METODIKA PRO VÝBĚR METOD URČENÝCH PRO KVANTIFIKACI PENALIZAČNÍCH FAKTORŮ V OBLASTI KONVERGOVANÉ BEZPEČNOSTI

METHODOLOGY FOR SELECTING METHODS DESIGNED FOR QUANTIFICATION OF PENALIZING FACTORS IN THE CONVERGENT SECURITY AREA

Jan VÁVRA, Martin HROMADA
Univerzita Tomáše Bati ve Zlíně
Nad Stráněmi 4511, 760 05, Zlín, Česká republika
jvavra@utb.cz

Abstrakt: *Bezpečnost je základním kamenem jakékoliv společnosti. Téměř každý stát byl v novodobé historii ovlivněn překotným vývojem v oblasti technologií, které propojují a zefektivňují jednotlivé oblasti lidské činnosti. Tento vývoj však také zásadně ovlivnilo fundamentální pojetí bezpečnosti. Oblasti bezpečnosti v současnosti vnímány jako jeden koherentní systém, ve které je vytvořeno velké množství vazeb a závislostí, je také znám pod názvem konvergovaná bezpečnost. Správná kvantifikace penalizačních faktorů je jednou ze základních podmínek pro monitorování konvergované bezpečnosti. Hlavní náplní tohoto článku je návrh metodiky pro výběr vyhovující metody pro kvantifikaci penalizačních faktorů.*

Klíčová slova: *kybernetická bezpečnost, fyzická bezpečnost, provozní bezpečnost, penalizační faktor, konvergovaná bezpečnost.*

Abstrakt: *Security is the cornerstone of any society. Almost every state has been influenced by modern technology in recent history. Moreover, technology is responsible for increasing of connects and effectiveness of human activities. However, this development has influenced the fundamental concept of security. Currently, individual security areas are perceived as one coherent system, where is a large number of links and dependencies. It is also known as converged security. Correct quantification of penalizing factors is one of the basic conditions for monitoring of converged security. The main purpose of the article is to design a methodology for selecting a suitable method for quantification of penalizing factors.*

Klíčová slova: *cyber security, physical security, operational safety, penalty factor, converged security.*

Úvod

S lidskou společností je historicky spojen technologický vývoj, který se v posledních desetiletí exponenciálně zrychluje. Tento fenomén podrobuje státy, ale i samotné obyvatelé novým příležitostem a hrozbám. Bezpečnostní hrozby ve 21. století vytvářejí turbulentní prostředí, ve kterém jsou zvláště ohrožené vzájemně propojené sofistikované systémy. Oblast bezpečnosti vždy reflektuje potřeby společnosti, a tudíž musí respektovat současné trendy. Bezpečnost byla donedávna separována do několika podskupin. V rámci tohoto článku jsou předmětem výzkumu následující oblasti bezpečnosti: fyzická bezpečnost, kybernetická bezpečnost a provozní bezpečnost. Vnímání předložených oblastí bezpečností jako jeden celek je ústředním motivem konvergované bezpečnosti. Důvodem změny již dlouhodobě zažitého úzusu je technologie, která umožnila propojení jednotlivý oblastí bezpečnosti na elementární úrovni.

Konvergovaná bezpečnost si klade za cíl sloučit jednotlivé oblasti bezpečnosti do jednoho celku, přičemž bude kladen důraz na vzájemnou propojenost. To však často bývá velmi obtížné z důvodu rozdílné struktury jednotlivých oblastí bezpečnosti. Vyvstává také zásadní otázka, jakým způsobem rozpoznat a poté i kvantifikovat nalezené závislosti. Popis negativního působení pomocí penalizačních faktorů je možnou cestou jak vyhodnotit zvolený systém v reálném čase. Pro kvantifikaci těchto faktorů lze využít celou řadu metod, které se zdají býti více či méně vhodnými. Z tohoto důvodu vnikla předkládaná studie, která má za cíl zefektivnit

rozhodovací proces výběru vhodné metody pro kvantifikaci penalizačních faktorů. Tyto faktory jsou využity pro výpočet odolnosti referenčního objektu. Odolnost je vlastnost referenčního objektu vyjadřující jeho schopnost odolávat vniklé krizové situaci za předpokladu zachování základních funkcí.

Konvergovaná bezpečnost, penalizační faktory, nebo metody pro kvantifikaci penalizačních faktorů jsou výrazy, které spolu elementárně souvisejí. Jejich pochopení je nutné pro pochopení samotné studie. Z tohoto důvodu jsou tyto témata popsána v následujících kapitolách.

