Ing. Ondřej Bos
Fakulta bezpečnostního managementu PA ČR v Praze
Katedra krizového řízení
Dr. Zdeněk Kovařík, CSc.
Oddělení vědy a výzkumu PA ČR v Praze

Identifikace a faktorové uspořádání hrozeb pro kontinuitu činností organizací veřejné správy v ČR

Úvod

Řízení kontinuity činností je třeba chápat jako integrální součástí systému managementu organizace, jehož hlavním úkolem je vytvoření stabilního prostředí pro plnění cílů organizace a podmínek pro minimalizaci dopadů souvisejících s případnými provozními výpadky.

Význam řízení kontinuity činností se projevuje zejména v těch oblastech a odvětvích, jejichž fungování je citlivé na neplánované a nepředpokládané události, kde může v důsledku výpadků a nefunkčností docházet ke značným negativním dopadům.

K těmto oblastem patří bezesporu i výkon veřejné správy, respektive plynulý chod institucí zajišťujících agendu veřejné správy (dále jen „organizace veřejné správy“). V České republice v současné době není řízení kontinuity činností veřejné správy systémově nastaveno a lze tak předpokládat, že přístup organizací veřejné správy k této metodě řízení je subjektivní a značně se liší, případ od případu.

Proto proběhl v roce 2017 empirický výzkum mezi zástupci organizací veřejné správy v České republice s následujícími cíli:

- identifikovat aktuální úroveň připravenosti organizací veřejné správy na situaci, která může zásadně ovlivnit jejich funkcionalitu a kontinuitu výkonu veřejné služby v případě neočekávaných a neplánovaných výpadků;
- porovnat představy a požadavky s obecnými standardy systému řízení kontinuity činností;
- posoudit vnímání současných a budoucích hrozeb pro fungování organizací veřejné správy.

Cílem tohoto článku je poskytnout základní evidenci pro posouzení relevance následujících **výzkumných předpokladů**:

1. *Vnímání hrozeb pro zajištění kontinuity činností organizací veřejné správy v České republice se shoduje s globálním průzkumem, a to jak mezisektorově, tak s přihlédnutím k oblasti veřejné správy;*
2. *Vnímání hrozeb pro zajištění kontinuity činností organizací veřejné správy v České republice se shoduje ze současného pohledu a ze střednědobé (tříleté) perspektivy;*
3. *Ve výzkumu použitá sada 29 hrozeb nepřekročí při redukci proměnných do adekvátních společných druhových oblastí celkem pět faktorů.*

Forma výzkumu a technika sběru dat

Sběr dat pro zjištění úrovně řízení kontinuity činností v organizacích působících ve veřejné správě v České republice proběhl formou dotazníkového šetření, přičemž respondenti, kteří tvořili výběrový soubor (na základě dostupnosti), byli manažeři organizací veřejné správy a specialisté v oblasti krizového řízení.

Pro oslovení respondentů byl zvolen online dotazníkový formulář vytvořený službou pro přípravu a hodnocení dotazníkových šetření specializovaných pro sociologické výzkumy http://www.i-Dotaznik.cz.

Struktura dotazníku byla následující:

Úvod: seznámení respondentů s cílem dotazníkového šetření, doložka o zachování anonymity respondentů při hodnocení výstupů, definice základních pojmů používaných v dotazníku;

Identifikační znaky respondenta: pracovní pozice, obor působnosti, délka praxe v oboru, typ organizace veřejné správy, kterou respondent zastupuje;

Úroveň řízení kontinuity činností v organizaci: popis systému řízení kontinuity činností, prioritizace činností/služeb při obnově po výpadku, zálohování a formy strategie obnovy.

Hrozby pro fungování organizace: významnost vybraných kategorií dopadů (reputační, finanční, legislativní, kvalita služby, environmentální, mezinárodní, ohrožení zdraví a života) nefunkčnosti organizace, vnímání závažnosti vybraných hrozeb pro fungování organizace v současnosti a v horizontu 3 let.

Otázky v dotazníku byly formulovány jako uzavřené, s výjimkou jedné polouzavřené otázky v části identifikace respondenta.

Struktura respondentů a organizací, které se zúčastnily dotazníkového šetření, je součástí přílohy k tomuto příspěvku. Populační soubor, na který se výzkum zaměřil, tvořili manažeři a odborní pracovníci v oblasti bezpečnosti, krizového řízení a řízení organizace.

Komparace vnímání hrozeb pro kontinuitu činností organizace

Jedním z hlavních iniciátorů, které generují a určují zájem organizace o zavedení i rozvoj systému řízení kontinuity, je subjektivní vnímání potenciálních hrozeb a jejich působení na zájmy organizace. Co je to však hrozba a jak ji je potřeba vnímat z pohledu řízení kontinuity činností?

Existuje celá řada definicí pojmu „hrozba“; podle Zemana je hrozba „primární, vnější fenomén, který může nebo chce poškodit konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a toho, jak si danou hodnotu ceníme. Hrozba může být jevem přírodním, definovaným fyzikálně – takovou hrozbu nazýváme hrozbou neintencionální. Realizace neintencionální hrozby je stochastické povahy. Zcela jiného původu je hrozba působená či zamýšlená činitelem nadaným vůlí,

úmyslem (hrozba intencionální) – zamýšlí ji, připravuje, spouští a realizuje lidský jedinec nebo kolektivní aktér.“[1]

Mezinárodní norma ISO 22300:2012 dále definuje, že hrozba vyjadřuje „kombinaci rizik, následky těchto rizik a pravděpodobnost, že k negativním účinkům dojde“ a dále, že „možné důsledky nežádoucí události mohou vést k poškození jedinců, systému či organizace, prostředí nebo společnosti“.[2]

V rámci dotazníku byli respondenti požádáni, aby ohodnotili svůj postoj k 29 konkrétním hrozbám v současnosti (obr. 1) a ve výhledu následujících 3 let; výběr typových hrozeb je odvozen z celosvětového průzkumu úrovně řízení kontinuity ve vztahu k modelovým hrozbám Horizon Scan Report, který každoročně organizuje The Business Continuity Institute.[3] V roce 2017 se průzkumu zúčastnilo 726 organizací ze 79 zemí; instituce veřejné správy reprezentovaly 13 % respondentů a byly tak 3. nejvíce zastoupeným odvětvím. Celkový výsledek tohoto průzkumu vnímání hrozeb pro provoz organizací pro rok 2017 a detailní hodnocení tří největších hrozeb pro veřejnou správu je uveden na obr. 2.

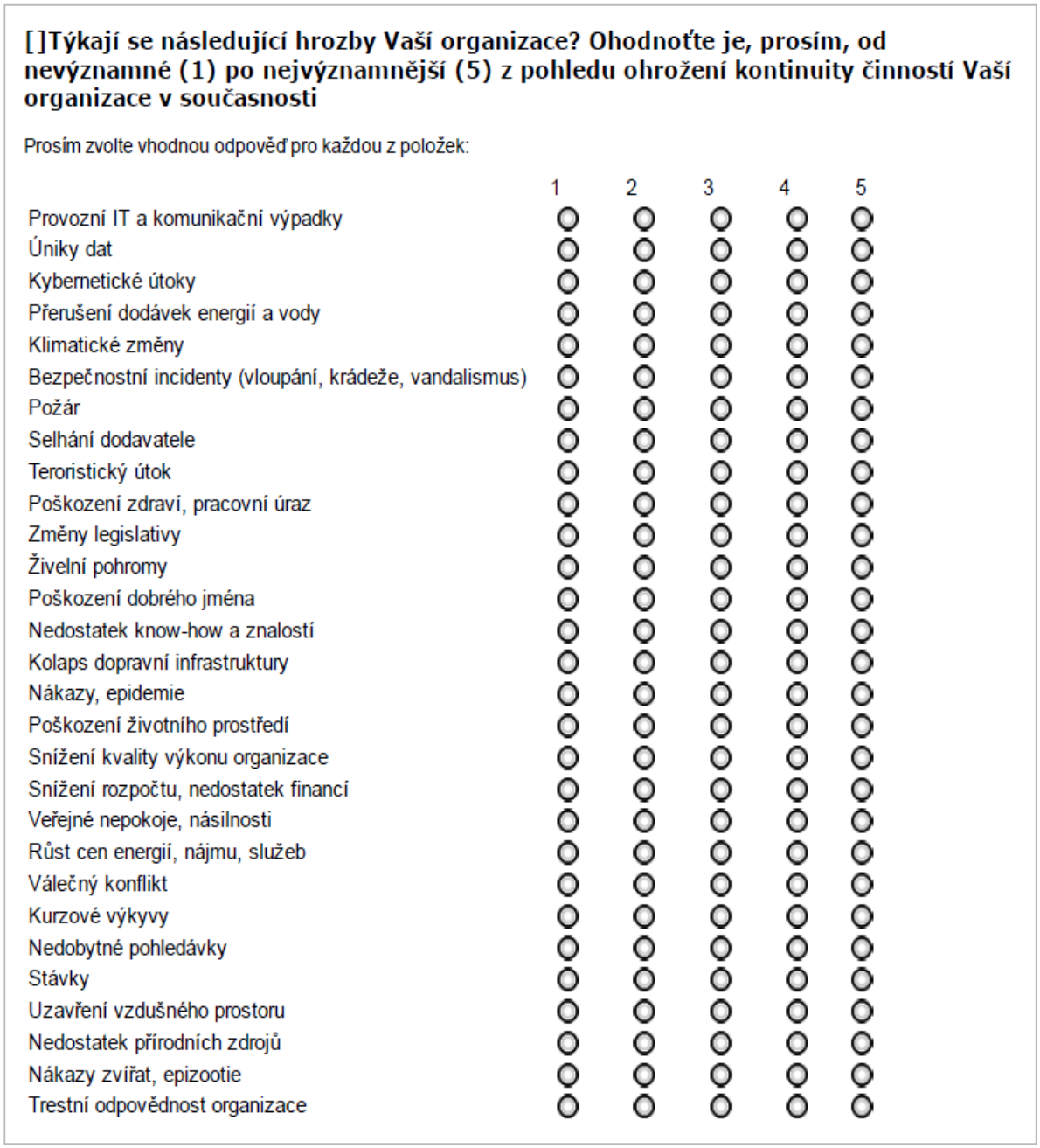
Oproti uvedenému průzkumu jsme pro hodnocení hrozeb připravili pětistupňovou škálu od nevýznamné (1) až po nejvýznamnější (5). Možnost „neaplikovatelné“ (0) nebyla v průzkumu přímo uvedena, aby při hodnocení nedocházelo ke zkreslení celkového výsledku; nicméně respondenti měli možnost nehodnotit u hrozby relevanci.

