.

Literatúra

[1] MORDOR INTELLIGENCE: CEP Market - Industry Analysis & Size - Courier, Express and Parcel Statistics. 2023. [online]. [cit. 26.11.2023]. Dostupné na internete: https://www.mordorintelligence.com/industry-reports/courier-express-and-parcel-cep-market

[2] ABHAY S, SONIA M.: Courier, Express, and Parcel (CEP) Market Size, Share, Trends. 2022. Allied Market Research. [online]. [cit. 26.11.2023]. Dostupné na internete: http://www.alliedmarketresearch.com/courier-express-and-parcel-market-A11516

[3] Courier, Express And Parcel (CEP) Market Size, Share, & Forecast. 2023. Verified Market Research. [online]. [cit. 26.11.2023]. Dostupné na internete: http://www.verifiedmarketresearch.com/product/courier-express-and-parcel-cep-market/

[4] Asia Pacific Express Delivery Market Forecast. 2021. Business Market Insights. [online]. [cit. 26.11.2023]. Dostupné na internete: https://www.businessmarketinsights.com/reports/asia-pacific-express-delivery-market

[5] Courier, Express, and Parcel (CEP) Market. 2023. Market Data Forecast. [online]. [cit. 26.11.2023]. Dostupné na internete: https://www.businessmarketinsights.com/reports/asia-pacific-express-delivery-market

[6] Largest courier companies by market cap. [online]. [cit. 27.11.2023]. Dostupné na internete: https://companiesmarketcap.com/delivery-services/largest-delivery-companies-by-market-cap/

[7] BELAN, Ľ. A MIŠÍK, J.: Aplikácia zásady ALARP pri znižovaní úrovne rizika, projekt VEGA 1/0787/14 a VEGA 1/0175/14, ŽU v Žiline. FBI.

[8] DVOŘÁK, Z., ČIŽLÁK, M., SOUŠEK, R., SVENTEKOVÁ, E., LEITNER, B.: Riadenie rizík v železničnej doprave. 2010. Pardubice: Univerzita Pardubice. ISBN 978-80-86530-71-0

[9] Metódy analýzy rizika, Bezpečnostné riziká. [online]. [cit. 28.11.2023]. Dostupné na internete: https://www.ktit.pf.ukf.sk/images/clanky/Dokumenty/Projekty/Elektronicka_podpora_vyucby/Elektronick-podpora-vuby_rizik.pdf

[10] DECKERT, C. A GÖRS, N.: Transport carbon footprint in the german courier, express and parcel industry (CEP industry). 2019. NachhaltigkeitsManagementForum | Sustainability Management Forum, 27. Dostupné na internete: https://link.springer.com/article/10.1007/s00550-018-0471-1

[11] DUCRET, R.: Parcel deliveries and urban logistics: Changes and challenges in the courier express and parcel sector in Europe — The French case. 2014. Research in Transportation Business & Management, Managing Freight in Urban Areas 11, 15–22. Dostupné na internete: https://doi.org/10.1016/j.rtbm.2014.06.009

[12] FAN, K., TIAN, Y., YAO, L., QIU, R.: Urban Logistics Vehicle Routing Problem Under the Carbon Trading Market. 2022. Proceedings of the Sixteenth International Conference on Management Science and Engineering Management – Volume 2, 340–352.

[13] GREASLEY, A.: Absolute Essentials of Operations Management. 2019. Routledge. ISBN: 9780367259341.

[14] MYERSON, P.: Omni-Channel Retail and the Supply Chain (1st edition). 2020. Productivity Press, New York. ISBN: 9781003123415.

[15] PUTZGER, I.: Parcel locker and low-cost network operators eye last-mile opportunities. 2020. Dostupné na internete: https://theloadstar.com/parcel-locker-and-low-cost-network-operators-eye-last-mile-opportunities/

[16] ENEZINI G., A. LAGORIO, R. PINTO, A. DE MARCO, R. GOLINI: The Collection-AndDelivery Points Implementation Process from the Courier, Express and Parcel Operator's Perspective. IFAC-PapersOnLine, Volume 51, Issue 11. 2018. Pages 594-599, ISSN 2405- 8963. Dostupné na internete: https://doi.org/10.1016/j.ifacol.2018.08.383

[17] SUBRIADI, A. P. A NAJWA, N. F.: The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. Heliyon, 6(1), e03161. 2020. Dostupné na internete: https://doi.org/10.1016/j.heliyon.2020.e03161

[18] ANDREJIĆ, M. A KILIBARDA, M.: Failure management in distribution logistics applying FMEA approach. 2017. 3rd International Logistics conference - LOGIC 2017. Dostupné na internete: https://www.researchgate.net/publication/317821709_Failure_management_in_distribution_logistics_applying_FMEA_approach

[19] STRENITZEROVÁ, M.: Uplatnenie metódy FMEA (Failure mode and effect analysis) pri diagnostikovaní kvality služieb. 2014. In: Diagnostika podniku, controlling a logistika: VII. medzinárodná vedecká konferencia : zborník prednášok a príspevkov: Žilina: Žilinská univerzita, 2014. ISBN 978-80-554-0856-9.

[20] STRENITZEROVÁ, M. A PONIŠČIAKOVÁ, O.: Diagnostika a manažment procesov v riadení ľudských zdrojov 1. vyd. 2016. Žilina: Žilinská univerzita, 135 s. ISBN 80-8070-579-8.

[21] LAGORIO, A., A PINTO, R.: The parcel locker location issues: An overview of factors affecting their location. 2020. International Conference on Information Systems, Logistics and Supply Chain. Dostupné na internete: https://www.researchgate.net/publication/350726102_The_parcel_locker_location_issues_an_overview_of_factors_affecting_their_location

[22] AN, H. S., PARK, A., SONG, J. M., & CHUNG, C.: Consumers' adoption of parcel locker service: Protection and technology perspectives. 2022. Cogent Business & Management, 9(1), 2144096. Dostupné na internete: https://doi.org/10.1080/23311975.2022.2144096

Grantová podpora

059ŽU-4/2021 Synergia teórie a praxe v študijnom programe „Distribučné technológie a služby“