1 Konvergovaná bezpečnost

Současné pojetí bezpečnosti je v řadě případů značně neefektivní. Separátní pojetí jednotlivých oblastí bezpečnosti vykazuje nedostatky v oblastech finanční (samostatný bezpečnostní tým pro každou oblast bezpečnosti) a zajištění bezpečnost. Právě efektivní správa bezpečnosti je v současné době velmi obtížným a komplexním úkolem. Vývoj technologie umožnil propojení jednotlivých oblastí bezpečnosti na dosud nevídané úrovni. Jako příklad může posloužit zvyšující se závislost jednotlivých oblastí bezpečnosti na informačních a komunikačních technologiích (IKT) jejichž ochranou se zabývá kybernetický bezpečnost. Závislost jednotlivých sektorů kritické infrastruktury na IKT byla názorně popsána v publikaci [1] prostřednictvím finančních nákladů. Výpadek IKT může například zásadně ovlivnit poplachové zabezpečovací systémy nebo kamerové systémy (CCTV), které spadají do oblasti fyzické bezpečnosti. Naopak, výpadek prvků fyzické bezpečnosti může zapříčinit nepovolený přístup k hardwarovým prvkům informačního systému a tím pádem i ohrožení kybernetické bezpečnosti.

Z výše uvedených důvodu je nutné hledat způsoby, jakými by bylo možné tuto problematiku uchopit a klasifikovat. Proto byl zaveden koncept konvergované bezpečnosti v rámci, kterého jsou dílčí oblasti bezpečnosti sloučeny do jednoho celku. Hlavním cílem konvergované bezpečnosti je vytvoření specifického druhu bezpečnosti, který bude reflektovat souvztažnosti za účelem zvýšení efektivity detekce a řešení vzniklých bezpečnostních incidentů.

Základní principy, na nichž je konvergovaná bezpečnost postavena:

- konvergovaná bezpečnost se zajišťuje pro určitý (společný) referenční objekt,
- do konvergované bezpečnosti lze zahrnout pouze slučitelné druhy bezpečnosti,
- je žádoucí, aby zahrnuté druhy bezpečnosti chránily shodná nebo alespoň částečně shodná aktiva,
- dopady působení hrozeb nesmí být protichůdné a projevují se na aktivech referenčního objektu negativně,
- všechny hrozby můžou mít pro referenční objekt existenciální dopady.

V rámci tohoto článku je konvergovaná bezpečnost zaměřena na tři oblasti bezpečnosti, u nichž je předpokládán výskyt vzájemných vazeb. Jedná se o fyzickou bezpečnost, kybernetickou bezpečnost a provozní bezpečnost. Každá ze zmíněných oblastí bezpečnosti je zaměřena na ochranu aktiv z rozdílného pohledu. Kybernetická bezpečnost je zaměřena na ochranu kybernetického prostoru, který tvořen „hardwarovými“ a „softwarovými prostředky“. Kybernetická bezpečnost bývá často těžce uchopitelná, zejména díky své dynamické povaze a globální podstatě hrozeb v kybernetickém prostoru. Cílem kybernetické bezpečnosti je zajištění integrity, dostupnosti a důvěrnosti chráněných aktiv. Fyzická bezpečnost je historicky jednou z nejstarších druhů bezpečnosti. Jejím cílem je ochrana aktiv před hrozbami fyzického charakteru. K tomu využívá vlastnosti elektronických systémů nebo vlastnosti materiálů. Provozní bezpečnost je zaměřena zajištění cílové funkce organizace, tedy zajištění její kritických procesů, které jsou nutné pro dosažení toho, k čemu byla dotyčná organizace vytvořena. Tato oblast bezpečnosti je zaměřena na zajištění podmínek, které i v době krize zajistí naplnění cílů organizace.

2 Penalizační faktory

Hodnocení odolnosti, pomocí penalizačních faktorů, vycházející z konvergované bezpečnosti si klade za cíl vyhodnotit výskyt negativních událostí a kvantifikovat jejich vliv na vybrané druhy bezpečnosti. To se následně projeví na velikosti odolnost referenčního objektu pomocí jednoho čísla, které se mění v reálném čase.
Pro výpočet aktuální hodnoty odolnosti jsou využity statické a dynamické penalizační faktory. Statické penalizační faktory mají dlouhodobý charakter, přičemž není možné, aby se sami napravili. Mezi zástupce statických penalizačních faktorů řadíme například nesoulad s platnou legislativou nebo nedostatky v bezpečnostní politice. Soupis statických penalizačních faktorů určuje vstupní audit organizace. Z něho vycházejí obecné statické penalizační faktory, které jsou vybírány z velké množiny penalizačních faktorů pro fyzickou bezpečnost (FB), kybernetickou bezpečnost (KB) a provozní bezpečnost (PB), jež se mohou vyskytnout v rámci daného aktiva. Je využito vah, které se liší pro jednotlivá aktiva. Výsledné ohodnocení vyjadřuje reálnou