[1] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

[2] ISO 22300:2012 Societal Security – Terminology patří do řady norem upravující principy systému řízení kontinuity činností. Další definice pojmu hrozba, které obsahují řady mezinárodních norem ISO, nicméně nejsou relevantní z pohledu řízení kontinuity činností naleznete pomocí prohlížeče ISO dostupného na odkazu https://www.iso.org/obp/ui.

[3] *The Business Continuity Institute: Research Reports* [online]. [cit. 2017-08-03]. Dostupné z: http://www.thebci.org/index.php/resources/bci-research-reports.

Obr. 1 Struktura části dotazníku, týkající se hodnocení hrozeb pro kontinuitu provozu organizace



[]Týkají se následující hrozby Vaší organizace? Ohodnoťte je, prosím, od nevýznamné (1) po nejvýznamnější (5) z pohledu ohrožení kontinuity činností Vaší organizace v současnosti

Prosím zvolte vhodnou odpověď pro každou z položek:

	1	2	3	4	5
Provozní IT a komunikační výpadky	○	○	○	○	○
Úniky dat	○	○	○	○	○
Kybernetické útoky	○	○	○	○	○
Přerušení dodávek energií a vody	○	○	○	○	○
Klimatické změny	○	○	○	○	○
Bezpečnostní incidenty (vloupání, krádeže, vandalismus)	○	○	○	○	○
Požár	○	○	○	○	○
Selhání dodavatele	○	○	○	○	○
Teroristický útok	○	○	○	○	○
Poškození zdraví, pracovní úraz	○	○	○	○	○
Změny legislativy	○	○	○	○	○
Živelní pohromy	○	○	○	○	○
Poškození dobrého jména	○	○	○	○	○
Nedostatek know-how a znalostí	○	○	○	○	○
Kolaps dopravní infrastruktury	○	○	○	○	○
Nákazy, epidemie	○	○	○	○	○
Poškození životního prostředí	○	○	○	○	○
Snížení kvality výkonu organizace	○	○	○	○	○
Snížení rozpočtu, nedostatek financí	○	○	○	○	○
Veřejné nepokoje, násilnosti	○	○	○	○	○
Růst cen energií, nájmu, služeb	○	○	○	○	○
Válečný konflikt	○	○	○	○	○
Kurzové výkyvy	○	○	○	○	○
Nedobytné pohledávky	○	○	○	○	○
Stávky	○	○	○	○	○
Uzavření vzdušného prostoru	○	○	○	○	○
Nedostatek přírodních zdrojů	○	○	○	○	○
Nákazy zvířat, epizootie	○	○	○	○	○
Trestní odpovědnost organizace	○	○	○	○	○

Zdroj: vlastní

Obr. 2 Hodnocení hrozeb pro provoz organizacemi, včetně hodnocení tří nejvýznamnějších hrozeb podle hlavních ekonomických sektorů

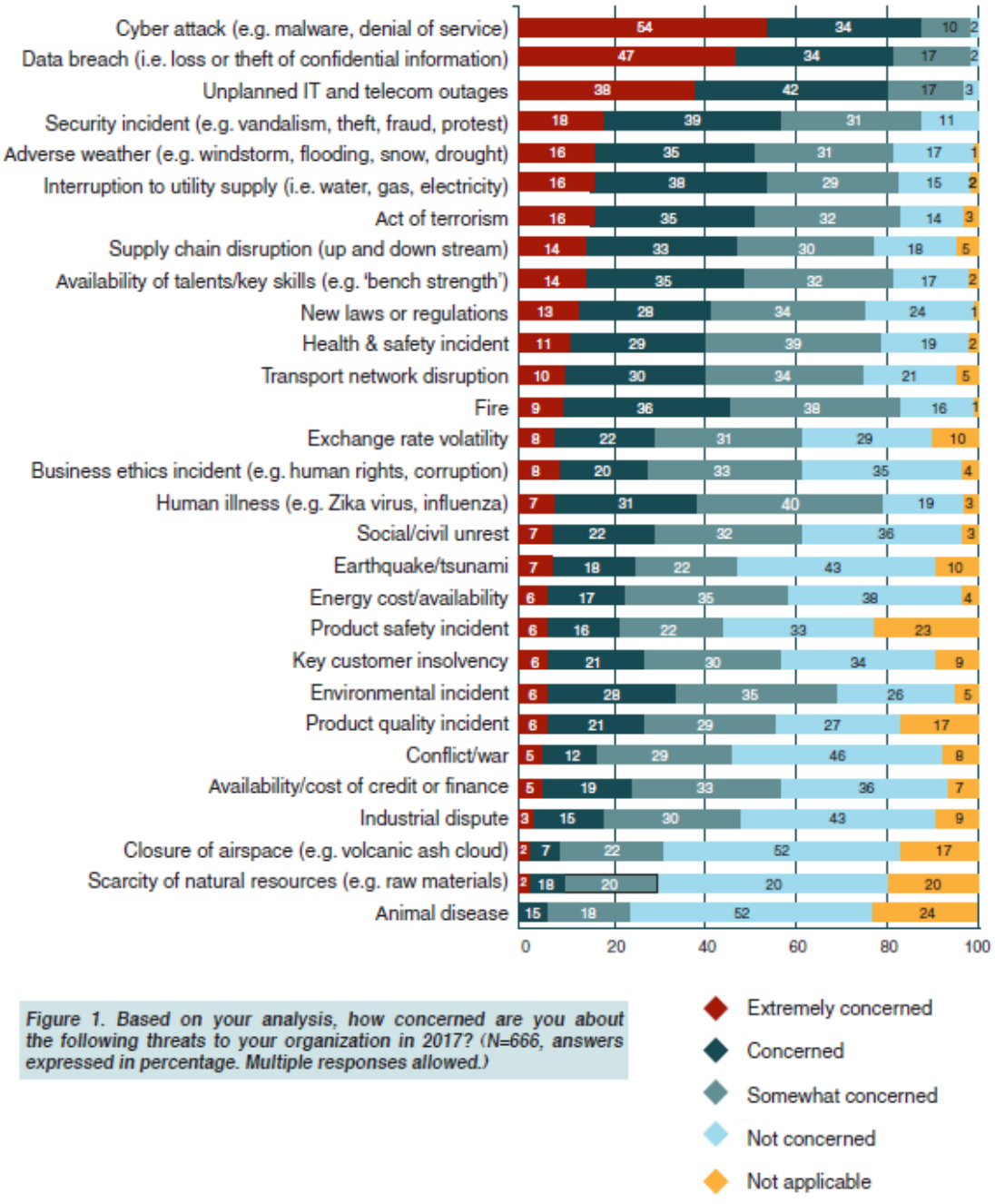


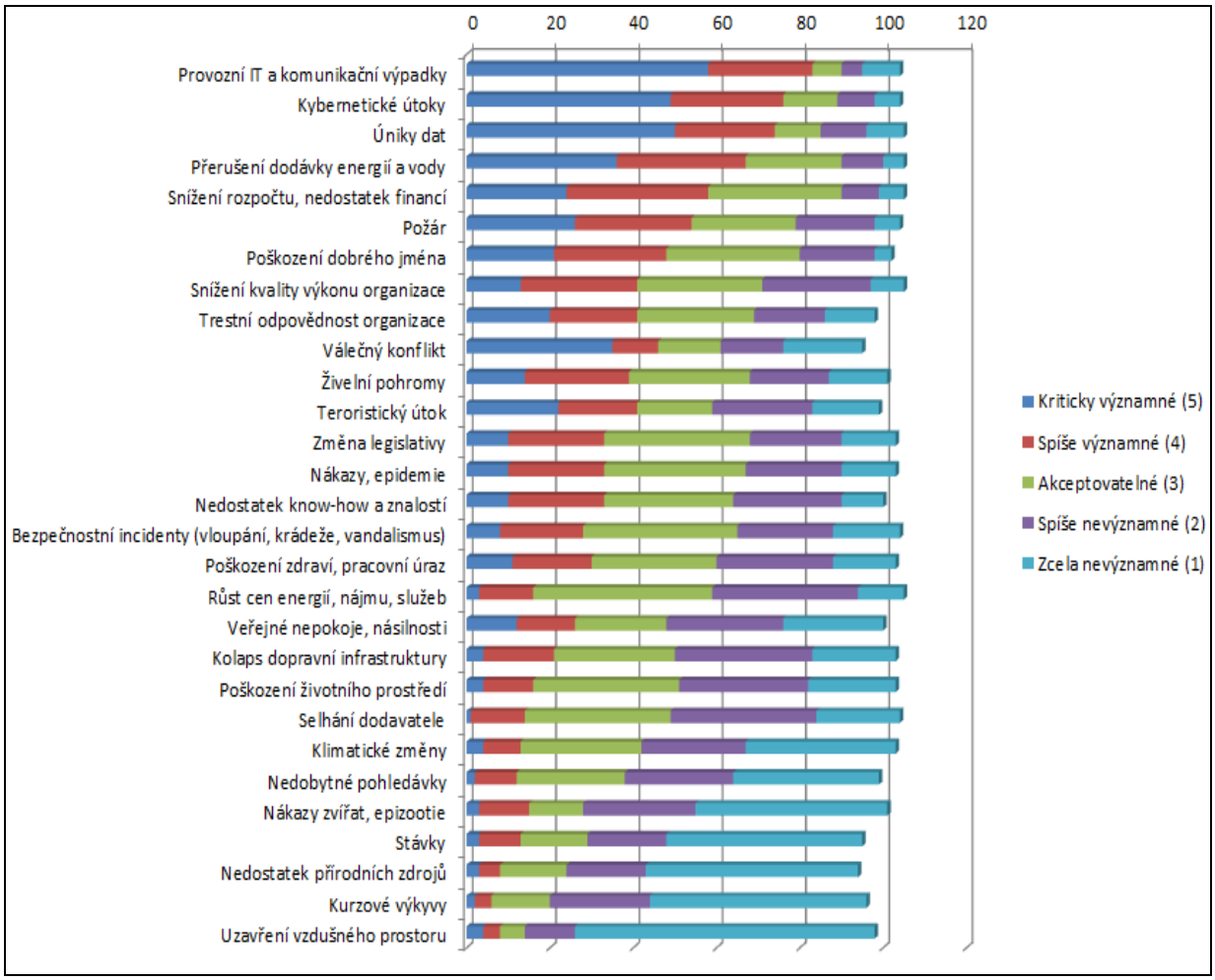
Figure 1. Based on your analysis, how concerned are you about the following threats to your organization in 2017? (N=666, answers expressed in percentage. Multiple responses allowed.)

	Financial & Insurance	Professional services	Public administration & defence	IT & Communications
Top three threats	Cyber attack (65%) Data breach (61%) Unplanned IT and telecom outages (46%)	Cyber attack (50%) Data breach (44%) Unplanned IT and telecom outages (34%)	Cyber attack (49%) Data breach (35% Unplanned IT and telecom outages (29%)	Cyber attack (68%) Data breach (56%) Unplanned IT and telecom outages (53%)

Zdroj: Horizon Scan Report 2017, The Business Continuity Institute, https://www.thebci.org/knowledge/horizon-scan-report-2017.html

Dalším rozdílem je použitá metrika pro hodnocení. **Horizon Scan Report** posuzuje závažnost hrozeb dle procenta respondentů, kteří ohodnotili svůj vztah tak, že se dané hrozby „zvláště obávají“ a „obávají“. V průzkumu hrozeb pro organizace veřejné správy v České republice jsou brány v potaz všechny úrovně významnosti a je jim přiřazena odpovídající váha.

Obr. 3 Aktuální hodnocení hrozeb pro kontinuitu provozu z pohledu organizací veřejné správy v České republice



Ověřovaný výzkumný předpoklad je v dané souvislosti následující: *„Vnímání hrozeb pro zajištění kontinuity činností organizací veřejné správy v České republice se shoduje s globálním průzkumem, a to jak mezisektorově, tak s přihlédnutím k oblasti veřejné správy.“*

Daný výzkumný předpoklad nelze zamítnout.

Zdůvodnění: Ke třem nejvýznamnějším hrozbám v hodnocení organizacemi veřejné správy České republiky i v hodnocení globálního se shodně objevují tyto typové hrozby: kybernetické útoky (1. místo v Horizon Scan, 2. místo v ČR), úniky dat (2. místo v Horizon Scan, 3. místo v České republice), provozní IT a komunikační výpadky (3. místo v Horizon Scan, 1. místo v České republice).

Obdobně je tomu i u vnímání nejméně závažných hrozeb, především uzavření vzdušného prostoru (27. pozice v Horizon Scan, 29. pozice v České republice),

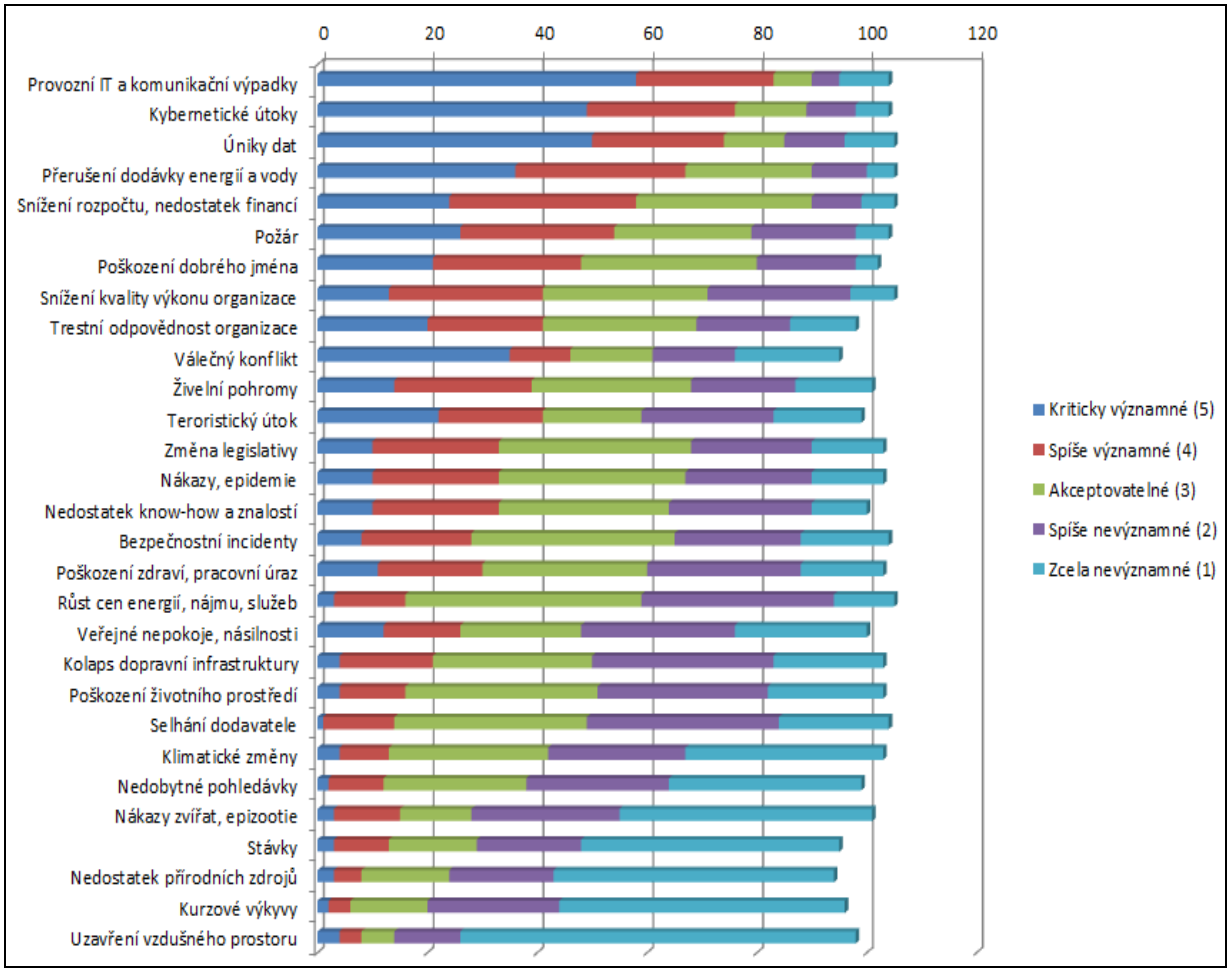
pracovněprávní spor/stávka (26. místo v Horizon Scan, 26. místo v České republice), nedostatek přírodních zdrojů (28. pozice v Horizon Scan, 27. místo v České republice).