hodnotu statického penalizačního faktoru, tedy vynásobení výchozích penalizačních faktorů váhami. Index statické odolnosti aktiva představuje odolnost aktiva (100%) sníženou o statické penalizační faktory. Výpočet indexu statické odolnosti je proveden podle vzorce (1) zvlášť pro FP, KB, PB.

$$I_{ods} = 100 - \frac{\sum_{i=1}^{n} P_{si} * V_i}{P_{smax}} * 100 \quad (1)$$

I_{ods} – index statické odolnosti aktiva
P_{si} – i-tý aktivní statický penalizační faktor (obecný)
V_i – váha statického penalizačního faktoru vzhledem k danému aktivu (pohybuje se v rozmezí 1 – 5; implicitně 3)
P_{smax} – suma všech statických penalizačních faktorů pro dané aktivum

Dynamické penalizační faktory představují události, které se v čase mění. Jejich délka trvání je proměnná. U každého dynamického penalizačního faktoru je nutné nastavit čas, po který bude faktor ovlivňovat odolnost aktiva. Dynamický penalizační faktor lze vnímat například jako vylomení okna v chráněném objektu, výpadek elektrické energie v objektu, nebo skenování portů u PC. Pro výpočet finálního indexu odolnosti aktiva je nutný součet dynamických penalizačních faktorů aktivních v daném čase s indexem statistické odolnosti aktiva. Výpočet je realizován podle vzorce (2).

$$I_{od} = I_{ods} - \frac{\sum_{j=1}^{m} P_{dj} * V_j}{P_{dmax}} * I_{ods} \quad (2)$$

I_{ods} – index statické odolnosti aktiva
I_{od} – index odolnosti aktiva
P_{dj} – j-tý aktivní dynamický penalizační faktor (obecný)
V_j – váha dynamického penalizačního faktoru vzhledem k danému aktivu (pohybuje se v rozmezí 1 – 5; implicitně 3)
P_{dmax} – suma všech dynamických penalizačních faktorů pro dané aktivum

Index statické odolnosti aktiva i index dynamické odolnosti aktiva je kalkulován pro každou vybranou oblast bezpečnosti (FB, KB PB) v závislosti na penalizačních faktorech pro FB, KB, PB. Výpočet výsledné hodnoty konvergované bezpečnosti je realizován pomocí aritmetického průměru indexu odolnosti aktiva pro fyzickou bezpečnost, kybernetickou bezpečnost a provozní bezpečnost.

3 Vybrané metody pro kvantifikaci penalizačních faktorů

Výpočet indexů odolnosti aktiva je zásadně závislý na správném nastavení hodnot penalizačních faktorů. Pro jejich kvantifikaci lze využít řadu metod. Tato kapitola je zaměřena na popis metod, které byly využity pro nastavení penalizačních faktorů v rámci této studie.

3.1 Checklist v kombinaci s bodovou metodou

Podstata stanovení hodnoty penalizačních faktorů spočívá ve využití metody kontrolního seznamu (Checklist) v kombinaci s bodovou metodou. Tyto metody patří mezi základní nástroje v oblasti hodnocení rizik. Základ této metody je postaven na využití checklistu, kde namísto běžných odpovědí ano/ne, jsou uvedeny body. Hodnoty bodů jsou v checklistu jsou určeny pomocí bodové metody. Tato metoda představuje nejpoužívanější postup pro hodnocení rizik. Míra rizika je zde kombinací pravděpodobností výskytu rizika a možné závažnosti následku rizika. Výsledná hodnota penalizačního faktoru je určena pomocí checklistu, kde je proveden součet bodů kladně zodpovězených otázek. Výsledná penalizace vychází ze sumy hodnot kladných otázek pro daný penalizační faktor.

3.2 Multikriteriální hodnocení velikosti penalizace

Ukazatelem, vyjadřujícím výši penalizace penalizačního faktoru, je index penalizace P. Podstata metody je založena na stanovení výše penalizace na základě kritérií, které budou ohodnoceny v závislosti na charakteru penalizačního faktoru a jeho atributů. Za základní kritéria jsou zvoleny následující atributy a tím i indexy: index snížení odolnosti P_o, index rozsahu vlivu P_r a index naléhavosti P_k.