Oproti tomu, u některých položek můžeme pozorovat výrazné odlišnosti. Markantní odchylky se týkají např. selhání dodavatele (8. místo v Horizon Scan, 22. místo v České republice) bezpečnostní incidenty (4. pozice v Horizon Scan, 16. místo v v), nedostatek know-how a znalostí (9. v Horizon Scan, 15. v ČR) nebo válečný konflikt (24. v Horizon Scan, 10. v České republice).

Mezičasové vnímání hrozeb pro kontinuitu činností organizace

Význam řízení kontinuity činností se výrazně projevuje zejména v obdobích výkyvů, dynamických změn a nepředvídatelného vývoje v oblasti sociální, ekonomické, technologické aj. Změny prostředí a nové hrozby pro organizace jsou z praktického pohledu jednou z nejvýraznějších výzev pro hledání rezerv v odolnosti procesů organizace. Řadu potenciálních významných hrozeb (které v současnosti představují marginální téma nebo nejsou řešeny vůbec) je však možné predikovat, např. na základě připravovaných legislativních změn, monitoringu a analýz hrozeb, strategického plánování nebo přechozích zkušeností managementu.

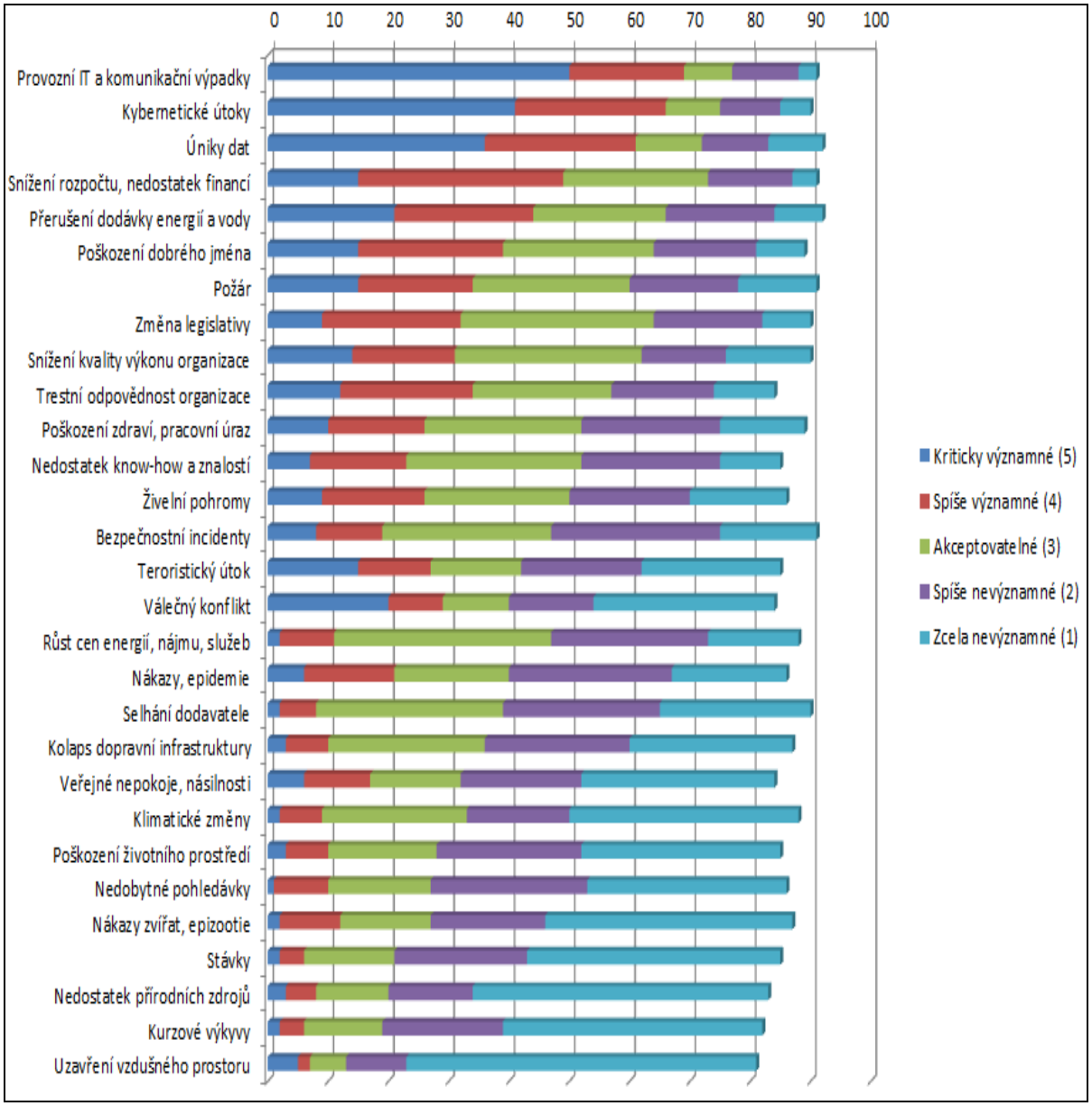
Obr. 4.1 Vnímání hrozeb pro fungování organizace z aktuálního pohledu



Zdroj: vlastní

Další část výzkumu byla proto zaměřena na mezičasové srovnání vnímání hrozeb v rámci veřejné správy České republiky, přičemž respondenti byli dotázáni, jaký vývoj v této souvislosti očekávají v tříletém horizontu. Cílem je především zkoumat, zda a jak se ve vnímání respondentů odráží perspektivy změny rizikovosti některých hrozeb.

Obr. 4.2 Vnímání hrozeb pro fungování organizace ve tříletém horizontu



Zdroj: vlastní

Ověřovaný výzkumný předpoklad v dané souvislosti zní: *„Vnímání hrozeb pro zajištění kontinuity činností organizací veřejné správy v České republice se shoduje ze současného pohledu a ze střednědobé (tříleté) perspektivy.“*

Daný výzkumný předpoklad nelze zamítnout.

Odůvodnění: při porovnání hodnot vnímání hrozeb z tříleté perspektivy lze konstatovat, že pozice nejvýznamnějších (provozní výpadky informačních

technologií, komunikační výpadky, kybernetické útoky, úniky dat) i nejméně významných (stávky, nedostatek přírodních zdrojů, kurzové výkyvy, uzavření vzdušného prostoru) hrozeb jsou shodné. K největšímu poklesu významnosti dochází u hodnocení válečného konfliktu (10. místo aktuálně, 16. pozice v tříletém horizontu), naopak nejprogresivnější hodnocení zaznamenaly hrozby pracovních úrazů (17. příčka aktuálně, 11. místo v tříletém horizontu) a legislativních změn (13. místo v současnosti, 8. pozice v tříletém horizontu).

Kvantitativní hodnocení hrozeb prostřednictvím explorační faktorové analýzy

Třetí ověřovaný výzkumný předpoklad je zaměřen na posouzení vzájemných vazeb mezi jednotlivými hrozbami a na možnost redukce datového souboru.

S ohledem k počtu respondentů a proměnných byla při hodnocení relevance uvedených hrozeb využita explorační faktorová analýza (dále jen EFA). V našem případě jsme použili EFA, která byla provedena volně dostupným programem Factor, verze 10.5.03. V souladu se standardním nastavením programu Factor 10.5.03 jsme použili pro extrakci faktorů metodu neválených nejmenších čtverců (Unweighted Least Squares, ULS) a k dosažení jednoduché faktorové struktury metodu faktorové rotace PROMIN.[1] Šikmá rotace je podle odborníků pravděpodobně více přiměřená většině praktických situací.

Pro určení dostačujícího počtu faktorů bylo použito Kelleyho kritérium pro stanovení maximální hodnoty průměrných standardizovaných reziduí. Jedná se o poměrně kvalitní postup, který je založen na porovnání navrženého faktorového modelu s originálními daty. V případě, že odmocnina střední hodnoty reziduí je nižší než očekávaná hodnota dle Kellyho kritéria, lze považovat počet extrahovaných faktorů za dostatečný. Jinak řečeno, při dosažení nízké hodnoty reziduí lze usuzovat, že použitá metoda exktrakce společných faktorů odfiltrovaly z dat podstatnou relevantní informaci. Námi uváděné výsledky analýzy splňují tuto zásadu ve všech případech.

4.1 Evidence pro přijetí optimálního faktorového modelu 29 hrozeb

Polychorická korelační matice je součástí Přílohy k článku. Obr. 4.1a předkládá evidenci pro potvrzení bivariátního normálního rozdělení všech 29 proměnných. Obr. 4.1b ukazuje výsledky Bartletova testu sféricity a hodnotu KMO o vhodnosti proměnných pro faktorovou analýzu. Test nulovosti korelačních koeficientů je zamítnut, dané proměnné jsou tedy vhodné. Velikost koeficientu KMO (good – dobrá) taktéž potvrzuje vhodnost proměnných pro faktorovou analýzu. Hodnoty reliability na Obr. 4.1c ukazují, že oba extrahované faktory jsou akceptovatelné. Příznivé hodnoty znázorňuje i Obr. 4.1d. Akceptovatelný je McDonaldův koeficient spolehlivosti mnohorozměrného faktorového modelu, RMSR – druhá odmocnina z průměru reziduí, hodnota je nižší než je očekávaná hodnota podle Kelleyho kritéria. Znamená to, že pětifaktorový model je postačující pro odfiltrování podstatné informace z originálních dat.

[1] Lorenzo-Seva, U. (1999). Promin: a method for oblique factor rotation. Multivariate Behavioral Research, 34, 347-356.

Obr. 4.1a Mardiův test bivariátní mnohorozměrné normality

Analysis of the Mardia's (1970) multivariate asymmetry skewness and kurtosis.

	Coefficient	Statistic	df	P
Skewness	357.705	4769.406	4495	0.9978
SKewness corrected for small sample	357.705	4960.507	4495	1.0000
Kurtosis	887.943	-1.166		0.1218

Zdroj: vlastní

Obr. 4.1b Vhodnost proměnných pro faktorovou analýzu

```
ADEQUACY OF THE CORRELATION MATRIX

Determinant of the matrix     = 0.000000000032494
Bartlett's statistic          =  1654.3 (df =   406; P = 0.000010)
Kaiser-Meyer-Olkin (KMO) test = 0.81836 (good)
```

Zdroj: vlastní

Obr 4.1c Spolehlivost pětifaktorového modelu po jednotlivých faktorech

Factor	Variance	ORION
1	4.973	0.913
2	2.286	0.875
3	4.227	0.938
4	1.987	0.864
5	3.354	0.945

Zdroj: vlastní

Obr 4.1d Spolehlivost pětifaktorového modelu a jeho RMSR

```
                McDonald's Omega =   0.919452
     Standardized Cronbach's alpha =   0.917915
           Total observed variance =  29.000
             Total Common Variance =  24.265
Root Mean Square of Residuals (RMSR) =  0.0402
Expected mean value of RMSR          =  0.1125
for an acceptable mode (Kelley's criterion)
```

Zdroj: vlastní

Na základě uvedené analytické evidence lze ověřovaný výzkumný předpoklad uzavřít následujícím způsobem: *„Mezi jednotlivými typy hrozeb existují vzájemné vazby a kvantitativní analýzou lze provést redukci jednotlivých proměnných do maximálně pěti společných druhových oblastí.“*

Daný výzkumný předpoklad nelze zamítnout. Optimální model obsahuje celkem 5 společných faktorů.

4.2 Interpretace výsledků pětifaktorového modelu

Setříděné výsledky EFA dle velikosti regresních koeficientů ve společných pěti faktorech podává tabulka 4.2.

Obr. 4.2 Setříděná skladba pětifaktorového modelu

	1	2	3	4	5
Uzavření vzdušného prostoru	0,8800				
Kurzové výkyvy	0,7960				
Klimatické změny	0,7590				
Nedobytné pohledávky	0,7100				
Nedostatek přírodních zdrojů	0,7080				
Nákazy zvířat, epizootie	0,6290				
Selhání dodavatele	0,5980				
Stávky	0,4840				
Kolaps dopravní infrastruktury		0,6880			
Nákazy, epidemie		0,6470			
Živelní pohromy		0,4710			
Poškození životního prostředí		0,4670			
Kybernetické útoky			0,8820		
Přerušení dodávek energií a vody			0,7450		
Provozní IT a komunikační výpadky			0,7190		
Úniky dat			0,6680		
Požár			0,6570		
Bezpečnostní incidenty (vloupání, krádeže, vandalismus)			0,5790		
Válečný konflikt				0,8560	
Veřejné nepokoje, násilnosti				0,4620	
Teroristický útok				0,4550	
Trestní odpovědnost organizace					0,8280
Poškození dobrého jména					0,7940
Snížení kvality výkonu organizace					0,7140
Snížení rozpočtu, nedostatek financí					0,4880
Nedostatek knowhow a znalostí					0,3800
Změny legislativy					0,3490
Růst cen energií, nájmu, služeb					0,3350
Poškození zdraví, pracovní úraz					0,3240

Zdroj: vlastní

První faktor sdružuje hrozby, které souvisí převážně s **působením externích vlivů** na provoz organizace.

Pro proměnné ve druhém faktoru je charakteristický dopad především v souvislosti s rizikem nepředpokládaného **masivního výpadku lidských zdrojů**, jako primárního prostředku pro zajištění akceschopnosti a udržitelné úrovně provozu organizace. Rozsáhlou nedostupnost lidských zdrojů může znamenat také vyhlášení stávky, která je zahrnuta ve skladbě prvního faktoru. Nicméně v tomto případě se nejedná principiálně o hrozbu nepředpokládaného výpadku, neboť stávková pohotovost musí být předem ohlášena a zdůvodněna.

Třetí faktor sytí proměnné reprezentující **kybernetické a provozně-bezpečnostní hrozby**, které mají potenciál poškodit aktiva organizace. Regresní

koeficienty daných proměnných ve třetím společném faktoru vykazují oproti regresním koeficientům ostatních proměnných na zbývajících faktorech nejvyšší hodnoty.

Čtvrtý faktor se týká **hrozeb síly a násilí**. Ty nemusí být směřovány adresně proti konkrétní organizaci, nicméně mohou zprostředkovaně ohrozit kontinuitu činností organizace tím, že negativně působí na bezpečnostní prostředí, v němž organizace působí.

Společným jmenovatelem hrozeb v pátém faktoru je **přímý ekonomický, legislativní a provozní dopad na kontinuitu fungování organizace a úroveň zajišťovaných služeb**. Hrozby se vztahují adresně k dané organizaci a mohou vycházet jak z vnitřního prostředí (trestní odpovědnost, reputační dopady, zhoršení kvality výkonu, nedostatek financí a know-how, pracovní úrazy), tak z okolí organizace (legislativní dopady, růst cen surovin a služeb).

Závěr

Řízení kontinuity činností je progresivní metoda managementu organizace. Jeho význam roste exponenciálně s frekvencí výskytu a závažností nepředpokládaných událostí, které mají potenciál poškodit chráněné zájmy organizace.[1]

Z provedeného šetření a globálního průzkumu lze usuzovat, že vnímání většiny hrozeb je obdobné jak ve srovnání tuzemských orgánů veřejné správy s organizacemi obecně, tak s organizacemi veřejného sektoru v různých částech světa. Nelze tedy zamítnout tvrzení, že vnímání nejvýznamnějších i nejméně významných hrozeb pro kontinuitu činností organizací není úzce provázáno se sektorem působnosti či geografickou, resp. geopolitickou oblastí, v níž se nachází.