Indexem snížení odolnosti P_o je vyjádřena míra vlivu penalizačního faktoru na snížení odolnosti systému ochrany (jedná-li se o penalizační faktor, který odráží/vyjadřuje přímé narušení bezpečnosti, nebo faktor, který odráží nepřímé snížení odolnosti, spočívající ve vzniku příznivějších podmínek pro narušení

bezpečnosti). V rámci fyzické bezpečnosti se za přímé snížení odolnosti považuje spuštění detektoru narušení při narušení prostorové ochrany. Za nepřímé snížení odolnosti lze považovat déšť, neobnovenou revizi zařízení atd.

Další kritérium, index rozsahu vlivu P_r vyjadřuje rozsah působnosti faktoru z pohledu referenčního objektu (působí-li faktor lokálně nebo plošné necelý referenční objekt). Spuštění detektoru narušení prostorové ochrany je lokální. Déšť lze považovat za celoplošný jev.

Poslední kritérium vyjadřuje naléhavost (kritičnost) vlivu na změny odolnosti. V některých případech je rychlost stupňování působení škodícího účinku vysoká a je proto potřebné rychle reagovat. V jiných případech rychlost stupňování menší a systém ochrany lépe odolává. Kritičnost je nižší.

Každé kritérium je ve dvou stavech, ohodnocených velikostí 1 nebo 2/4.

$$P = P_o * P_r * P_k \tag{3}$$

P – index penalizace
P_o – index snížení odolnosti (přímé snížení = 4, nepřímé (podmíněné) snížení =1)
P_r – index rozsahu vlivu (celoplošný = 2, lokální =1)
P_k – kritérium naléhavosti / kritičnosti vlivu /odezvy (naléhavý = 2, nenaléhavý = 1)

3.3 Metoda založená na expertním odhadu

Pro daný referenční objekt jsou sestavovány penalizační faktory tak, aby reflektovaly specifika daného objektu. První fází je poznání daného referenčního objektu a vypsání penalizačních faktorů z pohledu kybernetické, fyzické i provozní bezpečnosti.

Těmto faktorům jsou dále přiřazeny hodnoty, které určují, jak moc je daný faktor pro objekt důležitý z pohledu bezpečnosti. Faktory jsou rozděleny do skupin:

I. Kritické faktory – jedná se o tu skupiny faktorů, které jsou nezbytné pro fungování referenčního objektu a jejich narušení by vedlo ke zničení objektu nebo k zastavení jeho činnosti. Hodnoty 100 – 80
II. Významné faktory – jedná se o skupinu faktorů, které významným způsobem ovlivňují provoz objektu. Jejich narušení by vedlo k výraznému omezení činnosti nebo výraznému narušení procesů. Hodnoty 79 - 50
III. Málo významné faktory – jedná se o faktory, které naruší provoz nebo činnost objektu, ale nezpůsobí významné následky. Hodnoty 49 - 20
IV. Zanedbatelné faktory – jedná se o skupiny faktorů, které mají zanedbatelný vliv na referenční objekt, ale mají potenciál při opakujícím se výskytu objekt poškodit nebo omezit jeho činnost. Hodnoty 19 – 1

Pomocí vah jsou penalizační faktory upraveny pro konkrétní aktivum. To se děje pomocí určení dopadu na dané aktivum. Váhy jsou rozděleny podle toho, jak moc velký dopad na aktivum faktor má z pohledu zajištění funkčnosti aktiva.

3.4 Fullerova metoda

Fullerova metoda je ve své podstatě bodovací metoda (typ metody párového srovnávání) a užívá se především v situacích, kdy pro velký počet kritérií je pro hodnotitele obtížné obodovat jednotlivá kritéria. Pro použití této metody postačí hodnotiteli, když dokáže rozhodnout o důležitosti kritérií vždy pouze mezi dvěma. Určuje se, které z kritérií má větší míru vlivu na odolnost aktiva. Taktéž lze při této metodě říci, že dvě kritéria jsou pro odolnost aktiva stejně důležitá.[2]

Při aplikaci této metody sestavujeme váhy pomocí tzv. Fullerova trojúhelníku. Trojúhelník má vždy $k - 1$ dvojřádků. V prvním řádku jsou všechny kombinace pro porovnání s prvním kritériem, v druhém kombinace pro porovnání s druhým kritériem, kromě té, která je v předchozím řádku, v každém dalším řádku jsou kombinace pro porovnání s dalším kritériem, které nejsou v předchozích řádcích. Každý řádek má tedy o 1 člen méně, než řádek předchozí.[3]