Ve výsledcích průzkumů lze nalézt zajímavé synergie. Nejvýraznější je pravděpodobně vysoké hodnocení kybernetických hrozeb (vždy se umístily na nejvyšších příčkách), přičemž aspekty zajištění kybernetických služeb patří také k nejdůležitějším tématům při rozhodování o volbě outsourcingu.[2]

Selhání dodavatele se v globálním průzkumu umístilo na relativně vysoké příčce (8. místo) hodnocení hrozeb, což v uvedeném kontextu zní jako logický výstup. Oproti tomu však ve výsledcích tuzemského průzkumu je selhání dodavatele posuzováno jako relativně „neškodná“ hrozba a to jak ze současného (22. pozice), tak ve tříletém výhledu (19. místo).

Nelze tudíž vyloučit, že respondenti tuzemského průzkumu nedostatečně dovozují rizika související s negativním dopadem selhání „třetí strany“ na jejich vlastní kontinuitu. Tato rizika se týkají především „morálního hazardu“, k němuž

[1] Např. SKROUPA, Christopher P. Why Companies Need a Business Continuity Plan. *Forbes* [online]. [cit. 2017-12-08]. Dostupné z: https://www.forbes.com/sites/christopherskroupa/2014/08/22/why-companies-need-a-business-continuity-plan/#232506a5f15b

[2] 2016 Global Outsourcing Survey: Outsourcing Accelerates forward [online]. In: Deloitte Consulting LLP, 2016, s. 12 [cit. 2017-10-05]. Dostupné z:https://www2.deloitte.com/us/en/pages/operations/articles/global-outsourcing-survey.html.

dochází, pokud činnost dodavatele není odpovídajícím způsobem kontrolována poskytovatelem veřejné služby.[1]

Velmi významný závěr vychází z výsledků explorativní faktorové analýzy. Z výsledků analýzy nelze zamítnout předpoklad, že původní soubor proměnných lze redukovat na základě posouzení vzájemných korelací, přičemž lze výsledky kvantitativní analýzy interpretovat i z kvalitativního hlediska. Explorativní faktorová analýza umožňuje nejen redukovat poměrně obsáhlou a neheterogenní množinu typových hrozeb, ale navíc může pomoci prostřednictvím vytvořených faktorů nalézt další souvislosti, které by posuzováním jednotlivých hrozeb zůstaly skryty.

Proto můžeme konstatovat, že explorativní faktorová analýza je efektivním nástrojem při zkoumáním oblastí, jako je krizové řízení, řízení kontinuity činností a bezpečnosti společnosti obecně.

Literatura

HENDL, Jan. *Přehled statistických metod zpracování dat*. Praha: Portál, 2004. 583 s. ISBN 80-7367-123-9.

KOVAŘÍK, Zdeněk, KVAPIL Jaroslav a Petr VLACH. *Úvod do počítačové analýzy úloh s aplikacemi.* Brno: Tribun EU, 2010. 321 s. ISBN 978-80-7399-950-6.

LORENZO-SEVA, U. (1999). Promin: A method for oblique factor rotation. Multivariate Behavioral Research, 34, p. 347-365.

MCDONALD Roderick, Peter. *Faktorová analýza a příbuzné metody v psychologii*. Praha: Academia, 1991. s. 252. ISBN 80-200-0081-X.

Internetové zdroje:

Exlorativní faktorová analýza: Základní pojmy. *Univerzita Karlova, Pedagogická fakulta, Katedra psychologie* [online]. [cit. 2017-09-08]. Dostupné z: http://kps.pedf.cuni.cz/skalouda/fa/exp_fak_analyza.htm.

Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy. *Statistics How To* [online]. 2016 [cit. 2017-08-15]. Dostupné z: http://www.statisticshowto.com/kaiser-meyer-olkin/.

The Business Continuity Institute: Research Reports [online]. [cit. 2017-08-03]. Dostupné z: http://www.thebci.org/index.php/resources/bci-research-reports

[1] KUFOVÁ, Veronika. Outsourcing ve veřejném sektoru. *Veřejná správa*. 2017, (2), 20-23. ISSN 0027-8009.

R E S U M É

Předložený příspěvek je zaměřen na posouzení výsledků hodnocení typových hrozeb pro kontinuitu provozu organizací veřejné správy. Vstupní údaje byly získány z výzkumu, jehož se jako respondenti zúčastnili manažeři a odborní zaměstnanci obcí s rozšířenou působností, krajských úřadů, služebních úřadů,[1] útvarů Policie České republiky a útvarů Hasičského záchranného sboru České republiky. Cílem článku je ověření výzkumných předpokladů zaměřených na:

a) porovnání výsledků průzkumu s aktuálními výsledky globálního hodnocení hrozeb pro zajištění kontinuity (BCI Horizon Scan),
b) mezičasové hodnocení vývoje vnímání hrozeb v tříletém horizontu a
c) sdružení 29 typových hrozeb do oblastí dle relevance s využitím kvantitativní analytické metody – explorační faktorové analýzy.

Klíčová slova: řízení kontinuity činností, Business Continuity Management (BCM), veřejná správa, organizace veřejné správy, explorační faktorová analýza.

S U M M A R Y

BOS, Ondřej, KOVAŘÍK, Zdeněk: IDENTIFICATION AND FACTORIAL ORGANISATION OF THREATS TO THE CONTINUITY OF PUBLIC ADMINISTRATION ACTIVITIES IN THE CZECH REPUBLIC

The presented paper is focused on the assessment of types of threats regarding the continuity of operations in the governmental organizations in the Czech Republic. Input research data are derived from a research of BCM level, on which participated managers and experts of the Czech governmental organizations,[2] Police of the Czech Republic and Fire Rescue Service of the Czech Republic. The objective of the paper is to verify research hypothesis focused on:

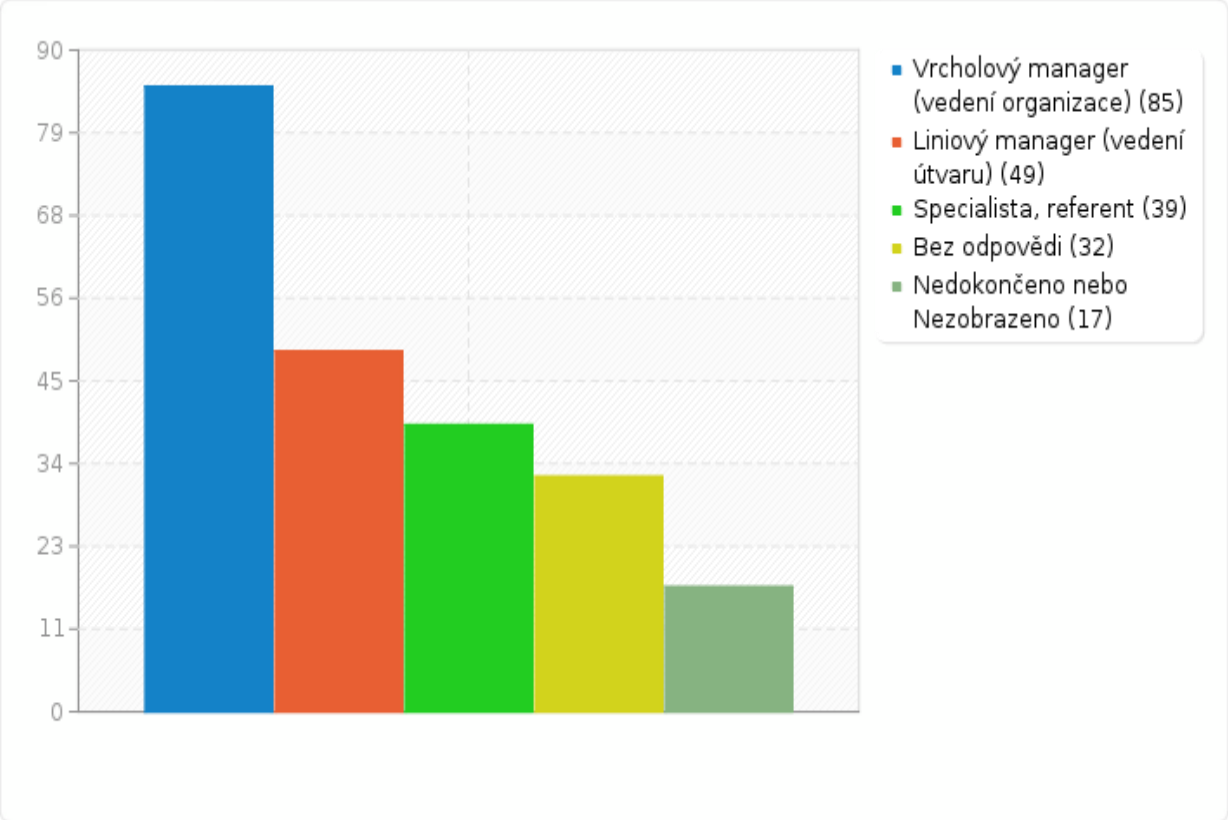
a) comparison of research results with the latest results of global threat assessment for securing continuity (BCM Global Horizon Scan),
b) inter-temporal development of assessment of threat perception on a three-year scale and
c) organisation of the 29 types of threats according to their fields of relevance while using quantitative analytical methods – exploratory factor analysis.