Princip této metody spočívá v tom, že hodnotiteli jsou postupně předkládány dvojice jednotlivých kritérií (tak, aby mu každá možná dvojice byla předložena právě jednou – viz výš popis Fullerova trojúhelníku), hodnotitel z této dvojice určí to kritérium, které je pro hodnocení odolnosti aktiva důležitější a tomu přidělí 1 bod. V případě, že jsou podle hodnotitele obě kritéria stejně důležitá, může přiřadit například 0,5 bodu oběma

kritériím. Na závěr se sečte počet bodů přidělený jednotlivým kritériím řádku a sloupci. Takto určíme, které kritéria mají na odolnost aktiva větší vliv a které menší. Určení konečné hodnoty penalizace se bude odvíjet v závislost od počtu kritérií a maximální penalizace, které chceme u nejdůležitějších kritérií dosáhnout.[2]

3.5 Modifikovaná Saatyho metoda

Pro výpočet hodnoty penalizačních faktorů je využito metody kvantitativního párového srovnávání (Saatyho metody). Tato metoda je původně využívána pro kvantifikaci vah jednotlivých proměnných. Avšak lze jí modifikovat a využít pro kvantifikaci penalizačních faktorů. Míra významnosti (závažnost dopadů) jednotlivých penalizačních faktorů lze mezi sebou vyjádřit pomocí určité číselné stupnice od 1 do 9, kde 1 představuje srovnání dvou kritérií (penalizačních faktorů), která jsou významově stejná (většinou se využívá, když se mezi sebou hodnotí dvě stejná kritéria) a hodnota 9 znázorňuje absolutní nevyváženost mezi kritérii (penalizačními faktory), kde jedno z nich je absolutně významnější než druhé. Na základě stupnice lze sestavit penalizační matici (Saatyho matice). Jednotlivé penalizační faktory jsou umístěny jak v úrovni řádků, tak v úrovni sloupců matice. Na diagonále matice je provedena komparace vždy stejných penalizačních faktorů. Mimo diagonálu je provedena komparace každého s každým penalizačním faktorem. Výsledná matice musí být co nejvíce konzistentní. To znamená, že jestliže faktor f_i je s_{ij} krát významnější jak f_j a zároveň f_j je s_{jk} krát významnější jak faktor f_k, pak z toho vyplývá, že prvně zmiňovaný faktor f_i bude také s_{ik} krát významnější jak faktor f_k.[4]

Další postup výpočtu penalizačních faktorů se však od Saatyho metody liší. Podle vztahu (4) je pro každý řádek Saatyho matice vypočten součet všech hodnot na dotyčném řádku matice. Aby byl reflektován celkový počet penalizačních faktorů v penalizační matici, tak je každý součet na řádcích podělen odmocninou z celkového počtu, podle vzorce (5).

$$f_i = \begin{bmatrix} \sum_{j=1}^{n} s_{1j} \\ \sum_{j=1}^{n} s_{2j} \\ \dots \\ \sum_{j=1}^{n} s_{ij} \end{bmatrix} \tag{4}$$

$$s_i = \frac{f_i}{\sqrt{n}} \tag{5}$$

Odmocnina z celkového počtu hodnocení byla zakomponována do vzorce z důvodu regulace absolutní hodnoty penalizačního faktoru, který by při velkém počtu hodnocení (velký počet prvků v penalizační matici) nabýval velmi vysokých hodnot, které by záviseli především na dimenzi matice. Využitím prostého počtu všech hodnocení by bylo dosaženo jen prostého aritmetického průměru, který by dosahoval jen velmi malých hodnot. Využitím odmocniny ze sumy ze všech hodnocení je dosaženo rostoucího penalizačního faktoru.

3.6 Párového srovnání rozšířené o ELO rating

Jedná se o statistické ohodnocení, které bylo vyvinuto pro ohodnocení hráčů v jakékoliv hře. Zde je srovnána výkonost jednotlivých hráčů, které může být provedeno nejenom na konci hry, ale i v průběhu hry. Tato metoda je využívána nejenom v oblasti her, ale i v jiných oblastech jako je například finančnictví. [5]

Vlastní výpočet se provádí na základě 2 metod a to „Průběžná metoda“ a „Periodická metoda“. Druhá zmíněná metoda je vhodnější pro „hráče“ (kritéria), kteří ještě ELO hodnocení nemají a výsledné hodnocení se počítá na základě výsledku v sérii „partií“ (porovnání) s „hráčem“, který již ELO má. [5]

Pro potřeba penalizací bude vhodnější využití první metody – průběžné, která je založena na rozdílu ELO hodnocení mezi 2 „hráči“. Vychází se z pravděpodobnostní tabulky.

Na začátku je všem přiřazena referenční hodnota (např. 1000) a provede se klasické párové porovnání. Za každou „výhru“ je kritériu přidělen bod, za remízu 0,5b a „prohra“ je bez bodového přídělu. Výsledné hodnocení se počítá podle následujícího vzorce:

$$R_n = R_o + K.(W - W_e) \tag{6}$$

Rn – nové hodnocení
K – koeficient rozvoje (v našem případě se může jednat o kritičnost nebo dopad)
W – dosažený počet bodů
We – očekávaný počet bodů

3.7 Metfesselova alokace

Jedná se o metodu rozhodování, která je založena seskupování faktorů do dílčích skupin. Je využito vah kritérií, které reprezentují procentuální podíl dílčího kritéria na kritéria vyšší úrovně. Využívá se stromové struktury pro reprezentaci vybraných kritérií. Na pomyslném vrcholu jsou dílčí kritéria první úrovně, které se dále rozdělují/větví až se dosáhne základních kritérií. Každé kritérium musí být bezezbytku rozděleno na kritéria nižší úrovně. Stanovení vah jednotlivých kritérií je periodický proces, při němž musí být zachována podmínka, která definuje, že každý součet vah kritérií ve větvení musí být roven jedné. Jinými slovy lze říci, že váhy v rámci každé úrovně mohou mít různé hodnoty vah, avšak jejich součet se musí rovnat 1 v rámci dané úrovně. V rámci řešené problematiky je vyhodnocena závažnost jednotlivých skupin penalizačních parametrů, jejichž součet je roven 1. Následně se určí závažnost dílčích penalizačních faktorů v rámci každé skupiny, přičemž součet v rámci každé skupiny penalizačních faktorů je 1. Výsledná hodnota penalizačního faktoru je získána vynásobením váhy penalizačního faktoru s váhou danou pro skupiny penalizačních faktorů.[6]

3.8 Stupnice hodnocení

Podstata metody je založená na stanovení stupnice hodnocení a slovním popsání jednotlivých dopadů na celý systém. Na základě této stupnice bude docházet k hodnocení za pomocí třech vědeckých týmů. Následně se hodnoty zprůměrují a můžeme nastavit váhy pro různé skupiny jinak (podle jejich odbornosti). Ze zprůměrovaných hodnot se nastaví hodnota penalizace pro daný penalizační faktor. Je potřebné brát v úvahu: Opakovaný penalizační faktor v určitém časovém intervalu. Zvýšení váhy penalizace v návaznosti na další faktory, mohou být různé pro jiné druhy objektů – váha penalizace ve vazbě na kategorii objektu. Penalizační faktor by měl být stanoven na základě významu/dopadu pro objekt.

Postup určení penalizace:

1. Sestavení stupnice intervalů, ve kterém se penalizace bude pohybovat,
2. Popsat dopady daného penalizačního faktoru na této stupnici.
3. Ověřit způsobilost stupnice.
4. Upravit stupnici podle zjištění a podle faktorů násobení.
5. Stanovení expertní týmy
6. Hodnotit dané penalizační faktory a nastavit hodnoty.

4 Metody vědeckého výzkumu

První fáze kvantifikace penalizačních faktorů zahrnovala výběr expertů, kteří pomocí vybraných metod ohodnotili penalizační faktory. Všechny vybrané metody byly rozděleny a využity pro kvantifikaci penalizačních faktorů. Rozpětí získaných výsledků bylo rozdílné v závislosti na použité metodě. Z tohoto důvodu bylo nutné provést normalizaci výsledku pro jejich budoucí vzájemnou komparaci. Normalizace hodnot penalizačních faktorů podle dílčích metod byla provedena podle následujícího vztahu (7) pro rozsah od 1 do 10.

$$x^* = \frac{x - min_v}{max_v - min_v}(nová\_max_v - nová\_min_v) + nová\_min_v \quad (7)$$