Keywords: Business Continuity Management, governmental administration, governmental organization, exploratory factor analysis.

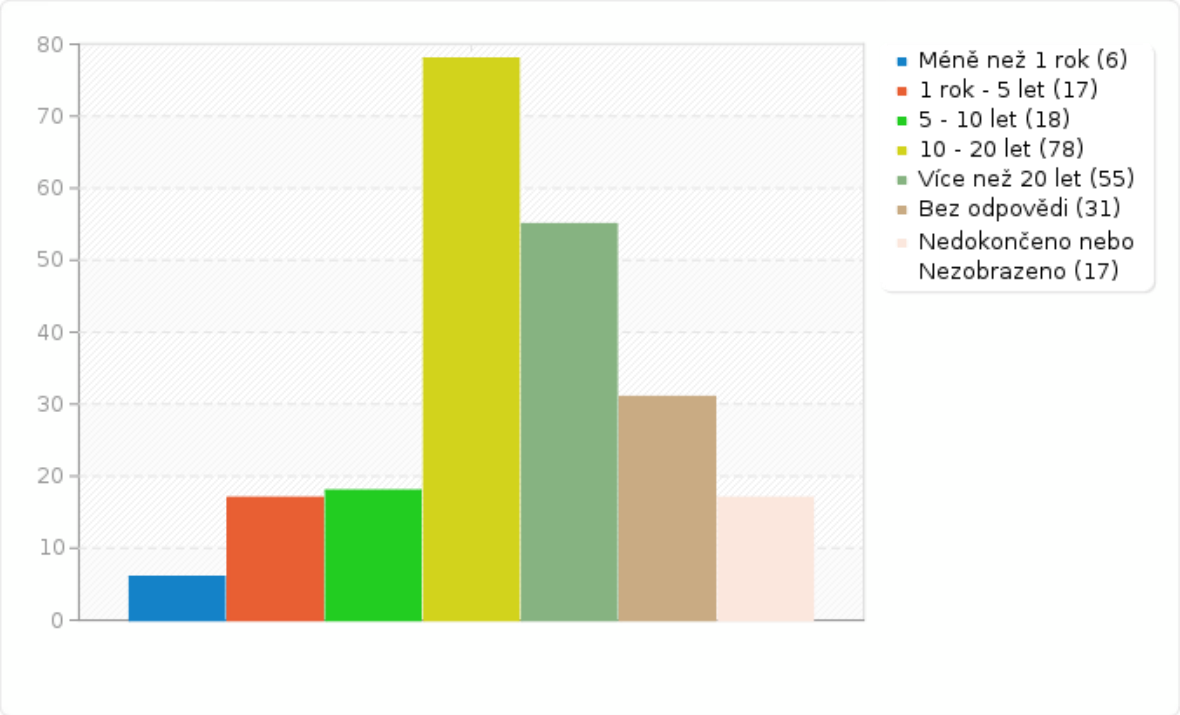
[1] Definice služebního úřadu je obsažena v § 4 zákona č. 234/2014 Sb., o státní službě.
[2] Definition of the governmental organization stipulated in the Section 4 of the Act No.234/2014 Coll., Public Service Act.

Příloha č. 1: Přehled respondentů zapojených do dotazníkového šetření

Jaké je Vaše pracovní zařazení?		
Odpověď	**Počet**	**Procenta**
Vrcholový manager (vedení organizace) (1)	85	38.29%
Liniový manager (vedení útvaru) (2)	49	22.07%
Specialista, referent (3)	39	17.57%
Bez odpovědi	32	14.41%
Nedokončeno nebo Nezobrazeno	17	7.66%

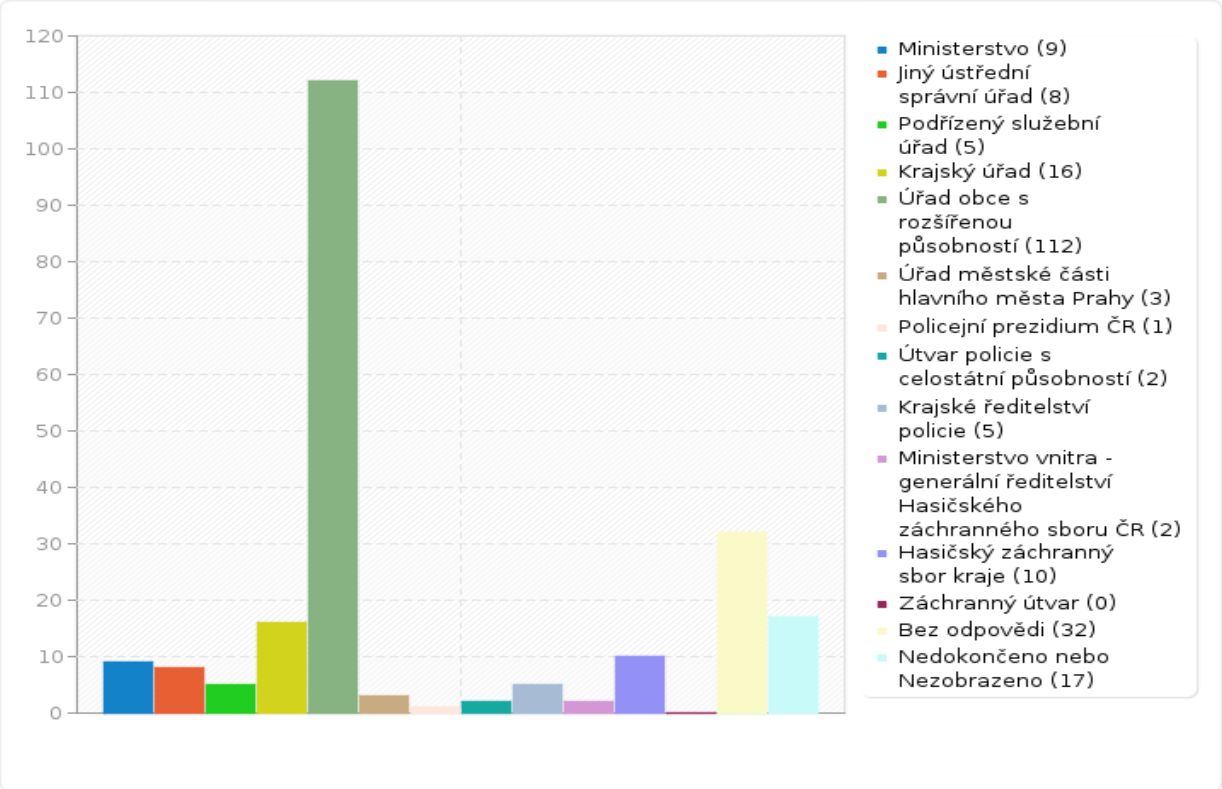


Jaká je délka Vaší praxe v oboru?		
Odpověď	**Počet**	**Procenta**
Méně než 1 rok (1)	6	2.70%
1 rok - 5 let (2)	17	7.66%
5 - 10 let (3)	18	8.11%
10 - 20 let (4)	78	35.14%
Více než 20 let (5)	55	24.77%
Bez odpovědi	31	13.96%
Nedokončeno nebo Nezobrazeno	17	7.66%