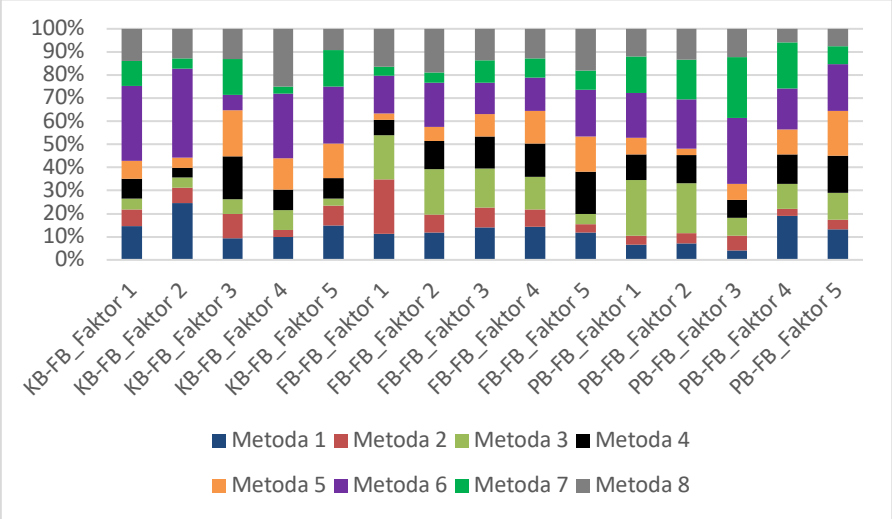
Pro porovnání všech penalizačních faktorů v rámci zvoleného příkladu v závislosti na jednotlivých metodách byl zvolen následující postup. Bylo vytvořeno 8 hodnot podle 8 zvolených metod pro každý penalizační faktor. Následně byl vypočten medián pro každý penalizační faktor z 8 hodnot pro sledované oblasti bezpečnosti. Od každé hodnoty penalizačního faktoru získané pomocí dílčí metody, byl odečten získaný medián. Následně, pomocí absolutní hodnoty byla vypočtena odchylka, která díky své velikosti vypovídá nakolik dotyčný penalizační faktor, vybočuje oproti ostatním (vyšší číslo značí větší odchylku) viz. vztah (8). Na závěr jsou výsledky pro jednotlivé penalizační faktory sečteny, přičemž je vyhodnocena nejefektivnější metoda podle velikosti vypočteného skóre.

$$|medián - penalizační\ faktor| \quad (8)$$

5 Výsledky

Pro demonstraci představené metodiky výběru metod pro kvantifikaci penalizačních faktorů byly vybrány penalizační faktory z oblasti fyzické bezpečnosti pro referenční objekt hlavního stavědla železniční

stanice. Pomocí zmíněných metod (8 metod) byla kvantifikována míra vlivů penalizačních faktorů (FB) na vybrané oblasti bezpečnosti (FB, KB, PB). Výsledné hodnoty byly normalizovány. Přehled těchto hodnot lze vidět v obr. 1. Výčet metod odpovídá metodám popsaných v kapitole 4. Tedy metod 1 odpovídá metodě popsané v kapitole 4.1, metod 2 odpovídá metodě popsané v kapitole 4.2 atd.



Obr. 1: Souhrnný graf penalizačních faktorů pro fyzickou bezpečnost v závislosti na metodách pro kvantifikaci penalizačních faktorů pro jednotlivé oblasti bezpečnosti (FB, KB, PB).

Podle grafu, který je zobrazen v obr. 1, lze vydedukovat, že bylo využito pěti penalizačních faktorů spadající do oblasti fyzické bezpečnosti. Jejich výčet je následující: neexistuje automatické rozpoznávání zařízení (BYOD), Neexistující pravidla pro tvorbu hesel, skenování portů zařízení v interní síti, zvýšená teplota v serverovně, výpadek IDS. Pro každý penalizační faktor je vypočten jaký má vliv na dílčí oblasti bezpečnosti (FB, KB, PB). Z tohoto důvodu vniklo 15 hodnot penalizačních faktorů, 5 pro každý druh bezpečnosti. Výsledné hodnoty odchylek pro jednotlivé penalizační faktory jsou obsaženy v tab. 1.

	Metoda 1	Metoda 2	Metoda 3	Metoda 4	Metoda 5	Metoda 6	Metoda 7	Metoda 8	Medián
Faktor 1	1,001	0,542	1,142	0,242	0,452	4,858	0,242	0,858	2,142
Faktor 2	4,388	0,273	0,327	0,327	0,273	7,673	0,327	1,673	1,327
Faktor 3	0,371	0,200	0,800	1,000	1,270	0,800	0,585	0,200	1,800
Faktor 4	0,171	1,971	0,171	0,171	1,380	6,029	1,971	5,029	2,971
Faktor 5	0,929	1,129	2,929	1,129	0,946	4,071	1,225	0,929	3,929
Faktor 6	1,071	4,071	2,271	3,129	4,724	1,071	4,236	1,071	5,929
Faktor 7	0,086	1,714	2,786	0,086	2,248	2,486	2,822	2,486	4,514
Faktor 8	0,286	2,800	2,000	0,200	2,322	0,000	2,154	0,000	8,000
Faktor 9	0,000	4,800	0,000	0,000	0,000	0,000	4,154	1,000	10,000
Faktor 10	0,727	4,413	4,113	2,187	0,727	2,987	2,243	1,987	6,013
Faktor 11	2,086	3,200	5,200	0,200	1,783	3,200	1,738	0,200	4,800
Faktor 12	2,086	3,200	3,400	0,200	3,800	3,200	1,738	0,200	4,800
Faktor 13	0,900	0,300	0,000	0,000	0,157	5,100	4,638	1,100	1,900
Faktor 14	3,621	4,350	0,450	0,450	0,545	3,050	4,050	2,950	5,950
Faktor 15	0,343	3,343	0,343	1,457	2,745	3,057	1,866	1,943	4,943
Suma	18,065	36,307	25,932	10,778	23,372	47,583	33,991	21,626	

Tab. 1: Odchylky penalizačních faktorů (FB) pro jednotlivé metody.

6 Závěr

V rámci článku byla představena metodika pro výběr vhodné metody z pohledu kvantifikace penalizačních faktorů. Ve výsledné množině bylo zahrnuto 8 metod. Výsledky pro jednotlivé penalizační parametry byly normalizovány pro jednotlivé oblasti bezpečnosti. Pomocí součtu odchylek pro každou metodu pro všechny penalizační faktory bylo docíleno výběru nejvhodnější metody. Podle výsledků lze zvolit nejlepší metodu, která je podle výsledného indexu metoda 4 (Fullerova metoda). Ta je následovaná metodou 1 s mírným náskokem. Navržená metodologie postupu při výběru vhodných metod má však svá úskalí. Účastníci vybraní pro hodnocení podle metod musejí býti experty v dané oblasti bezpečnosti, kterou budou hodnotit. Při hodnocení větším množstvím „laiků" může dojít k posunutí mediánu do takové míry, že poté přesnější hodnocení expertů bude identifikováno jako nevyžádaná odchylka oproti většině hodnocení „laiků". Také je nutné, aby každý expert provedl výpočet pomocí všech metod v rámci své odbornosti z důvodu statistického porovnání mezi dotčenými metodami.

Tento článek byl financován prostřednictvím Interní Grantové Agentury (IGA/FAI/2019/002) a podporován projektem VI20172019054 „Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti" podporovaný Ministerstvem vnitra České republiky v letech 2017-2019.

Literatura

[1] MACAULAY, Tyson. Critical infrastructure: understanding its component parts, vulnerabilities, operating risks, and interdependencies. CRC press, 2016.

[2] KLICNAROVÁ, Jana. Vícekriteriální hodnocení variant – metody [online]. České Budějovice, 2010 [cit. 2019-03-05]. Dostupné z: http://home.ef.jcu.cz/~janaklic/oa_zsf/VHV_II.pdf. Jihočeská Univerzita v Českých Budějovicích.

[3] SEKNIČKOVÁ, Jana. Vícekriteriální hodnocení variant – VHV [online]. Praha [cit. 2019-03-05]. Dostupné z: http://jana.kalcev.cz/vyuka/kestazeni/EKO422-Vahy.pdf. Vysoká škola ekonomická v Praze.

[4] BOROVCOVÁ, Martina. Metody vícekriteriálního hodnocení variant a jejich využití při výběru produktu finanční instituce. cit, 2017, 11-19.

[5] ŠŤASTNÁ, Lucie. Rating hráčů v kolektivních hrách [online]. Brno, 2015 [cit. 2019-03-05]. Dostupné z: https://is.muni.cz/th/sojcw/Rating_hracu_v_kolektivnich_hrach.pdf. Bakalářská práce. Masarykova Univerzita.

[6] HÉŽA, Lukáš. Metody stanovení vah kritérií v modelech vícekriteriálního rozhodování [online]. Olomouc, 2011 [cit. 2019-03-06]. Dostupné z: https://theses.cz/id/o777ux/. Bakalářská práce. Univerzita Palackého v Olomouci.