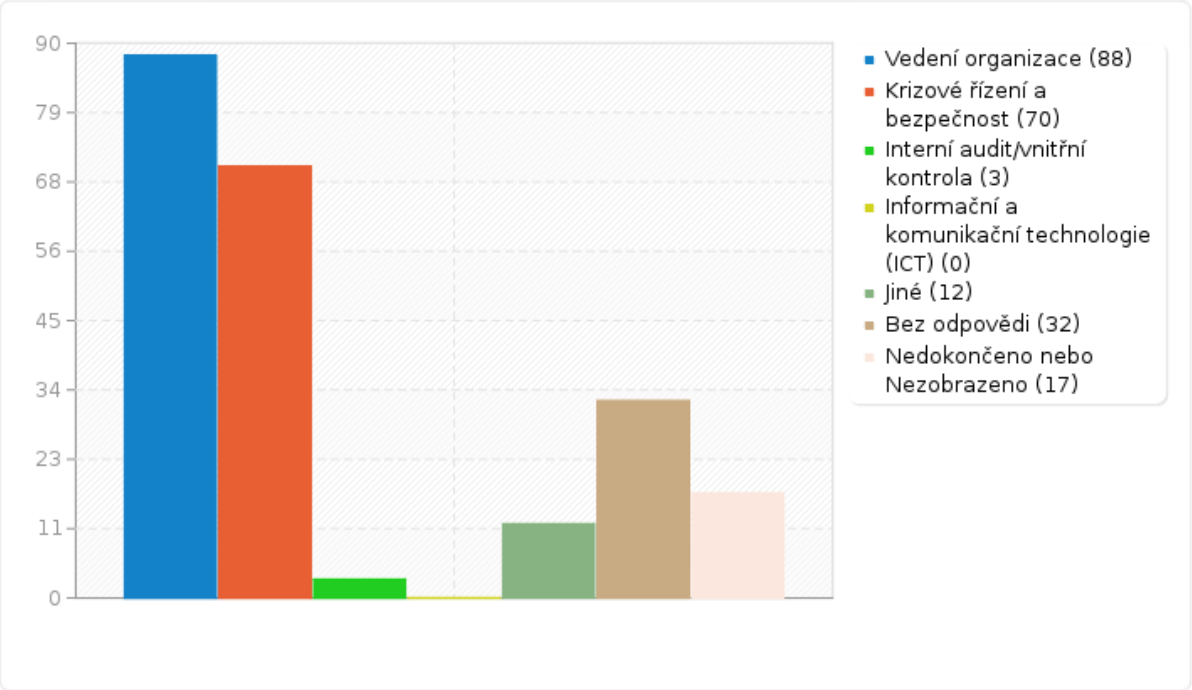


Do jaké skupiny patří organizace, kterou zastupujete?		
Odpověď	**Počet**	**Procenta**
Ministerstvo (1)	9	4.05%
Jiný ústřední správní úřad (2)	8	3.60%
Podřízený služební úřad (3)	5	2.25%
Krajský úřad (4)	16	7.21%
Úřad obce s rozšířenou působností (5)	112	50.45%
Úřad městské části hlavního města Prahy (6)	3	1.35%
Policejní prezidium ČR (7)	1	0.45%
Útvar policie s celostátní působností (8)	2	0.90%
Krajské ředitelství policie (9)	5	2.25%
Ministerstvo vnitra - generální ředitelství	2	0.90%

Do jaké skupiny patří organizace, kterou zastupujete?		
Odpověď	**Počet**	**Procenta**
Hasičského záchranného sboru ČR (10)		
Hasičský záchranný sbor kraje (11)	10	4.50%
Záchranný útvar (12)	0	0.00%
Bez odpovědi	32	14.41%
Nedokončeno nebo Nezobrazeno	17	7.66%



V rámci Vaší organizace zastupujete oblast:		
Odpověď	**Počet**	**Procenta**
Vedení organizace (1)	88	39.64%
Krizové řízení a bezpečnost (2)	70	31.53%
Interní audit/vnitřní kontrola (3)	3	1.35%
Informační a komunikační technologie (ICT) (4)	0	0.00%
Jiné	12	5.41%
Bez odpovědi	32	14.41%
Nedokončeno nebo Nezobrazeno	17	7.66%


90
79
68
56
45
34
23
11
0
Vedení organizace (88)
Krizové řízení a bezpečnost (70)
Interní audit/vnitřní kontrola (3)
Informační a komunikační technologie (ICT) (0)
Jiné (12)
Bez odpovědi (32)
Nedokončeno nebo Nezobrazeno (17)

Příloha č. 2: Polychorická korelační matice 29 proměnných

Variable	1	2	3	4	5	6	7	8	9	10	11
P01	1.000										
P02	0.620	1.000									
P03	0.671	0.770	1.000								
P04	0.610	0.503	0.530	1.000							
P05	-0.051	0.172	0.108	0.186	1.000						
P06	0.374	0.426	0.467	0.448	0.308	1.000					
P07	0.553	0.429	0.490	0.571	0.072	0.586	1.000				
P08	-0.043	0.178	0.137	0.067	0.478	0.232	0.088	1.000			
P09	0.348	0.365	0.435	0.329	0.227	0.452	0.467	0.247	1.000		
P10	0.279	0.443	0.422	0.262	0.346	0.534	0.438	0.196	0.438	1.000	
P11	0.030	0.219	0.189	0.012	0.159	0.197	0.145	0.297	0.050	0.251	1.000
P12	0.351	0.386	0.345	0.430	0.432	0.516	0.498	0.269	0.509	0.526	0.230
P13	0.324	0.458	0.261	0.171	0.154	0.264	0.136	0.075	0.198	0.344	0.173
P14	0.438	0.402	0.343	0.268	0.286	0.391	0.340	0.149	0.379	0.424	0.231
P15	0.153	0.189	0.080	0.231	0.389	0.287	0.272	0.326	0.238	0.407	0.137
P16	0.362	0.335	0.315	0.441	0.352	0.512	0.512	0.183	0.530	0.497	0.169
P17	0.033	0.274	0.157	0.153	0.550	0.308	0.200	0.322	0.260	0.497	0.164
P18	0.374	0.429	0.306	0.273	0.241	0.356	0.343	0.144	0.235	0.458	0.170
P19	0.297	0.358	0.263	0.161	0.022	0.204	0.257	0.005	0.083	0.180	0.315
P20	0.150	0.307	0.349	0.250	0.443	0.542	0.278	0.287	0.583	0.495	0.128
P21	0.108	0.228	0.111	0.097	0.355	0.204	0.172	0.257	0.146	0.369	0.125
P22	0.201	0.230	0.249	0.226	0.124	0.299	0.297	-0.036	0.630	0.334	0.043
P23	-0.274	-0.110	-0.090	-0.089	0.514	0.295	0.080	0.319	0.321	0.280	0.043
P24	-0.152	0.076	-0.058	0.003	0.551	0.207	0.127	0.365	0.194	0.263	0.103
P25	-0.118	-0.060	-0.030	0.031	0.401	0.329	0.134	0.262	0.372	0.254	0.134
P26	-0.500	-0.211	-0.250	-0.128	0.584	0.158	-0.062	0.243	0.216	0.190	-0.042
P27	-0.297	-0.089	-0.153	-0.088	0.588	0.138	-0.044	0.338	0.169	0.191	0.066
P28	-0.221	0.011	-0.068	-0.081	0.548	0.237	0.047	0.385	0.177	0.263	0.226
P29	0.124	0.493	0.278	0.130	0.163	0.307	0.237	0.119	0.226	0.518	0.309

Variable	12	13	14	15	16	17	18	19	20
P12	1.000								
P13	0.459	1.000							
P14	0.488	0.496	1.000						
P15	0.475	0.239	0.444	1.000					
P16	0.629	0.182	0.457	0.546	1.000				
P17	0.544	0.317	0.374	0.599	0.516	1.000			
P18	0.472	0.597	0.486	0.279	0.352	0.426	1.000		
P19	0.140	0.183	0.303	0.003	0.165	0.075	0.376	1.000	
P20	0.495	0.325	0.474	0.368	0.517	0.455	0.429	0.194	1.000
P21	0.281	0.249	0.278	0.307	0.212	0.388	0.371	0.237	0.252
P22	0.394	0.226	0.375	0.097	0.456	0.213	0.293	0.266	0.604
P23	0.294	-0.015	0.230	0.333	0.286	0.442	0.157	-0.010	0.442
P24	0.296	0.094	0.243	0.402	0.276	0.563	0.316	0.043	0.352
P25	0.305	0.075	0.286	0.256	0.371	0.300	0.223	0.068	0.616
P26	0.163	-0.061	0.072	0.231	0.128	0.383	0.074	-0.087	0.431
P27	0.276	0.035	0.180	0.343	0.336	0.542	0.189	-0.106	0.315
P28	0.399	0.143	0.230	0.468	0.376	0.588	0.204	-0.013	0.354
P29	0.467	0.572	0.340	0.333	0.311	0.466	0.570	0.279	0.338

Variable	21	22	23	24	25	26	27	28	29
P21	1.000								
P22	0.201	1.000							
P23	-0.274	-0.110	1.000						
P24	-0.152	0.076	-0.058	1.000					
P25	-0.118	-0.060	-0.030	0.031	1.000				
P26	-0.500	-0.211	-0.250	-0.128	0.584	1.000			
P27	-0.297	-0.089	-0.153	-0.088	0.588	0.138	1.000		
P28	-0.221	0.011	-0.068	-0.081	0.548	0.237	0.047	1.000	
P29	0.124	0.493	0.278	0.130	0.163	0.307	0.237	0.119	1.000